If this request-for-share-distribution signal is received, the authentication server 23 will search the public key certification of the automatic setting equipment 11 corresponding to the automatic setting device identifier in the automatic setting equipment 11 of this connection destination with reference to the repository 105 based on the automatic setting device identifier of the received request-for-share-distribution signal (S115). The authentication server 23 creates the signal transmission (handing out signal) which accommodates the public key certification of the searched automatic setting equipment 11 of a connection destination, and replies it to the automatic setting equipment 11 of a connecting agency (S116).

[0111]

If this handing out signal is received, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency will verify whether the public key certification of the automatic setting equipment 11 of a connection destination is genuine using the public key certification of the authentication server 23 (S117).

[0112]

Next, it describes about the method of obtaining the public key certification of another side by exchanging the public key certification of the automatic setting equipment 11 mutually in the automatic setting equipment 11 of a connection destination a connecting agency.

[0113]

The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency creates the signal transmission (public key certification notification signal) which accommodated the public key certification of the own (automatic setting equipment 11 of a connecting agency) automatic setting equipment 11, and transmits to the automatic setting equipment 11 of a connection destination (S118).

[0114]

The tunnel set part 62 in the automatic setting equipment 11 of the connection destination received from the automatic setting equipment 11 of this public key certification notification signal connection-origin, It is verified whether it is genuine using the public key certification of the authentication server 23 in the public key certification of the automatic setting equipment 11 of the connection origin accommodated in this received public key certification notification signal (S119). And the tunnel set part 62 in the automatic setting equipment 11 of a connection destination judges whether the public key certification of the automatic setting equipment 11 of a connecting agency is a public key certification of the genuine automatic setting equipment 11 by judging the result verified by the processing S118 (S120). According to this embodiment, since the public key certification of the authentication server 23 is a self signature, it is improving the reliability of the public key of the automatic setting equipment 11 by performing such processing S120.

[0115]

The tunnel set part 62 in the automatic setting equipment 11 of a connection destination, The signal transmission (decision result notification signal) which accommodated the decision result is created to the automatic setting equipment 11 of a connecting agency, and it transmits to it (S121), and in not being a genuine public key certification as a result of judgment, the automatic setting equipment 11 of a connecting agency judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in being a genuine public key certification as a result of judgment, The tunnel set part 62 in the automatic setting equipment 11 of a connection destination transmits the signal transmission (public key certification notification signal) which accommodated the public key certification of the own (automatic setting

equipment 11 of a connection destination) automatic setting equipment 11 to the automatic setting equipment 11 of a connecting agency (S122).

[0116]

The tunnel set part 62 in the automatic setting equipment 11 of the connection origin which received this public key certification notification signal from the automatic setting equipment 11 of the connection destination, It is verified whether it is genuine using the public key certification of the authentication server 23 in the public key certification of the automatic setting equipment 11 of a connection destination accommodated in this received public key certification notification signal (S123). And the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency judges whether the public key certification of the automatic setting equipment 11 of a connection destination is a public key certification of the genuine automatic setting equipment 11 by judging the result verified by the processing S123 (S124).

[0117]

The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, The signal transmission (decision result notification signal) which accommodated the decision result is created to the automatic setting equipment 11 of a connection destination, and it transmits to it (S125), and in not being a genuine public key certification as a result of judgment, the automatic setting equipment 11 of a connection destination judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in being a genuine public key certification as a result of judgment, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency generates a challenge character string at random (S126). And the automatic setting equipment 11 of a connecting agency creates the signal transmission (challenge character string notification signal) which accommodates the generated challenge character string, and transmits to the automatic setting equipment 11 of a connection destination (S127).

[0118]

The tunnel set part 62 in the automatic setting equipment 11 of a connection destination, If a challenge character string notification signal is received, the challenge character string accommodated in this signal will be calculated with the predetermined arithmetic method on which it decided previously between the automatic setting equipment 11, A response character string is generated by enciphering the result of an operation with the secret key (secret key of the automatic setting equipment 11 of a connection destination) of the own (automatic setting equipment 11 of a connection destination) automatic setting equipment 11 (S128). Although what kind of arithmetic method it may be sufficient as this predetermined arithmetic method, it is a one-way hash function (one-way hash function) in this embodiment, for example. Therefore, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination generates a response character string by calculating the hash value of a challenge character string and enciphering the calculated hash value with the secret key of the own automatic setting equipment 11. Next, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination creates the signal transmission (response character string notification signal) which accommodates a response character string, and transmits to the automatic setting equipment 11 of a connecting agency (S129).

[0119]

The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, The result of an operation which calculated the challenge character string generated by the processing S126 with the above-mentioned predetermined arithmetic method when the response character string notification signal was received, The decoding result which decrypted the response character

string accommodated in this signal by the public key of the automatic setting equipment 11 of the connection destination included in the public key certification of the automatic setting equipment 11 of a connection destination is compared, and it is judged whether it corresponds or not (S130).

[0120]

The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, In creating the signal transmission (decision result notification signal) which accommodated the decision result to the automatic setting equipment 11 of a connection destination, transmitting to it (S131) and not corresponding as a result of judgment, the automatic setting equipment 11 of a connection destination judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in corresponding as a result of judgment, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency continues the below-mentioned processing.

[0121]

If a decision result notification signal is received, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination will create the challenge character string notification signal which generates a challenge character string at random (S132), and accommodates the generated challenge character string, and will transmit to the automatic setting equipment 11 of a connecting agency (S133).

[0122]

The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, If this challenge character string notification signal is received, the challenge character string accommodated in this signal will be calculated with an above-mentioned predetermined arithmetic method, A response character string is generated by enciphering the result of an operation with the secret key (secret key of the automatic setting equipment 11 of a connection destination) of the own automatic setting equipment 11 (S134). Next, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency creates the response character string notification signal which accommodates a response character string, and transmits to the automatic setting equipment 11 of a connection destination (S135).

[0123]

The tunnel set part 62 in the automatic setting equipment 11 of a connection destination, The result of an operation which calculated the challenge character string generated by the processing S132 with the above-mentioned predetermined arithmetic method when the response character string notification signal was received, The decoding result which decrypted the response character string accommodated in this signal by the public key of the automatic setting equipment 11 of the connection origin included in the public key certification of the automatic setting equipment 11 of a connecting agency is compared, and it is judged whether it corresponds or not (S136). The tunnel set part 62 in the automatic setting equipment 11 of a connection destination, In creating the decision result notification signal which accommodated the decision result to the automatic setting equipment 11 of a connecting agency, transmitting to it (S137) and not corresponding as a result of judgment, the automatic setting equipment 11 of a connecting agency judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in corresponding as a result of judgment, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination continues the below-mentioned processing.

[0124]

Thus, according to this embodiment, the cryptographic key pair was likened with the password and challenge-response authentication technology is used.

[0125]

The automatic setting equipment 11 of a connecting agency and the automatic setting equipment 11 of a connection destination perform mutual recognition using the authentication server 23 which is an independent organization by performing the above the processing S101 thru/or the processing S137.

[0126]

If it succeeds in mutual recognition, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency and the tunnel set part 62 in the automatic setting equipment 11 of a connection destination will exchange mutually information required for setting out of 6o4 tunnel. Namely, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, The own tunnel external IP address in the automatic setting equipment 11, inside IP address of a tunnel, and its prefix length, Create the signal transmission (tunnel construction indication signal) which accommodated IPsec setup information and the information on the purport that construction of a tunnel is instructed, and it transmits to the automatic setting equipment 11 of a connection destination (S138), On the other hand, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination, The own tunnel external IP address in the automatic setting equipment 11, inside IP address of a tunnel, and its prefix length, The signal transmission (tunnel construction indication signal) which accommodated IPsec setup information and the information on the purport that construction of a tunnel is instructed is created, and it transmits to the automatic setting equipment 11 of a connecting agency (S139). Here, the inside IP address of a tunnel and its prefix length are information which is needed in order to set up the security policy of IPsec.

[0127]

It is judged whether the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency can set up 6o4 tunnel using the memorized information (S140). Judgment of the propriety of this tunnel setting out The tunnel external address of a connecting agency, The inside IP address of a tunnel of a connecting agency, the tunnel external IP address of a connection destination, It is the existence of the inside IP address of a tunnel of a connection destination, and IPsec setup information, when there is these information, it is judged that setting out of 6o4 tunnel is possible, and when it is missing among these information whether it is either, setting out of 6o4 tunnel is judged to be impossible. When it is judged as a result of judgment that it is impossible, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency creates the signal transmission (decision result notification signal) which accommodates a decision result, transmits to the automatic setting equipment 11 of a connection destination (S149), and ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is possible, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency creates the signal transmission (decision result notification signal) which accommodates a decision result, and transmits to the automatic setting equipment 11 of a connection destination (S141).

[0128]

It is judged whether on the other hand, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination can set up 6o4 tunnel using the memorized information (S142). When it is judged as a result of judgment that it is impossible, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination creates the signal transmission

(decision result notification signal) which accommodates a decision result, transmits to the automatic setting equipment 11 of a connecting agency (S155), and ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is possible, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination creates the signal transmission (decision result notification signal) which accommodates a decision result, and transmits to the automatic setting equipment 11 of a connecting agency (S143).

[0129]

If the decision result notification signal which accommodates the decision result of the purport that it was judged from the automatic setting equipment 11 of another side that setting out of 6o4 tunnel was possible is received, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency and a connection destination will perform processing which eliminates a connection, respectively (S144). If a connection is eliminated, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency and the tunnel set part 62 in the automatic setting equipment 11 of a connection destination will perform tunnel construction processing which builds 6o4 tunnel, respectively (S145, S146).

[0130]

If it describes in details more about this tunnel construction processing, in Fig.19, the tunnel set part 62 in the control part 52 of the automatic setting equipment 11 will generate the tunnel name of the 6o4 tunnel which it is going to set up automatically according to a predetermined procedure (S151).

[0131]

The predetermined procedure which generates a tunnel name, for example like the procedure which assigns a numerical value in order, or the procedure which assigns the alphabet to order, If it overlaps and a tunnel name is not generated, what kind of procedure may be sufficient, but in this embodiment, it is a procedure which gives the alphabet to "6o4" which called for short the IPv6overIPv4 tunnel in which the kind of tunnel is shown in order.

[0132]

Next, the tunnel set part 62 in the control part 52 of the automatic setting equipment 11 judges whether IPsec is set up or not by referring to the IPsec setup information accommodated in the tunnel construction indication signal (S152). In not setting up IPsec as a result of judgment (un-setting up), the tunnel set part 62 of the automatic setting equipment 11 performs the below-mentioned processing S155.

[0133]

On the other hand, in setting up IPsec as a result of judgment (setting out), the tunnel set part 62 of the automatic setting equipment 11 sets up the security policy (Security Policy) which specifies the processing method of an IP packet about the tunnel to build (S153). Namely, the tunnel set part 62 of the automatic setting equipment 11, The security policy database which matches and registers the information (selector) for specifying the processing method of an IP packet, and an IP packet () [Security Policy Database and] Hereafter, it is written as "SPD". It creates and created SPD is memorized to the storage part 53. A selector A security policy number, a transmitting agency IP address, destination IP addresses, The polish which are a transmission origin port number, a destination port number, and a transport layer protocol, and specifies the processing method of an IP packet, They are an IP address of the processing method (action) of an IP packet, a security protocol, encapsulation Mohd, ****** of input and output, and the Nobumoto side security gateway, and destination IP addresses of the address side

security gateway. The processing methods of an IP packet are cancellation of an IP packet, the passage for IPsec unsuitable, and passage of IPsec application. These are set up about the tunnel to build. Namely, in the automatic setting equipment 11 of a connecting agency between the automatic setting equipment 11 of a connection destination, In setting up the security policy that the direction of input and output is set to out among security policies, A number is assigned in order by the security policy number, and for a transmitting agency IP address, They are set up by the inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of a connecting agency, and in destination IP addresses, The inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of the connection destination acquired by the processing S139 are set up, A transmission origin port number, a destination port number, a transport layer protocol, To action, a security protocol, and encapsulation Mohd (for example, in this embodiment, it fixes to tunnel mode.), Based on the IPsec pertinent information memorized previously, it is set to the storage part 53 of the automatic setting equipment 11, and for the IP address of the transmitting agency side security gateway, It is set up by the tunnel external IP address in the automatic setting equipment 11 of a connecting agency, and in the destination IP addresses of the address side security gateway, The tunnel external IP address in the automatic setting equipment 11 of a connection destination accommodated in the connection destination tunnel external IP address reply signal acquired from the information server 21 by the processing S104 is set up. Passage of IPsec application is set to the processing method of an IP packet. In setting up the security policy that the direction of input and output is set to in among security policies, between the automatic setting equipment 11 of a connection destination in the automatic setting equipment 11 of a connecting agency, A number is assigned in order by the security policy number, and for a transmitting agency IP address, They are set up by the inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of the connection destination acquired by the processing S139, and in destination IP addresses, The inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of a connecting agency are set up, A transmission origin port number, a destination port number, a transport layer protocol, To action, a security protocol, and encapsulation Mohd (for example, in this embodiment, it fixes to tunnel mode.), Based on the IPsec pertinent information memorized previously, it is set to the storage part 53 of the automatic setting equipment 11, and for the IP address of the transmitting agency side security gateway, By the processing S104, it is set up by the tunnel external IP address in the automatic setting equipment 11 of a connection destination accommodated in the connection destination tunnel external IP address reply signal acquired from the information server 21, and in the destination IP addresses of the address side security gateway, The tunnel external IP address in the automatic setting equipment 11 of a connecting agency is set up, and passage of IPsec application is set to the processing method of an IP packet. On the other hand in the automatic setting equipment 11 of a connection destination, between the automatic setting equipment 11 of a connection destination, In setting up the security policy that the direction of input and output is set to out among security policies, A number is assigned in order by the security policy number, and for a transmitting agency IP address, They are set up by the inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of a connection destination, and in destination IP addresses, The inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of the connection origin transmitted from the automatic setting equipment 11 of the connecting agency by the processing S138 are set up, A transmission origin port number, a destination port number, a transport layer protocol, To action, a security protocol, and encapsulation Mohd (for example, in this embodiment, it fixes to

tunnel mode.), Based on the IPsec pertinent information memorized previously, it is set to the storage part 53 of the automatic setting equipment 11, and for the IP address of the transmitting agency side security gateway, It is set up by the tunnel external IP address in the automatic setting equipment 11 of a connection destination, and in the destination IP addresses of the address side security gateway, The tunnel external IP address in the automatic setting equipment 11 of the connection origin acquired from the connection information established in tunnel construction processing between the automatic setting equipment 11 of a connecting agency and the automatic setting equipment 11 of a connection destination is set up. Passage of IPsec application is set to the processing method of an IP packet. In setting up the security policy that the direction of input and output is set to in among security policies, between the automatic setting equipment 11 of a connection destination in the automatic setting equipment 11 of a connection destination, A number is assigned in order by the security policy number, and for a transmitting agency IP address, They are set up by the inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of the connection origin acquired by the processing S138, and in destination IP addresses, The inside IP address of a tunnel in the automatic setting equipment 11 and its prefix length of a connection destination are set up, A transmission origin port number, a destination port number, a transport layer protocol, To action, a security protocol, and encapsulation Mohd (for example, in this embodiment, it fixes to tunnel mode.), Based on the IPsec pertinent information memorized previously, it is set to the storage part 53 of the automatic setting equipment 11, and for the IP address of the transmitting agency side security gateway, The tunnel external IP address in the automatic setting equipment 11 of the connection origin acquired from the connection information established in tunnel construction processing between the automatic setting equipment 11 of a connecting agency and the automatic setting equipment 11 of a connection destination is set up, The tunnel external IP address in the automatic setting equipment 11 of a connection destination is set to the destination IP addresses of the address side security gateway.

[0134]

Next, the tunnel set part 62 of the automatic setting equipment 11 establishes a security association (Security Association and the following write it as "SA".) about each of a connection destination and a connection destination to a connecting agency from a connecting agency (S154). Namely, about each of SA from a connecting agency to a connection destination, and SA from a connection destination to a connecting agency the tunnel set part 62 of the automatic setting equipment 11, Perform the negotiation which performs presentation of an encryption algorithm, determination, exchange of an encryption key, etc. using IKE, and SA is determined, Determined SA is registered into a security association database (Security Association Database and the following write it as "SAD".). SAD is memorized by the storage part 53. The encryption algorithms shown using IKE are common key encryption systems, such as DES-CBC, 3 DES-CBC, CAST-128, RC-5, IDEA, and Blowfish.

[0135]

Next, the tunnel set part 62 of the automatic setting equipment 11, The tunnel name generated by the processing S151, the IP address assigned by DHCP server 26 by the processing S153 (tunnel external IP address of a connecting agency), The inside IP address of a connecting agency tunnel, the connection destination automatic setting device identifier which is input from the input part 54 and memorized by the storage part 53, The connection destination tunnel external IP address acquired from the information server 21 by the processing 103, The inside IP address of a connection destination tunnel generated by the processing S151, the IPsec setup information

which is input from the input part 54 and memorized by the storage part 53, And it registers with each field which is the information which shows ending with setting out and where the setting-out tunnel-pipes Osamu information table 101 corresponds "finishing [setting out]", respectively (S155).
[0136]
And it is judged whether the tunnel set part 62 of the automatic setting equipment 11 has the built normally usable tunnel (S156). As a result of judgment, the automatic setting equipment 11 starts operation of 6o4 tunnel, when normally usable (Yes) (S157), and when not normally usable, it redoes tunnel automatic setting processing from the processing S61 again to (No) (S158). For example, the tunnel set part 62 of the automatic setting equipment 11 transmits the ping (Ping) to the 6o4 built tunnel, and judges whether the reply is received. When it is judged that the 6o4 built tunnel was normally built usable when the reply of a ping was received and the reply of a ping is not received, it is judged that the 6o4 built tunnel was not built usable normally.
[0137]
When the tunnel set part 62 in the automatic setting equipment 11 of such processing S151 thru/or the processing S158 connection-origin and the tunnel set part 62 in the automatic setting equipment 11 of a connection destination perform, respectively, 6o4 tunnel is built and communication using 6o4 tunnel is attained.
[0138]
And when setting up two or more 6o4 tunnels, the automatic setting equipment 11. After performing initial processing of the processing S61 thru/or the processing S68, the processing S101 thru/or tunnel construction processing of the processing S146 (the processing S151 thru/or tunnel construction processing of the processing S155 are included) are performed every six oeach 4 tunnel. For example, as shown in Fig.1, when automatic setting equipment 11-A sets up 6o4 tunnel, respectively between automatic setting equipment 11-B and automatic setting equipment 11-C. First, automatic setting equipment 11-A performs initial processing of the processing S61 thru/or the processing S68, next performs the processing S101 thru/or tunnel construction processing of the processing S146 between automatic setting equipment 11-B, 6o4 tunnel 5-AB is set up, and the processing S101 thru/or tunnel construction processing of the processing S146 are performed between automatic setting equipment 11-C, and 6o4 tunnel 5-AC is set up. After automatic setting equipment 11-A sets up 6o4 tunnel 5-AC, the order which may set up 6o4 tunnel 5-AB and sets up 6o4 tunnel is arbitrary.
[0139]
The automatic setting equipment 11 can set up 6o4 tunnel automatically by Kami who performed mutual recognition using an independent organization to have described above. For this reason, setting up 6o4 tunnel among the unauthorized automatic setting equipment 11 which is not meant, such as spoofing, is prevented. Since IPsec is available, high communication of security can be performed.
[0140]
And since it is selectable every 6o4 tunnel by inputting from the input part 54 and registering with the setting-out tunnel-pipes Osamu information table 101 every 6o4 tunnel, use of this IPsec, Since IPsec can be used according to the communicative contents when required, when communicating, the amount of information processings of the automatic setting equipment 11 can be reduced, and the load of the automatic setting equipment 11 can be reduced.
[0141]

When ending use of 6o4 tunnel, tunnel cut treating which cuts automatically the tunnel which used the authentication server 23 is performed.
[0142]
Next, it describes about tunnel cut treating. Fig.22 thru/or Fig.26 are the sequence diagrams (the 1- the 5) showing operation of the tunnel deletion in tunnel automatic setting processing.
[0143]
In Fig.22 thru/or Fig.26, the tunnel cutout 65 in the control part 52 of the automatic setting equipment 11 of a cutting agency,First, "under cutting" is registered into the tunnel established-state information field 119 of the record corresponding to the 6o4 tunnel which it is going to cut in the setting-out tunnel-pipes Osamu information table 101 (S303). [which is the information which shows under cutting of 6o4 tunnel]
[0144]
Next, the tunnel cutout 65 of the automatic setting equipment 11 of a cutting agency performs the update process which updates the public key certification of the automatic setting equipment 11 that the validity of the public key certification of the automatic setting equipment 11 should be checked (S304). Since this update process is the same as the above-mentioned update process described using Fig.20 and Fig.21, that description is omitted.
[0145]
Next, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency creates the signal transmission (cutting start notification signal) which accommodated the information on the purport that cutting of 6o4 tunnel is started, and transmits to the automatic setting equipment 11 of a cutting place (S305).
[0146]
If a cutting start notification signal is received, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place will perform the update process which updates the public key certification of the automatic setting equipment 11 that the validity of the public key certification of the automatic setting equipment 11 should be checked (S306). Since this update process is the same as the above-mentioned update process described using Fig.20 and Fig.21, that description is omitted.And the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place creates the signal transmission (cutting consent notification signal) which accommodated the information on the purport that it consents to the cutting start of a tunnel, and replies it to the automatic setting equipment 11 of a cutting agency (S307).
[0147]
If a cutting consent notification signal is received, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency will create an automatic setting device identifier notification signal, and will transmit to the automatic setting equipment 11 of a cutting place (S308).
[0148]
If this automatic setting device identifier notification signal is received from the automatic setting equipment 11 of a cutting agency, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place, The signal transmission (automatic setting device identifier notification signal) which accommodates an own (automatic setting equipment 11 of a cutting place) automatic setting device identifier is created, and it transmits to the automatic setting equipment 11 of a cutting agency (S309).
[0149]
Next, the automatic setting equipment 11 of a cutting agency and a cutting place has two kinds of obtaining methods of this public key certification, although the public key certification of the

automatic setting equipment 11 of another side comes to hand and the public key certification of ********** 11 of another side which came to hand checks it in Shinsei, respectively.

[0150]

First, it describes a cutting agency about the method of obtaining the public key certification of the automatic setting equipment 11 of another side from an authentication server in the automatic setting equipment 11 of a cutting place.

[0151]

The tunnel cutout 65 in the automatic setting equipment 11 of a cutting place creates a request-for-share-distribution signal, and transmits to the authentication server 23 so that it may receive handing out of the public key certification in the automatic setting equipment 11 of a cutting agency (S310).

[0152]

If this request-for-share-distribution signal is received, the authentication server 23 will search the public key certification of the automatic setting equipment 11 corresponding to the automatic setting device identifier in the automatic setting equipment 11 of this cutting origin with reference to the repository 105 based on the automatic setting device identifier of the received request-for-share-distribution signal (S311). Based on search results, the authentication server 23 creates a handing out signal, and replies it to the automatic setting equipment 11 of a cutting place (S312).

[0153]

If this handing out signal is received, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place will verify whether the public key certification of the automatic setting equipment 11 of a cutting agency is genuine using the public key certification of the authentication server 23 (S313).

[0154]

the automatic setting equipment 11 of a cutting place to this automatic setting device identifier notification signal -- receiving (S309) -- the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency, A request-for-share-distribution signal is created and it transmits to the authentication server 23 in order to receive handing out of the public key certification in the automatic setting equipment 11 of a cutting place (S314).

[0155]

If this request-for-share-distribution signal is received, the authentication server 23 will search the public key certification of the automatic setting equipment 11 corresponding to the automatic setting device identifier in the automatic setting equipment 11 of this cutting place with reference to the repository 105 based on the automatic setting device identifier of the received request-for-share-distribution signal (S315). The authentication server 23 creates a handing out signal based on search results, and replies it to the automatic setting equipment 11 of a cutting agency (S316).

[0156]

If this handing out signal is received, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency will verify whether the public key certification of the automatic setting equipment 11 of a cutting place is genuine using the public key certification of the authentication server 23 (S317).

[0157]

Next, it describes about the method of obtaining the public key certification of another side by exchanging the public key certification of the automatic setting equipment 11 mutually in the automatic setting equipment 11 of a cutting place a cutting agency.

[0158]
The tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency creates an own (automatic setting equipment 11 of a cutting agency) public key certification notification signal, and transmits to the automatic setting equipment 11 of a cutting place (S318).
[0159]
The tunnel cutout 65 in the automatic setting equipment 11 of the cutting place which received this public key certification notification signal from the automatic setting equipment 11 of the cutting agency, It is verified whether it is genuine using the public key certification of the authentication server 23 in the public key certification of the automatic setting equipment 11 of the cutting origin accommodated in this received public key certification notification signal (S319). And the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place judges whether the public key certification of the automatic setting equipment 11 of a cutting agency is a public key certification of the genuine automatic setting equipment 11 by judging the result verified by the processing S319 (S320).
[0160]
The tunnel cutout 65 in the automatic setting equipment 11 of a cutting place, A decision result notification signal is created to the automatic setting equipment 11 of a cutting agency, and it transmits to it (S321), and in not being a genuine public key certification as a result of judgment, the automatic setting equipment 11 of a cutting agency judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in being a genuine public key certification as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place transmits an own (automatic setting equipment 11 of a cutting place) public key certification notification signal to the automatic setting equipment 11 of a cutting agency (S322).
[0161]
The tunnel cutout 65 in the automatic setting equipment 11 of the cutting origin which received this public key certification notification signal from the automatic setting equipment 11 of the cutting place, It is verified whether it is genuine using the public key certification of the authentication server 23 in the public key certification of the automatic setting equipment 11 of a cutting place accommodated in this received public key certification notification signal (S323). And the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency judges whether the public key certification of the automatic setting equipment 11 of a cutting place is a public key certification of the genuine automatic setting equipment 11 by judging the result verified by the processing S323 (S324).
[0162]
The tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency, A decision result notification signal is created to the automatic setting equipment 11 of a cutting place, and it transmits to it (S325), and in not being a genuine public key certification as a result of judgment, the automatic setting equipment 11 of a cutting place judges that it is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in being a genuine public key certification as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency generates a challenge character string at random (S326). And the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency creates a challenge character string notification signal, and transmits to the automatic setting equipment 11 of a cutting place (S327).
[0163]

The tunnel cutout 65 in the automatic setting equipment 11 of a cutting place, If a challenge character string notification signal is received, the challenge character string accommodated in this signal will be calculated with the predetermined arithmetic method on which it decided previously between the automatic setting equipment 11, A response character string is generated by enciphering the result of an operation with the secret key (secret key of the automatic setting equipment 11 of a cutting place) of the own (automatic setting equipment 11 of a cutting place) automatic setting equipment 11 (S328). Next, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place creates a response character string notification signal, and transmits to the automatic setting equipment 11 of a cutting agency (S329).

[0164]

The tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency, The result of an operation which calculated the challenge character string generated by the processing S326 with the above-mentioned predetermined arithmetic method when the response character string notification signal was received, The decoding result which decrypted the response character string accommodated in this signal by the public key of the automatic setting equipment 11 of a cutting place accommodated in the public key certification of the automatic setting equipment 11 of a cutting place is compared, and it is judged whether it corresponds or not (S330). When creating a decision result notification signal to the automatic setting equipment 11 of a cutting place, transmitting to it (S331) and not corresponding as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency judges that the automatic setting equipment 11 of a cutting place is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in corresponding as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency continues the below-mentioned processing.

[0165]

If a decision result notification signal is received, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place will generate a challenge character string at random (S332), will create a challenge character string notification signal, and will transmit to the automatic setting equipment 11 of a cutting agency (S333).

[0166]

The tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency, If this challenge character string notification signal is received, the challenge character string accommodated in this signal will be calculated with an above-mentioned predetermined arithmetic method, A response character string is generated by enciphering the result of an operation with the secret key (secret key of the automatic setting equipment 11 of a cutting place) of the own automatic setting equipment 11 (S334). Next, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency creates a response character string notification signal, and transmits to the automatic setting equipment 11 of a cutting place (S335).

[0167]

The tunnel cutout 65 in the automatic setting equipment 11 of a cutting place, The result of an operation which calculated the challenge character string generated by the processing S332 with the above-mentioned predetermined arithmetic method when the response character string notification signal was received, The decoding result which decrypted the response character string accommodated in this signal by the public key of the automatic setting equipment 11 of the cutting origin accommodated in the public key certification of the automatic setting equipment 11 of a cutting agency is compared, and it is judged whether it corresponds or not

(S336). When creating a decision result notification signal to the automatic setting equipment 11 of a cutting agency, transmitting to it (S337) and not corresponding as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place judges that the automatic setting equipment 11 of a cutting agency is not the genuine automatic setting equipment 11, and ends this processing. On the other hand, in corresponding as a result of judgment, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place continues the below-mentioned processing.

[0168]

The automatic setting equipment 11 of a cutting agency and the automatic setting equipment 11 of a cutting place perform mutual recognition using the authentication server 23 which is an independent organization by performing the above the processing S304 thru/or the processing S337.

[0169]

If it succeeds in mutual recognition, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency and the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place will exchange mutually information required for cutting of 6o4 tunnel. Namely, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency, Create the signal transmission (tunnel disconnect indication signal) which accommodated the information for identifying the tunnel to cut, and the information on the purport that cutting of 6o4 tunnel is instructed, and it transmits to the automatic setting equipment 11 of a cutting place (S338), On the other hand, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place also creates a tunnel disconnect indication signal, and transmits to the automatic setting equipment 11 of a cutting agency (S339). The information for identifying the tunnel to cut here is with the tunnel external address of a connecting agency, a tunnel internal address and an automatic setting device identifier, the tunnel external address of a connection destination, a tunnel internal address and an automatic setting device identifier, and a tunnel name, for example.

[0170]

If a tunnel disconnect indication signal is received from the automatic setting equipment 11 of a cutting place, it will be judged whether the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency can cut a tunnel using the memorized information (S340). It is judged that cutting of 6o4 tunnel is possible for judgment of the propriety of this tunnel setting out when it is the existence of the applicable tunnel information on an offer tunnel table and there is these information, and when it is missing among these information whether it is either, cutting of 6o4 tunnel is judged to be impossible. When it is judged as a result of judgment that it is impossible, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency ends this processing which cuts 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is possible, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency creates a decision result notification signal, and transmits to the automatic setting equipment 11 of a cutting place (S341).

[0171]

On the other hand, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place, If this decision result notification signal is received from the automatic setting equipment 11 of a cutting agency, it will be judged whether the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place can cut 6o4 tunnel using the memorized information (S342). When it is judged as a result of judgment that it is impossible, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place ends this processing which cuts TO 6o4 NNERU automatically.

On the other hand, when it is judged as a result of judgment that it is possible, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place creates a decision result notification signal, and transmits to the automatic setting equipment 11 of a cutting agency (S343).
[0172]
If the decision result notification signal which accommodates the decision result of the purport that it was judged from the automatic setting equipment 11 of another side that cutting of 6o4 tunnel was possible is received, the tunnel cutout 65 in a cutting agency and the automatic setting equipment 11 of a cutting place will perform processing which eliminates a connection, respectively (S344). If a connection is eliminated, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting agency and the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place will perform cutting of 6o4 tunnel, respectively (S345, S346). Delete the record corresponding to the 6o4 tunnel cut from the setting-out tunnel-pipes Osamu information table 101, and cutting of 6o4 tunnel. It is carried out by deleting the security policy and security association corresponding to the 6o4 tunnel cut from SPD and SAD, respectively.
[0173]
Thus, since 6o4 tunnel is cut after performing mutual recognition, unjust cutting can be avoided, the information corresponding to the 6o4 tunnel which also cuts the automatic setting equipment 11 of the connection destination of a tunnel can be deleted, and resources, such as the control part 52 and the storage part 53, can be saved.

CONTINUE

Due to excessive amounts of data, whole translation was NOT completed.
For subsequent translation(s), please click on the above "CONTINUE" button.
When continued, the current translation will be overwritten with the new translation.

[Translation done.]

Continued translation.

[0174]
Although the automatic setting equipment 11 was embedded previously and the creation information of the IPv6 address made it the own automatic setting device identifier in the above-mentioned embodiment at the time of shipment, Any character string which serves as a meaning

at the time of shipment, for example, the serial number of a product, etc., may be embedded, and in initial processing, by using any character string which serves as this meaning, IPv6 address creation information may be constituted so that it may acquire from the information server 21.
[0175]
Fig.27 is a figure showing the composition of the inside IP address creation information table of a tunnel in the information server in the case of acquiring IPv6 creation information from an information server. Fig.28 is some sequence diagrams showing operation of the initial processing of the automatic setting equipment applied when acquiring IPv6 creation information from an information server. Fig.29 is a flow chart which shows operation of an information server in a part of initial processing of the automatic setting equipment applied when acquiring IPv6 creation information from an information server.
[0176]
In Fig.27, the inside IP address creation information table of a tunnel matches with the automatic setting device identifier of the automatic setting equipment 11 the inside IP address creation information of a tunnel assigned according to the demand from the automatic setting equipment 11, and registers it. The inside IP address creation information table 106 of a tunnel, for example, the management number field 161 which registers the management number which manages each record as shown in Fig.27 and the automatic setting device identifier field 162 which registers the automatic setting device identifier of the automatic setting equipment 11 -- and, It has the inside IP address creation information field 163 of a tunnel which registers the inside IP address creation information of a tunnel assigned to the automatic setting equipment 11 concerned, and is constituted, and a record is created every automatic setting equipment 11 which had inside IP address creation information of a tunnel assigned.
[0177]
Processing shown in Fig.28 between the processing S64 and the processing S65 which were described using the Fig.13 in the above-mentioned embodiment is performed.That is, in Fig.28, the tunnel set part 62 of the automatic setting equipment 11 creates the signal transmission (inside IP address creation information requirement signal of a tunnel) which accommodates the information on the purport that an automatic setting device identifier and the inside IP address creation information of a tunnel are required, and transmits to the information server 21 (S171). The information server 21 will assign the inside IP address creation information of a tunnel to the automatic setting device identifier accommodated in this signal, if the inside IP address creation information requirement signal of a tunnel is received (S172).
[0178]
Next, it describes still in detail about the processing S172. In Fig.28, if the inside IP address creation information requirement signal of a tunnel is received, the information server 21, Based on the automatic setting device identifier accommodated in this signal, the tunnel external IP address corresponding to this automatic setting device identifier is searched from the inside IP address creation information table 106 of a tunnel, It is judged whether it is the inside IP address creation information of tunnel registered Mika no corresponding to this automatic setting device identifier (S81). This judgment whether to be registered or not, It is carried out by searching whether the record which the automatic setting device identifier and the inside IP address creation information of a tunnel which are accommodated in the inside IP address creation information requirement signal of a tunnel are matched, and is registered exists in the inside IP address creation information table 106 of a tunnel, When a record exists, it is judged that it is registered, and when a record does not exist, it is judged that it is not registered. When it is

judged as a result of judgment that it is not registered, The information server 21 chooses the network prefix of an unassigned IPv6 address out of the network prefix of the IPv6 address currently prepared previously, Give a new management number to the inside IP address creation information table 106 of a tunnel, and a new record is created, In the automatic setting device identifier field 162 and the inside IP address creation information field 163 of a tunnel in the created record, The automatic setting device identifier of the inside IP address creation information requirement signal of a tunnel and the selected network prefix of an IPv6 address are registered, respectively (S82). On the other hand, when it is judged as a result of judgment that it is registered, The information server 21 exists in the inside IP address creation information table 106 of a tunnel, The automatic setting device identifier and the inside IP address creation information of a tunnel which are accommodated in the inside IP address creation information requirement signal of a tunnel acquire the inside IP address creation information of a tunnel from the record matched and registered (S83).

[0179]

And the information server 21 creates the signal transmission (inside IP address creation information reply signal of a tunnel) which accommodated the network prefix of the assigned IPv6 address as inside IP address creation information of a tunnel, and replies it to the tunnel automatic setting equipment 11 (S173). Then, the tunnel set part 62 of the automatic setting equipment 11 will continue processing not more than processing S65, if the inside IP address registration reply signal of a set up tunnel is received from the information server 21.

[0180]

The information server 21 carries out batch management of the IPv6 address which is assigned by the automatic setting equipment 11 and used as an inside IP address of a tunnel in operating in this way, Since the IPv6 address is assigned according to the demand of the automatic setting equipment 11, By deleting timely about the IPv6 address which is not used for the long period of time with the registered IPv6 address from the table 106 continuing, When the automatic setting equipment 11 is not canceled or it is no longer used, IPv6 addresses can be collected and an IPv6 address can be efficiently used about.

[0181]

And although it is not confirming whether the connection from the automatic setting equipment 11 of a connecting agency is proper in the automatic setting equipment 11 of a connection destination in the case of tunnel construction processing, it may constitute from an above-mentioned embodiment so that it may check. moreover -- setting to the automatic setting equipment 11 of a cutting place in an above-mentioned embodiment in the case of tunnel deletion -- the connection from the automatic setting equipment 11 of a cutting agency -- although it is not confirming whether it is proper, it may constitute so that it may check.

[0182]

Fig.30 is some sequence diagrams showing operation of tunnel construction processing of the automatic setting equipment applied when checking a tunnel external IP address. Fig.31 is some sequence diagrams showing operation of the tunnel deletion of the automatic setting equipment applied when checking a tunnel external IP address.

[0183]

Processing shown in Fig.30 between the processing S108 described using the Fig.14 in the above-mentioned embodiment and the processing S109 of Fig.15 is performed.Namely, the tunnel set part [in / on Fig.30 and / the automatic setting equipment 11 of a connection destination] 62, The automatic setting device identifier in the automatic setting equipment 11 of

the connection origin accommodated in the automatic setting device identifier notification signal received from the automatic setting equipment 11 of the connecting agency in the processing S108, And the signal transmission (connecting agency tunnel external IP address requirement signal) which accommodated the information on the purport that the tunnel external IP address in the automatic setting equipment 11 of a connecting agency is required is created, and it transmits to the information server 21 (S161). The information server 21 will search the tunnel external IP address corresponding to this automatic setting device identifier from 102 from an offer tunnel setting information table based on the automatic setting device identifier accommodated in this signal, if a connecting agency tunnel external IP address requirement signal is received (S162). And the information server 21 creates the signal transmission (connecting agency tunnel external IP address reply signal) which accommodated the searched tunnel external IP address, and replies it to the automatic setting equipment 11 of a connection destination (S163). If a connecting agency tunnel external IP address reply signal is received from the information server 21, it will be judged whether the tunnel set part 62 in the automatic setting equipment 11 of a connection destination has a genuine connection from the automatic setting equipment 11 of a connecting agency (S164). This judgment whether to be genuine or not is made by comparing the IP address of the automatic setting equipment 11 of the connection origin which has established the connection with the connecting agency tunnel external IP address accommodated in the connecting agency tunnel external IP address reply signal acquired from the information server 21, When both IP addresses correspond, it is judged that it is genuine, and when both IP addresses are inharmonious, it is judged that it is not genuine. When it is judged as a result of judgment that it is not genuine, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is genuine, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination continues processing not more than processing S109.

[0184]

And processing shown in Fig.31 between the processing S308 described using the Fig.22 in the above-mentioned embodiment and the processing S309 of Fig.23 is performed.Namely, the tunnel cutout [in / on Fig.31 and / the automatic setting equipment 11 of a cutting place] 65, The automatic setting device identifier in the automatic setting equipment 11 of the cutting origin accommodated in the automatic setting device identifier notification signal received from the automatic setting equipment 11 of the cutting agency in the processing S308, And the signal transmission (cutting agency tunnel external IP address requirement signal) which accommodated the information on the purport that the tunnel external IP address in the automatic setting equipment 11 of a cutting agency is required is created, and it transmits to the information server 21 (S361). The information server 21 will search the tunnel external IP address corresponding to this automatic setting device identifier from 102 from an offer tunnel setting information table based on the automatic setting device identifier accommodated in this signal, if a cutting agency tunnel external IP address requirement signal is received (S362). And the information server 21 creates the signal transmission (cutting agency tunnel external IP address reply signal) which accommodated the searched tunnel external IP address, and replies it to the automatic setting equipment 11 of a cutting place (S363). If a cutting agency tunnel external IP address reply signal is received from the information server 21, it will be judged whether the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place has a genuine connection from the automatic setting equipment 11 of a cutting agency (S364). This judgment

whether to be genuine or not is made by comparing the IP address of the automatic setting equipment 11 of the cutting origin which has established the connection with the cutting agency tunnel external IP address accommodated in the cutting agency tunnel external IP address reply signal acquired from the information server 21, When both IP addresses correspond, it is judged that it is genuine, and when both IP addresses are inharmonious, it is judged that it is not genuine. When it is judged as a result of judgment that it is not genuine, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is genuine, the tunnel cutout 65 in the automatic setting equipment 11 of a cutting place continues processing not more than processing S309.

[0185]

In operating in this way, in tunnel construction processing, the automatic setting equipment 11 of a connection destination, With whether the automatic setting equipment 11 of a connecting agency is the automatic setting equipment 11 with a genuine tunnel external IP address, and it checking, Security can be raised and the load of the automatic setting equipment 11 can be lowered by not performing tunnel construction processing after it by performing immediately after the start of tunnel construction processing, when the automatic setting equipment of a connecting agency is unauthorized. In tunnel deletion, the automatic setting equipment 11 of a cutting place, With whether the automatic setting equipment 11 of a cutting agency is the automatic setting equipment 11 with a genuine tunnel external IP address, and it checking, Security can be raised and the load of the automatic setting equipment 11 can be lowered by not performing tunnel deletion after it by performing immediately after the start of tunnel deletion, when the automatic setting equipment of a cutting agency is unauthorized.

[0186]

Although it is not confirming whether the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connecting agency in the automatic setting equipment 11 of a connection destination on the occasion of tunnel construction processing is proper, it may constitute from an above-mentioned embodiment so that it may check. Although it is not confirming whether the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connection destination in the automatic setting equipment 11 of a connecting agency on the occasion of tunnel construction processing is proper, it may constitute from an above-mentioned embodiment so that it may check.

[0187]

Fig.32 is a figure showing the composition of the inside IP address table of a set up tunnel in the information server which starts when checking the inside IP address of a tunnel. Fig.33 is some sequence diagrams showing operation of the initial processing of the automatic setting equipment applied when checking the inside IP address of a tunnel. Fig.34 and Fig.35 are some sequence diagrams showing operation of tunnel construction processing of the automatic setting equipment applied when checking a tunnel external IP address.

[0188]

In Fig.32, the inside IP address table of a set up tunnel matches with an automatic setting device identifier inside IP address ** of a tunnel set as the LAN side interface part of the automatic setting equipment 11 according to the demand of the automatic setting equipment 11, and registers it. Inside IP address table 107 of a set up tunnel, for example, the management number field 171 which registers the management number which manages each record as shown in Fig.32 and the automatic setting device identifier field 172 which registers the automatic setting

device identifier of the automatic setting equipment 11 -- and, Have the inside IP address field 173 of a set up tunnel which registers the inside IP address of a tunnel set as the LAN side interface part of the automatic setting equipment 11 concerned, and it is constituted, A record is created in the inside IP address of a tunnel every automatic setting equipment 11 set to the LAN side interface.

[0189]

Processing shown in Fig.33 between the processing S66 and the processing S67 which were described using the Fig.13 in the above-mentioned embodiment is performed.Namely, in Fig.33 the tunnel set part 62 of the automatic setting equipment 11, An automatic setting device identifier, The signal transmission (inside IP address registration request signal of a set up tunnel) which accommodates the information on the purport that registration of the inside IP address of a set up tunnel (tunnel internal address set as the LAN side interface) and the inside IP address of a set up tunnel is required is created. It transmits to the information server 21 (S91). If the inside IP address registration request signal of a set up tunnel is received, the information server 21, Give a new management number to inside IP address table 107 of a set up tunnel, and a new record is created, To the automatic setting device identifier field 172 and the inside IP address field 173 of a set up tunnel in the created record, The inside IP address of a tunnel accommodated in the automatic setting device identifier and the inside IP address registration request signal of a set up tunnel which are accommodated in the inside IP address registration request signal of a set up tunnel is registered, respectively (S92). And the information server 21 creates the signal transmission (inside IP address registration reply signal of a set up tunnel) which accommodated everybody's information which registration of the inside IP address of a set up tunnel completed, and replies it to the tunnel automatic setting equipment 11 (S93). Then, the tunnel set part 62 of the automatic setting equipment 11 will continue processing not more than processing S67, if the inside IP address registration reply signal of a set up tunnel is received from the information server 21.

[0190]

And processing shown in Fig.34 between the processing S139 described using the Fig.17 in the above-mentioned embodiment and the processing S140 of Fig.18 is performed.Namely, the tunnel set part [in / on Fig.34 and / the automatic setting equipment 11 of a connecting agency] 62, If a tunnel construction indication signal is received from the automatic setting equipment 11 of a connection destination in the processing S139, The signal transmission (inside IP address requirement signal of a set up connection destination tunnel) which accommodated the information of everybody who demands the inside IP address of a tunnel in the automatic setting equipment 11 of a connection destination as the automatic setting identifier in the automatic setting equipment 11 of a connection destination is created, and it transmits to the information server 21 (S171).

[0191]

When this inside IP address requirement signal of a set up connection destination tunnel is received, the information server 21, Based on the automatic setting device identifier of the automatic setting equipment 11 of a connection destination accommodated in this received inside IP address requirement signal of a set up connection destination tunnel, inside IP address table 107 of a set up tunnel is referred to, The inside IP address of a set up tunnel corresponding to the automatic setting device identifier of the automatic setting equipment 11 of this connection destination is searched (S172). The information server 21 creates the signal transmission (inside IP address reply signal of a set up connection destination tunnel) which accommodates the

searched inside IP address of a set up connection destination tunnel, and replies it to the automatic setting equipment 11 of a connecting agency (S173). If the inside IP address reply signal of a set up connection destination tunnel is received, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, By comparing the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connection destination by the processing S139 with the inside IP address of a set up connection destination tunnel accommodated in the inside IP address reply signal of a set up connection destination tunnel acquired from this information server 21, It is judged whether the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connection destination is genuine (S174). It is judged that this judgment is genuine when the inside IP address of a tunnel and the inside IP address of a set up connection destination tunnel which were transmitted from the automatic setting equipment 11 of the connection destination correspond, When the inside IP address of a tunnel and the inside IP address of a set up connection destination tunnel which were transmitted from the automatic setting equipment 11 of the connection destination are inharmonious, it is judged that it is not genuine. When it is judged as a result of judgment that it is not genuine, The tunnel set part 62 in the automatic setting equipment 11 of a connecting agency creates the signal transmission (decision result notification signal) which accommodates a decision result, transmits to the automatic setting equipment 11 of a connection destination (S149), and ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is genuine, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency continues processing not more than processing S140.

[0192]

Processing shown in Fig.35 between the processing S141 and the processing S142 which were described using the Fig.18 in the above-mentioned embodiment is performed.Namely, the tunnel set part [in / on Fig.35 and / the automatic setting equipment 11 of a connection destination] 62, If a tunnel construction indication signal is received from the automatic setting equipment 11 of a connecting agency in the processing S138, The signal transmission (inside IP address requirement signal of a set up connection former tunnel) which accommodated the information of everybody who demands the inside IP address of a tunnel in the automatic setting equipment 11 of a connecting agency as the automatic setting device identifier in the automatic setting equipment 11 of a connecting agency is created, and it transmits to the information server 21 (S181).

[0193]

When self of this inside IP address requirement signal of a set up connection former tunnel is carried out, the information server 21, Based on the automatic setting device identifier of the automatic setting equipment 11 of the connection origin accommodated in this received inside IP address requirement signal of a set up connection former tunnel, inside IP address table 107 of a set up tunnel is referred to, The inside IP address of a set up tunnel corresponding to the automatic setting device identifier of the automatic setting equipment 11 of this connection origin is searched (S182). The information server 21 creates the signal transmission (inside IP address reply signal of a set up connection former tunnel) which accommodates the searched inside IP address of a set up connection former tunnel, and replies it to the automatic setting equipment 11 of a connection destination (S183). If the inside IP address reply signal of a set up connection former tunnel is received, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination, By comparing the inside IP address of a tunnel transmitted from the

automatic setting equipment 11 of the connecting agency by the processing S139 with the inside IP address of a set up connection former tunnel accommodated in the inside IP address reply signal of a set up connection former tunnel acquired from this information server 21, It is judged whether the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connecting agency is genuine (S184). It is judged that this judgment is genuine when the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connecting agency and the inside IP address of a set up connection former tunnel correspond, When the inside IP address of a tunnel transmitted from the automatic setting equipment 11 of the connecting agency and the inside IP address of a set up connection former tunnel are inharmonious, it is judged that it is not genuine. When it is judged as a result of judgment that it is not genuine, The tunnel set part 62 in the automatic setting equipment 11 of a connection destination creates the signal transmission (decision result notification signal) which accommodates a decision result, transmits to the automatic setting equipment 11 of a connecting agency (S149), and ends this processing which sets up 6o4 tunnel automatically. On the other hand, when it is judged as a result of judgment that it is genuine, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination continues processing not more than processing S142.

[0194]

Security can be raised with whether in operating in this way, it is the automatic setting equipment 11 in which the automatic setting equipment 11 of a connecting agency has an inside IP address of a tunnel with the genuine automatic setting equipment 11 of a connection destination in tunnel construction processing, and it checking. In tunnel construction processing, the automatic setting equipment 11 of a connection destination can raise security with whether the automatic setting equipment 11 of a connecting agency is the automatic setting equipment 11 with a genuine inside IP address of a tunnel, and it checking.

[0195]

In an above-mentioned embodiment, although two or more 6o4 tunnels were simultaneously set to two or more of other automatic setting equipment 11, respectively by generating two or more logical interfaces to the physical WAN side [one piece] interface part 55, the automatic setting equipment 11, By having two or more physical WAN side interface parts, it may constitute so that two or more 6o4 tunnels may be simultaneously set to two or more of other automatic setting equipment 11, respectively.

[0196]

Fig.36 is a block diagram showing the composition of the network containing tunnel automatic setting equipment provided with two or more WAN side interface parts. Fig.37 is a figure showing the composition of the setting-out tunnel-pipes Osamu information table concerning tunnel automatic setting equipment provided with two or more WAN side interface parts. Fig.38 is a figure showing the composition of the offer tunnel setting information table of an information server in case tunnel automatic setting equipment is provided with two or more WAN side INTAFE parts.

[0197]

In Fig.36, the automatic setting equipment 11' is provided with the control part 52', the storage part 53' and the input part 54, and two or more WAN side interface part 55' (55 '-0, 55'-1, ..., 55' -n), and is constituted. [the LAN side interface part 51,] These LAN side interface part 51, the control part 52', the storage part 53' and the input part 54, and WAN side interface part 55', WAN side interface part 55' is plurality, and Each WAN side interface part 55 '-0, 55'-1, ..., The

WAN side interface device name which is an identifier for identifying 55'-n Each WAN side interface part 55 '-0, 55'-1, ..., It is given to 55'-n, respectively, To Fig.37. So that it may be shown. To the setting-out tunnel-pipes Osamu information storage part 73'. The setting-out tunnel-pipes Osamu information table 101 showing in Fig.3 the WAN side interface device name field 112 which registers the WAN side interface device name is further equipped with setting-out tunnel-pipes Osamu information table 101' memorized, and it is constituted, It removes using this WAN side interface device name, when the tunnel set part 62' of the control part 52' sets up 6o4 tunnel automatically, Since it is the same as that of the LAN side interface part 51 mentioned above, the control part 52, the storage part 53, the input part 54, and the WAN side interface part 55 respectively, the description is omitted.

[0198]

And in order to manage individually the tunnel external IP address given to each WAN side interface part 55'-0 and 55 '-1, ..., 55'-n, respectively, the information server 21, Offer tunnel setup information is matched with the group of the WAN side interface device name and an automatic setting device identifier, and an offer tunnel setting information storage part memorizes. For example, offer tunnel setting information table 102' memorized by the offer tunnel setting information storage part as shown in Fig.38, Prepare for the offer tunnel setting information table 102 showing in Fig.4 the WAN side interface device name field 122 which registers the WAN side interface device name further, and it is constituted, A record is created for every group of the WAN side interface device name and an automatic setting device identifier.

[0199]

And in processing of the processing S64, the processing S65, the processing S108, the processing S109, the processing S110, and the processing S111, it replaces with an automatic setting device identifier, and the group of an automatic setting device identifier and the WAN side interface device name is used. When the automatic setting equipment 11 of the connection destination is provided with two or more WAN side interface parts 55, here, Although the tunnel set part 62' in the automatic setting equipment 11' of a connecting agency will acquire two or more tunnel external IP addresses from the information server 21 by performing the processing S102 thru/or processing S104, The tunnel set part 62' in the automatic setting equipment 11 of a connecting agency should just use one tunnel external IP address arbitrarily from two or more tunnel external IP addresses.

[0200]

Since the 6o4 tunnel which should be cut by receiving a tunnel disconnect indication signal in the case of tunnel cut treating is specified, 6o4 tunnel can be cut by performing the processing S303 thru/or the processing S343 mentioned above even when multidata input of the 6o4 tunnel was carried out.

[0201]

And although the automatic setting equipment 11 and 11' described about the case where it is included in a router device, in the above-mentioned embodiment, You may also include in the gateway unit further provided with the function to perform protocol conversion for example, in addition to the routing function which performs routing of a communication packet instead of what is limited to this.

[0202]

Constituted the automatic setting equipment 11 and 11' from an above-mentioned embodiment so that the location information of the information server 21, the registration server 22, the

authentication server 23, and NTP server 24 might be memorized to the storage part 53 by an IP address, but. The database which described the correspondency of a host name and an IP address is managed, According to the demand from a client, the IP address is searched from a host name, The network 1 is made to equip Fig.1 with the DNS (Domain Name System) server 25 which replies search results to a client further, as a dashed line shows. The automatic setting equipment 11 and 11' may be constituted so that at least one location information may be memorized to the storage part 53 by a host name among the information server 21, the registration server 22, the authentication server 23, and NTP server 24. By constituting in this way, even when the IP address of the information server 21, the registration server 22, the authentication server 23, or NTP server 24 is changed, the automatic setting equipment 11 and 11' can be connected to the information server 21 etc. Since especially location information, such as the information server 21, is memorized by the manufacturing stage etc. at the storage part 53, even when IP addresses, such as the information server 21, are changed after the automatic setting equipment 11 and 11' were shipped, the automatic setting equipment 11 and 11' can be connected to the information server 21 etc.

[0203]

Two 6o4 tunnels with the 6o4 tunnel whose connecting agency and connection destination are the same and apply IPsec in an above-mentioned embodiment, and the 6o4 tunnel which does not apply IPsec are set up, By constituting so that either may be chosen from among two 6o4 tunnels according to the communicative contents, Since IPsec can be used according to the communicative contents when encryption is required, when communicating, the amount of information processings of the control part 52 can be reduced, and the burden of the control part 52 can be eased.

[0204]

And the control part 52 and 52' may judge whether the obstacle has arisen to the 6o4 tunnel set up, and they may constitute it from an above-mentioned embodiment so that 6o4 tunnel may be deleted, also when the obstacle has arisen. Ping (Ping) is transmitted to the automatic setting equipment 11 of the setting-out place of 6o4 tunnel, and 11', and the existence of an obstacle judges that there is no obstacle, when it receives before timing out, and when it times out, it judges the received response to the ping concerned that there is an obstacle, for example. By constituting in this way, neglect of the 6o4 tunnel it became impossible to use according to an obstacle can be avoided, and the futility of resources, such as the control part 52, 52', the storage part 53, 53', can be lost. And when 6o4 tunnel is deleted, the tunnel cutout 66 may be constituted so that 6o4 tunnel may newly be automatically reset by making into a connection destination the automatic setting equipment 11 of another side in the 6o4 tunnel which deleted [use] the tunnel set part 62, and 11'. Since an obstacle is automatically removable by constituting in this way, the fault tolerance of the 6o4 tunnel [itself] can be improved, and 6o4 tunnel can be maintained in the usable state.

[0205]

In an above-mentioned embodiment, the automatic setting equipment 11 is an embodiment which forms IPv6overIPv4 tunnel among other automatic setting equipment 11 on ISP networks 3 of IPv4, and the network 4 of IPv4. Even when it shifts to the network of IPv6 when the network of IPv4 adopts IPv6 sequentially, and above-mentioned ISP networks 3 and the network 4 in an embodiment become IPv6, by same operation, The automatic setting equipment 11 of 1 can form IPv6overIPv6 tunnel among other automatic setting equipment 11 on ISP networks 3 and the network 4. Thus, by using the automatic setting equipment 11 concerning the present

invention, even when all the nodes of the network 1 come to operate by IPv6 manufacturing enterprises, The tunnel automatic setting equipment 11 can not only be manageable, but a secure (it is safe) communication path is securable by setting up a tunnel between the networks 2 of each IPv6.

[Brief Description of the Drawings]

[0206]

[Drawing 1]It is a figure showing the entire configuration of the network in an embodiment.

[Drawing 2]It is a block diagram showing the composition of the network containing tunnel automatic setting equipment.

[Drawing 3]It is a figure showing the composition of the setting-out tunnel-pipes Osamu information table in tunnel automatic setting equipment.

[Drawing 4]It is a figure showing the composition of the offer tunnel setting information table in an information server.

[Drawing 5]It is a figure showing the composition of the login certification information registration table in a registration server.

[Drawing 6]It is a figure showing the composition of the automatic setting equipment book humanity news registration table in a registration server.

[Drawing 7]It is a figure showing the composition of the repository in an authentication server.

[Drawing 8]It is a sequence diagram showing operation of public key certification acquisition processing.

[Drawing 9]It is a flow chart which shows the operation in the issue processing of the public key certification of automatic setting equipment.

[Drawing 10]It is a flow chart which shows the operation in the memory processing of the public key certification of automatic setting equipment.

[Drawing 11]It is a sequence diagram showing the operation in the update process to the public key certification of an authentication server.

[Drawing 12]It is a flow chart which shows the operation in the update process to the public key certification of an authentication server.

[Drawing 13]It is a sequence diagram showing operation of the initial processing of tunnel automatic setting processing.

[Drawing 14]It is a sequence diagram (the 1) showing operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 15]It is a sequence diagram (the 2) showing operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 16]It is a sequence diagram (the 3) showing operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 17]It is a sequence diagram (the 4) showing operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 18]It is a sequence diagram (the 5) showing operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 19]It is a flow chart which shows operation of the tunnel construction processing in tunnel automatic setting processing.

[Drawing 20]It is a sequence diagram showing the operation in the update process to the public key certification of automatic setting equipment.

[Drawing 21]It is a flow chart which shows operation of the usability judging process in the public key certification of automatic setting equipment.

[Drawing 22]It is a sequence diagram (the 1) showing operation of the tunnel deletion in tunnel automatic setting processing.
[Drawing 23]It is a sequence diagram (the 2) showing operation of the tunnel deletion in tunnel automatic setting processing.
[Drawing 24]It is a sequence diagram (the 3) showing operation of the tunnel deletion in tunnel automatic setting processing.
[Drawing 25]It is a sequence diagram (the 4) showing operation of the tunnel deletion in tunnel automatic setting processing.
[Drawing 26]It is a sequence diagram (the 5) showing operation of the tunnel deletion in tunnel automatic setting processing.
[Drawing 27]It is a figure showing the composition of the inside IP address creation information table of a tunnel in the information server in the case of acquiring IPv6 creation information from an information server.
[Drawing 28]They are some sequence diagrams showing operation of the initial processing of the automatic setting equipment applied when acquiring IPv6 creation information from an information server.
[Drawing 29]It is a flow chart which shows operation of an information server in a part of initial processing of the automatic setting equipment applied when acquiring IPv6 creation information from an information server.
[Drawing 30]When checking a tunnel external IP address, they are some sequence diagrams showing operation of tunnel construction processing of the automatic setting equipment to apply.
[Drawing 31]When checking a tunnel external IP address, they are some sequence diagrams showing operation of the tunnel deletion of the automatic setting equipment to apply.
[Drawing 32]When checking the inside IP address of a tunnel, it is a figure showing the composition of the inside IP address table of a set up tunnel in the starting information server.
[Drawing 33]When checking the inside IP address of a tunnel, they are some sequence diagrams showing operation of the initial processing of the automatic setting equipment to apply.
[Drawing 34]When checking a tunnel external IP address, they are some sequence diagrams showing operation of tunnel construction processing of the automatic setting equipment to apply.
[Drawing 35]When checking a tunnel external IP address, they are some sequence diagrams showing operation of the tunnel deletion of the automatic setting equipment to apply.
[Drawing 36]It is a block diagram showing the composition of the network containing tunnel automatic setting equipment provided with two or more WAN side interface parts.
[Drawing 37]It is a figure showing the composition of the setting-out tunnel-pipes Osamu information table concerning tunnel automatic setting equipment provided with two or more WAN side interface parts.
[Drawing 38]It is a figure showing the composition of the offer tunnel setting information table of an information server in case tunnel automatic setting equipment is provided with two or more WAN side INTAFE parts.
[Explanations of letters or numerals]
[0207]
1 Network
2 The network of IPv6
3 ISP networks of IPv4
4 The network of IPv4
5 IPv6overIPv4 tunnel

11 and 11' tunnel automatic setting equipment
21 Information server
22 Registration server
23 Authentication server
24 NTP server
25 DNS server
26 DHCP server
51 Local area network side interface part
52 and 52' control part
53 and 53' storage part
54 Input part
55 and 55' wide area network side interface part
62 and 62' tunnel set part
63 Inside IP address generation part of a connection destination tunnel
64 Public key certification Management Department
65 Tunnel cutout
66 Clock part
71 The information storage part for tunnel setting out
72 Security information storage part
73 and 73' setting-out tunnel-pipes Osamu information storage part
101 and 101' setting-out tunnel-pipes Osamu information table
102 and 102' offer tunnel setting information table
103 Login certification information registration table
104 Automatic setting equipment book humanity news registration table
105 Repository
106 Inside IP address creation information table of a tunnel
107 Inside IP address table of a set up tunnel

[Translation done.]

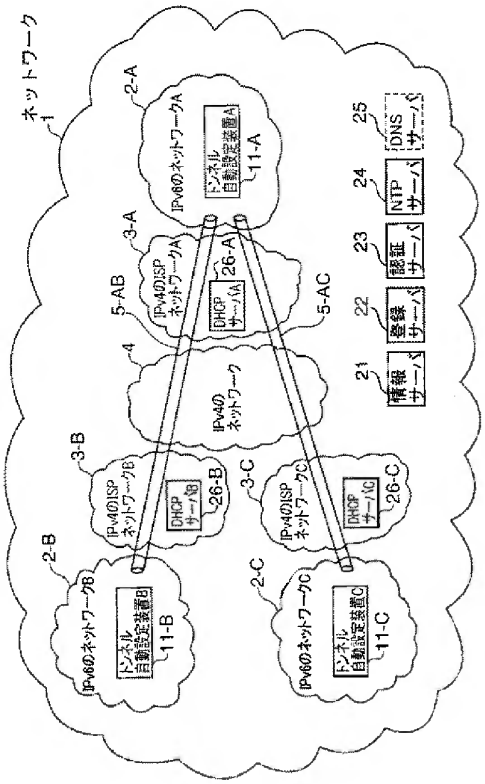
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

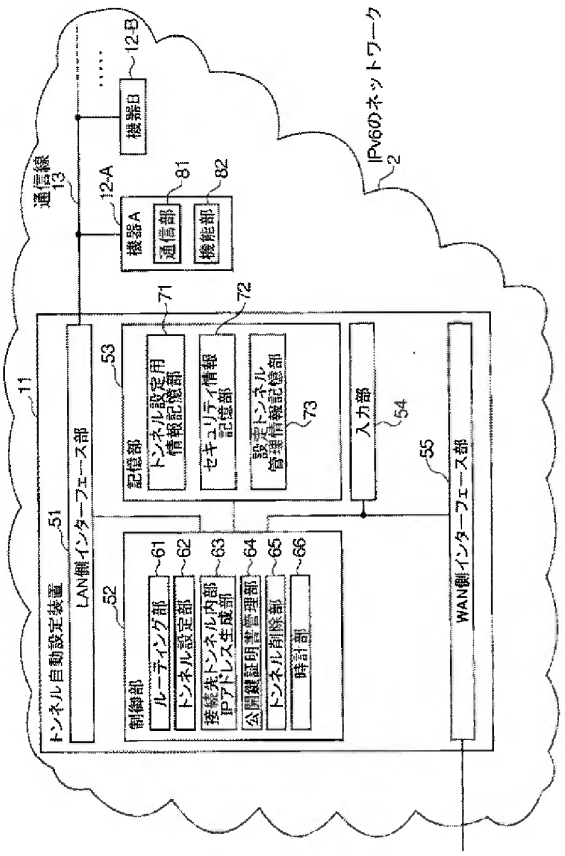
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

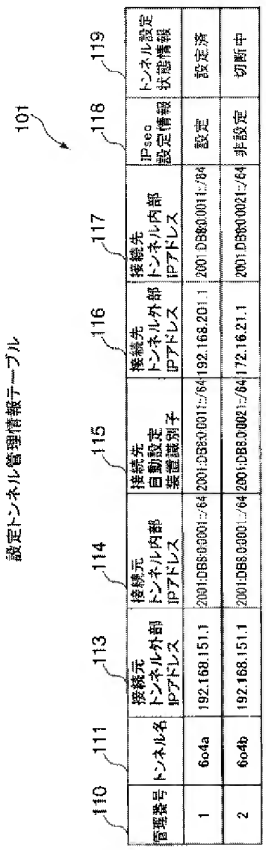
[Drawing 1]



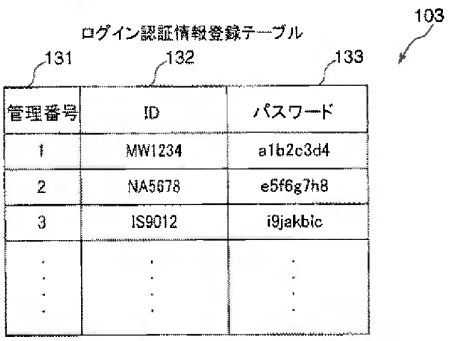
[Drawing 2]


IPv6のネットワーク
2
通信線
13
12-B
機器B
12-A
機器A
81
通信部
82
機能部
11
トンネル自動設定装置
LAN側インターフェース部
51
52
53
記憶部
71
トンネル設定用情報記憶部
72
セキュリティ情報記憶部
73
設定トンネル管理情報記憶部
入力部
54
55
WAN側インターフェース部
制御部
61
ルーティング部
62
トンネル設定部
63
接続先トンネル内部IPアドレス生成部
64
公開鍵証明書管理部
65
トンネル削除部
66
時計部

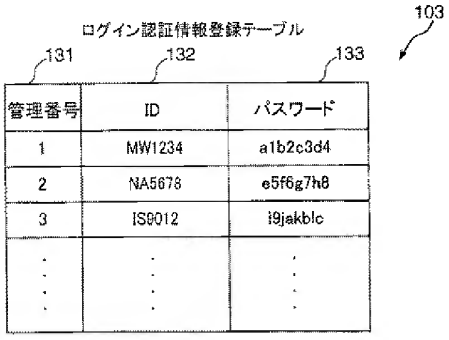
[Drawing 3]



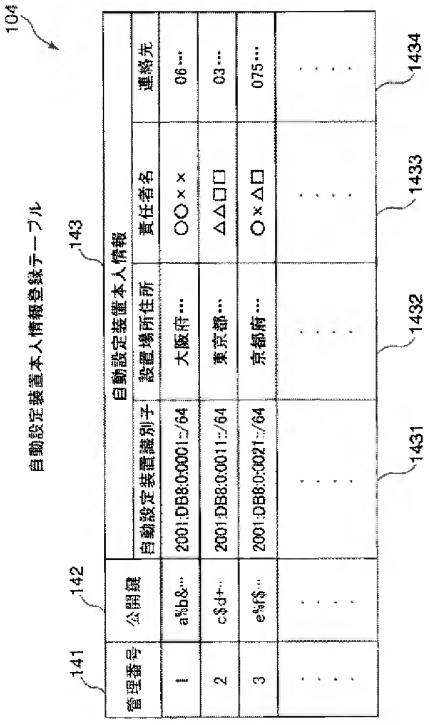
[Drawing 4]



[Drawing 5]



[Drawing 6]

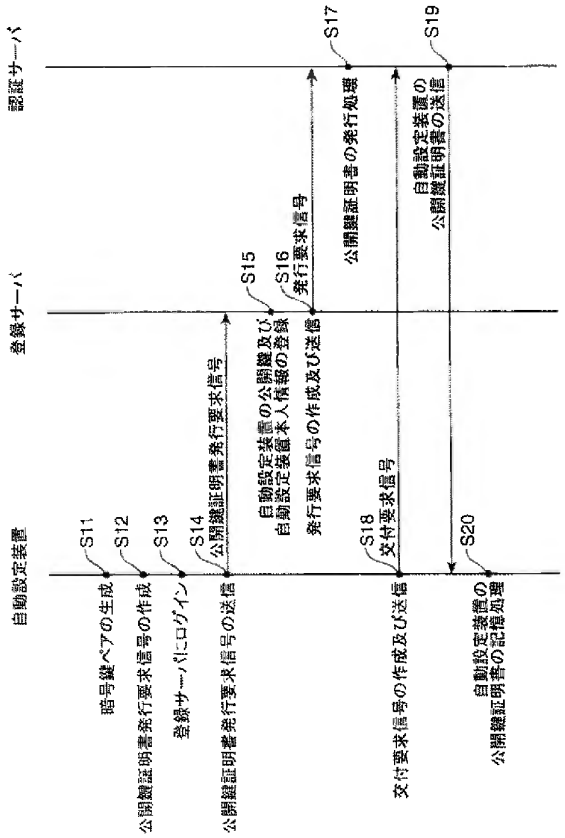


[Drawing 7]

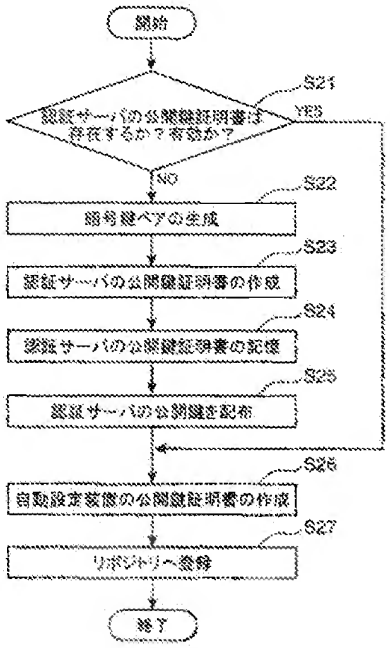
リポジトリ 105

151 管理番号	152 自動設定装置識別子	153 公開鍵証明書
1	2001:DB8:0:0001::/64	a%b&…
2	2001:DB8:0:0011::/64	c$d+…
3	2001:DB8:0:0021::/64	e%f$…
…	…	…

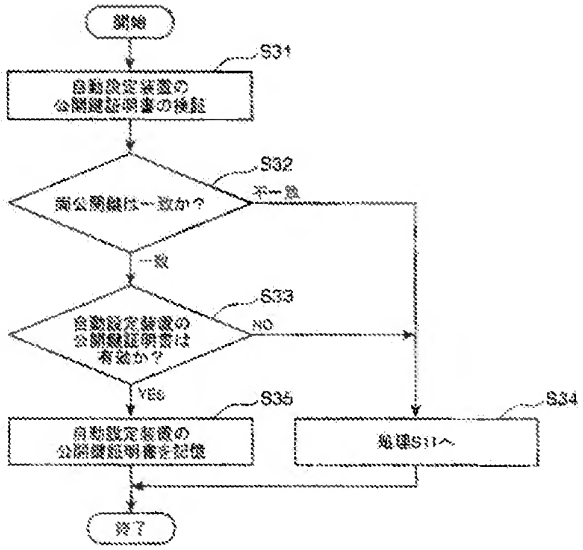
[Drawing 8]



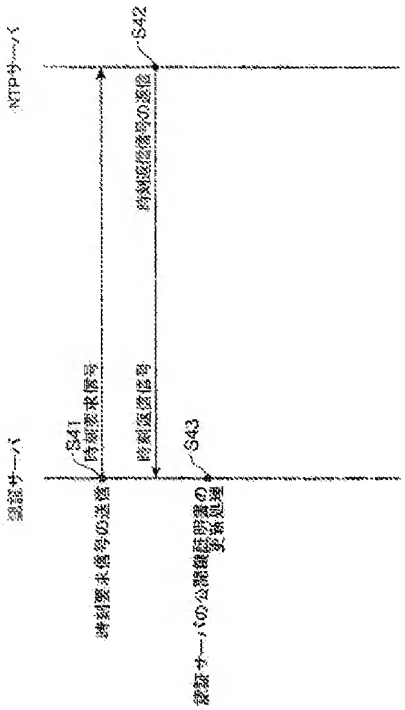
[Drawing 9]



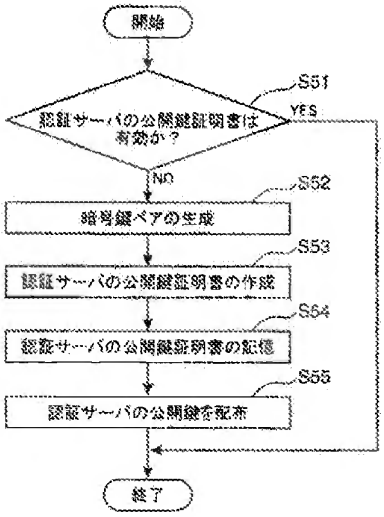
[Drawing 10]



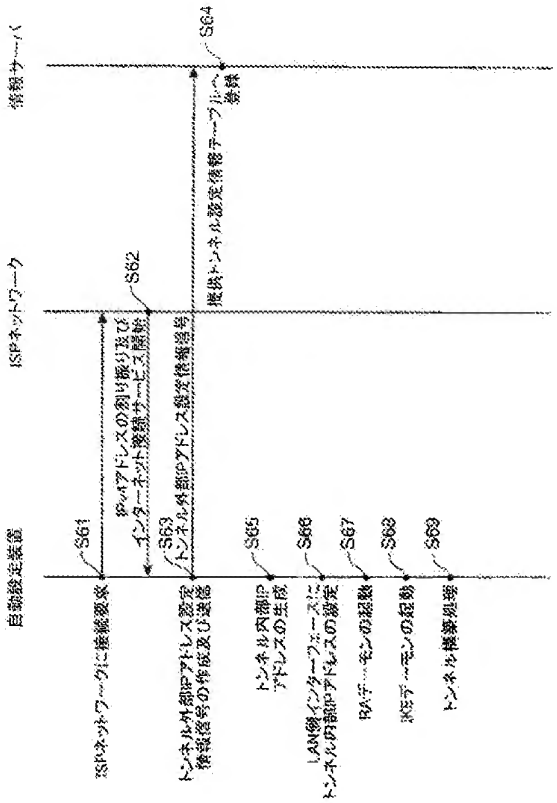
[Drawing 11]



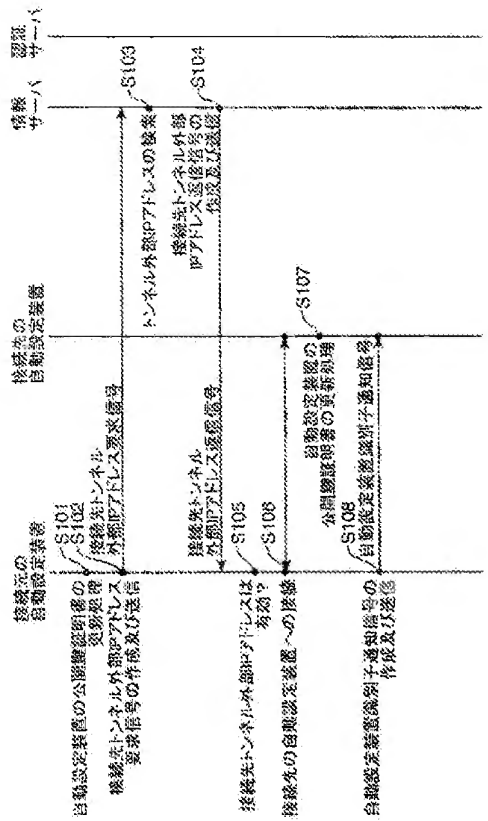
[Drawing 12]



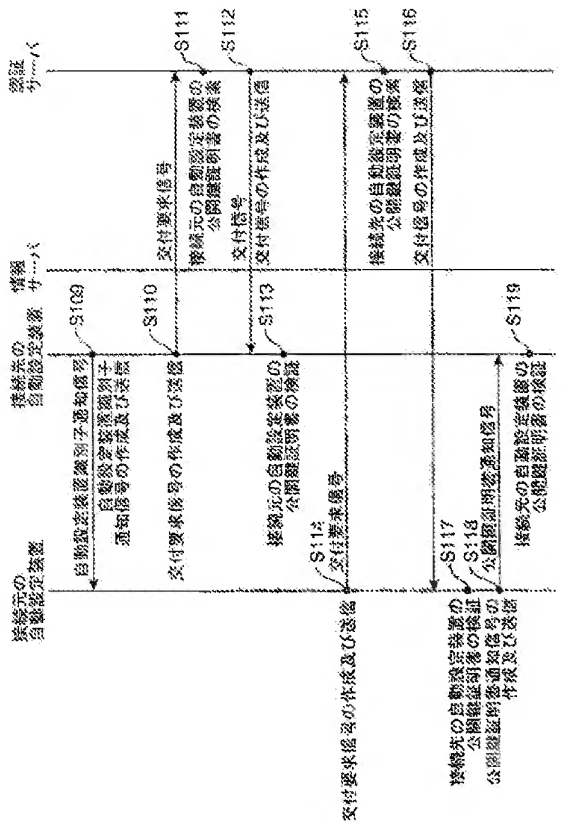
[Drawing 13]


自動設定装置
ISPネットワーク
接続サーバ
S61
S62
S63
S64
S65
S66
S67
S68
S69
ISPネットワークに接続要求
IPv4アドレスの割り振り及び
インターネット接続サービス開始
トンネル外部IPアドレス設定
情報信号の作成及び送信
接続トンネル設定情報テーブル
トンネル内部IP
アドレスの生成
LAN側インターフェースに
トンネル内部IPアドレスの設定
ルーティングの起動
設定データベースの起動
トンネル機能起動

[Drawing 14]


接続元の自動設定装置
接続先の自動設定装置
情報サーバ
認証サーバ
S101
S102
S103
S104
S105
S106
S107
S108
接続先トンネル外部IPアドレス要求信号
トンネル外部IPアドレスの登録
接続先トンネル外部IPアドレス応答信号
接続先トンネル外部IPアドレスは有効？
接続先の自動設定装置への接続
自動設定装置の公開鍵証明書の更新処理
自動設定装置識別子通知信号の作成及び送信

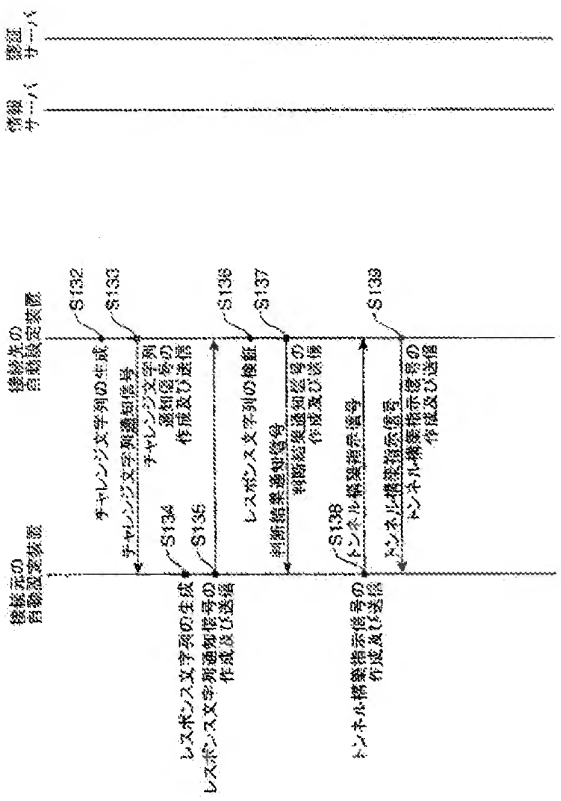
[Drawing 15]


接続元の自動設定装置
接続先の自動設定装置
情報サーバ
認証サーバ
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
S119
自動設定装置識別子通知信号
自動設定装置識別子通知信号の作成及び送信
交付要求信号
交付要求信号の作成及び送信
接続元の自動設定装置の公開鍵証明書の検証
交付要求信号の作成及び送信
接続元の自動設定装置の公開鍵証明書の検索
交付信号
交付信号の作成及び送信
接続先の自動設定装置の公開鍵証明書の検索
交付信号の作成及び送信
接続先の自動設定装置の公開鍵証明書の検証
接続先の自動設定装置の公開鍵証明書の検証
公開鍵証明書通知信号の作成及び送信

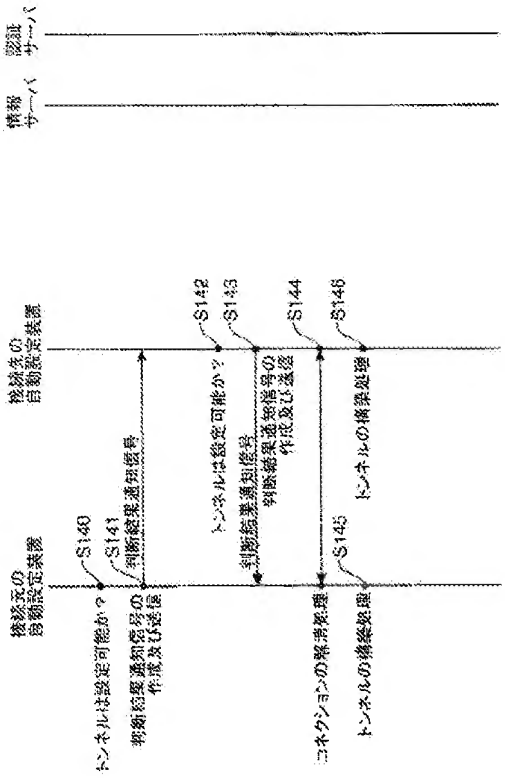
[Drawing 16]

[図24]

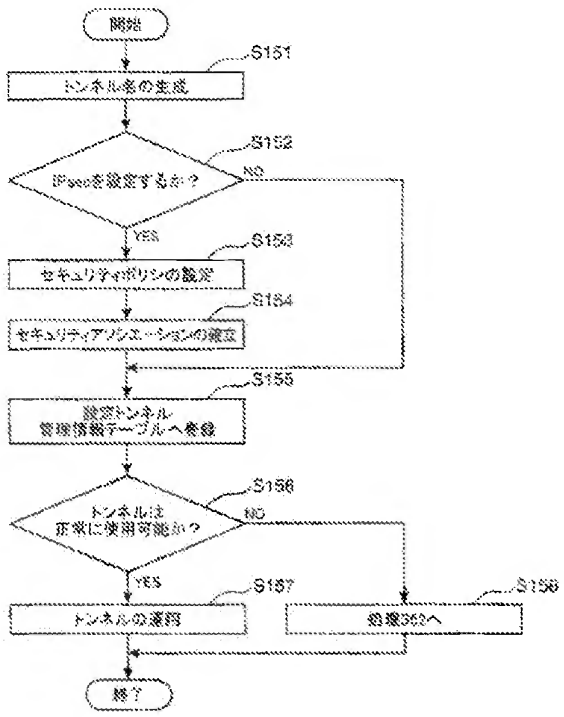
接続元の自動設定装置
接続先の自動設定装置
情報サーバ
認証サーバ
S120
S121
S122
S123
S124
S125
S126
S127
S128
S129
S130
S131


S132
S133
S134
S135
S136
S137
S138
S139
チャレンジ文字列の生成
チャレンジ文字列通知信号の作成及び送信
レスポンス文字列の生成
レスポンス文字列通知信号の作成及び送信
レスポンス文字列の検証
判断結果通知信号の作成及び送信
トンネル構築指示信号の作成及び送信
トンネル構築指示信号の作成及び送信

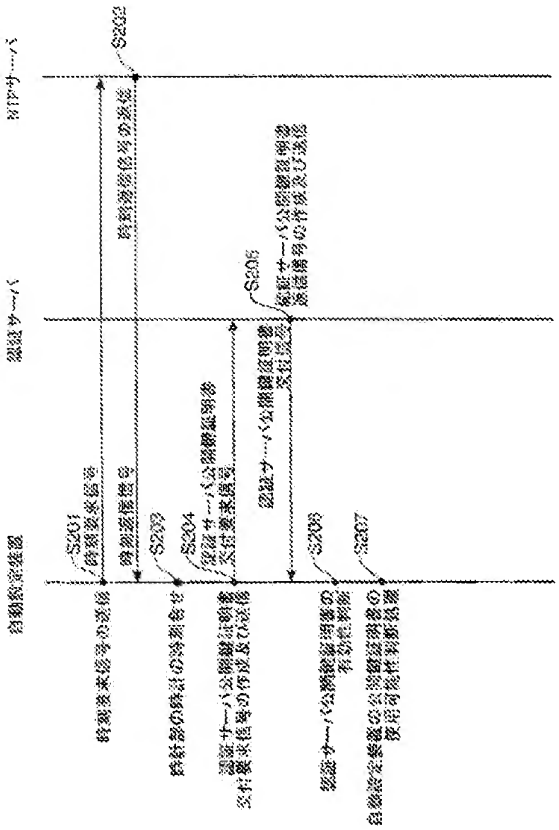
[Drawing 18]


認証サーバ
情報サーバ
接続先の自動設定装置
接続元の自動設定装置
S140
S141
S142
S143
S144
S145
S146
トンネルは設定可能か？
判断結果通知信号の作成及び送信
トンネルは設定可能か？
判断結果通知信号
判断結果通知信号の作成及び送信
コネクションの解消処理
トンネルの構築処理

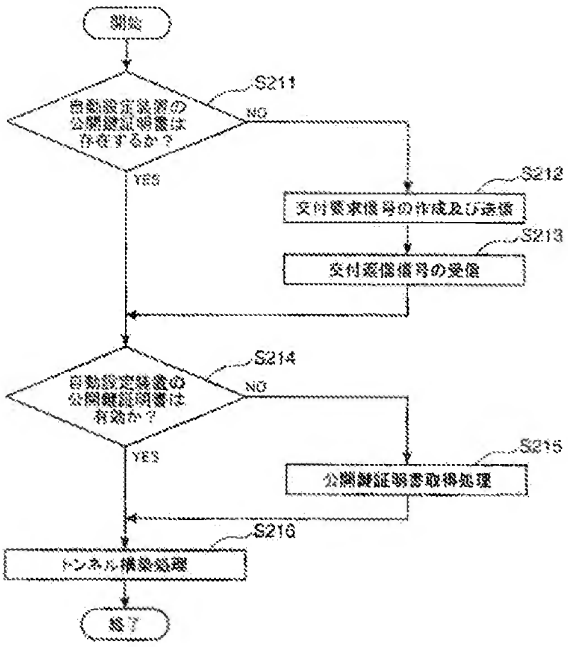
[Drawing 19]


開始
S151
トンネル表の生成
S152
IPsecを設定するか？
NO
YES
S153
セキュリティポリシの設定
S154
セキュリティアソシエーションの確立
S155
設定トンネル
管理情報テーブルへ登録
S156
トンネルは
正常に使用可能か？
NO
YES
S157
トンネルの運用
S158
終了

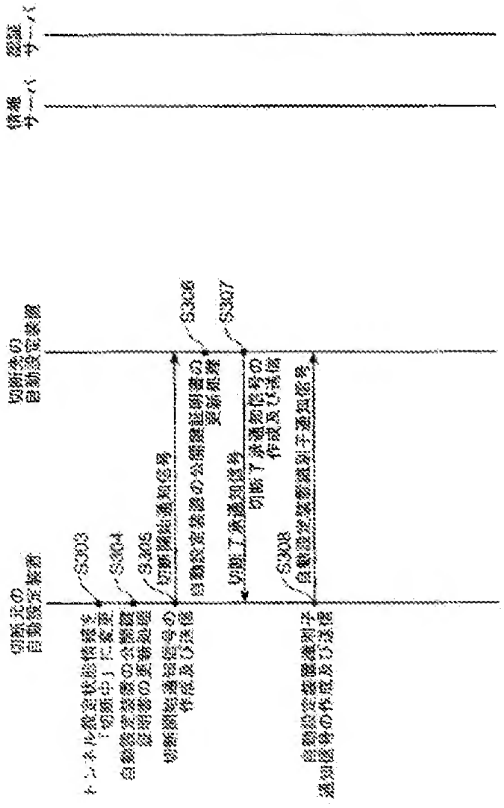
[Drawing 20]



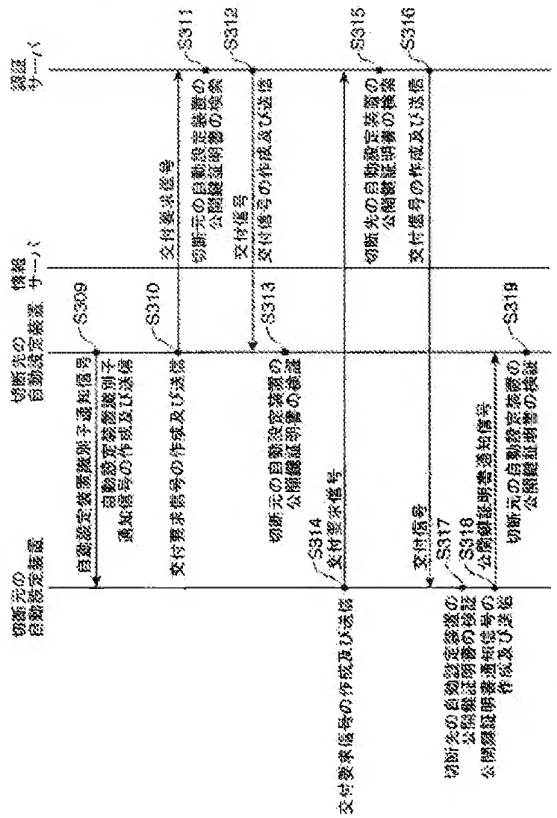
[Drawing 21]


S211
NO
YES
S212
S213
S214
NO
YES
S215
S216

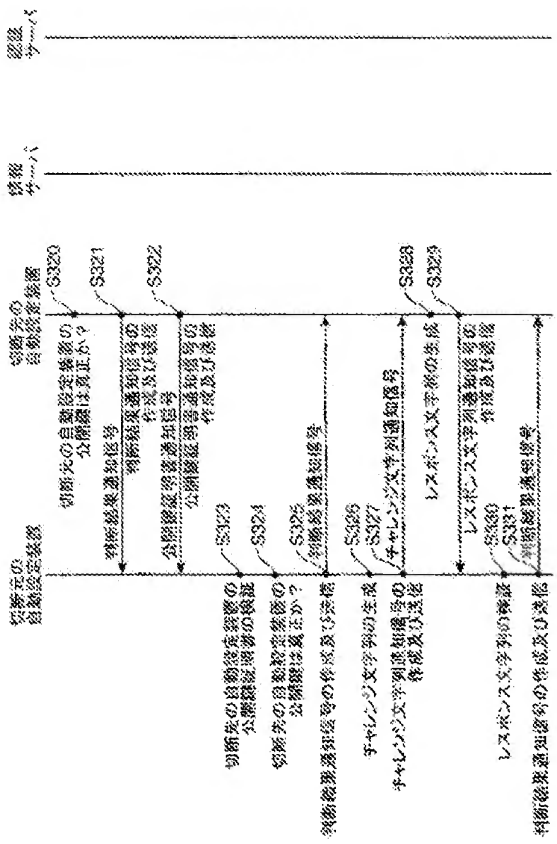
[Drawing 22]


S306
S307
S303
S304
S305
S308

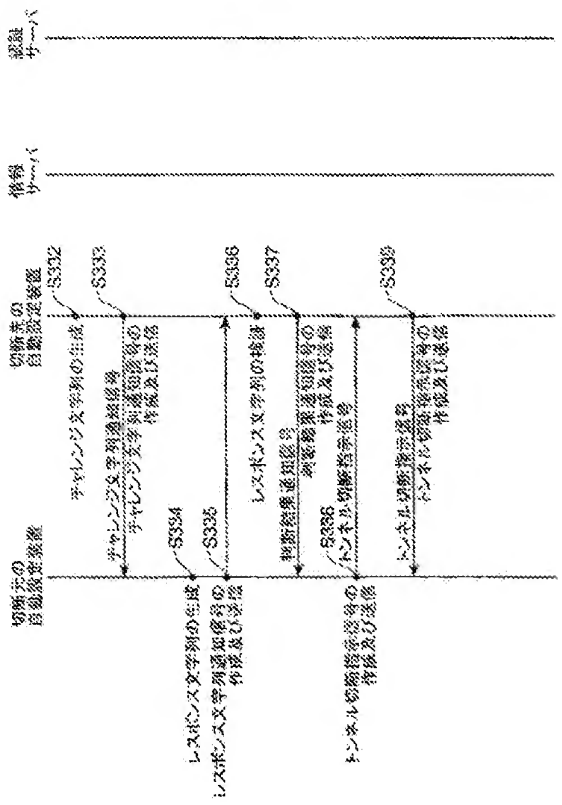
[Drawing 23]



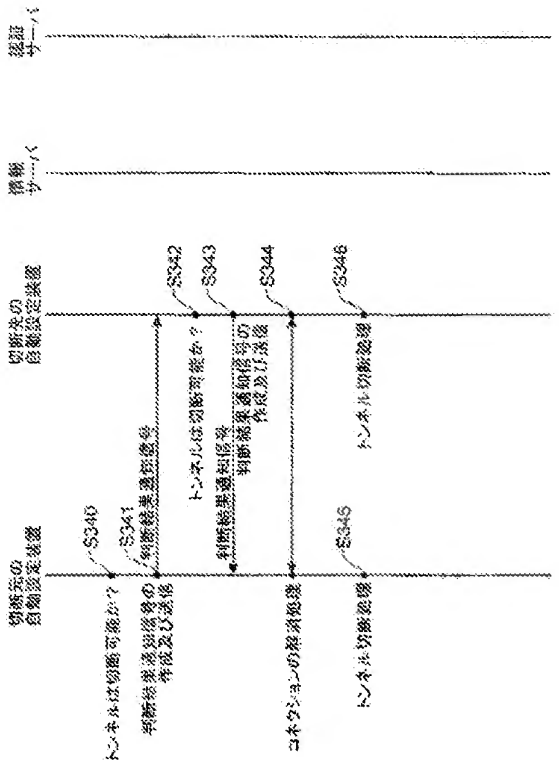
[Drawing 24]



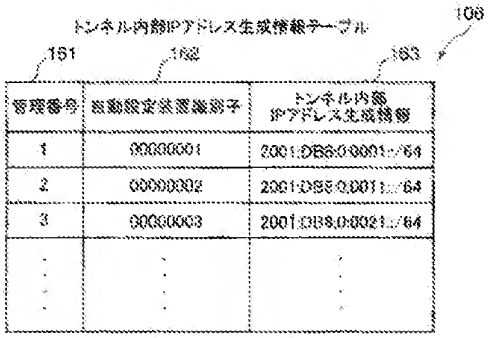
[Drawing 25]


認証サーバ
検疫サーバ
切断元の自動設定装置
切断先の自動設定装置
S332
S333
S334
S335
S336
S337
S338
S339
チャレンジング文字列の生成
チャレンジング文字列通知信号の作成及び送信
レスポンス文字列の生成
レスポンス文字列通知信号の作成及び送信
レスポンス文字列の検証
判断結果通知信号の作成及び送信
トンネル切断指示信号の作成及び送信
トンネル切断指示信号の作成及び送信

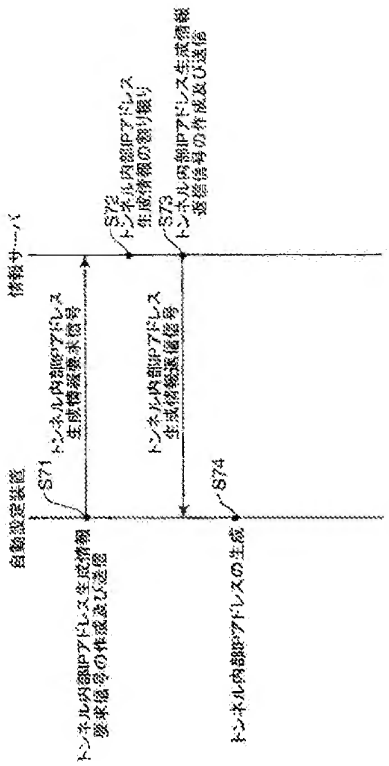
[Drawing 26]



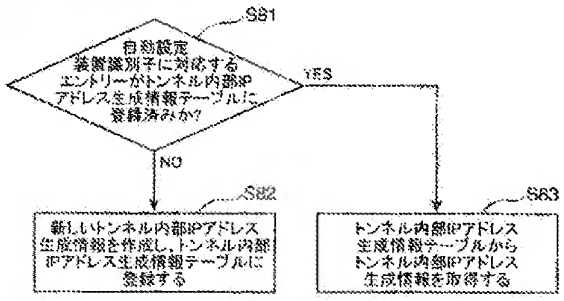
[Drawing 27]



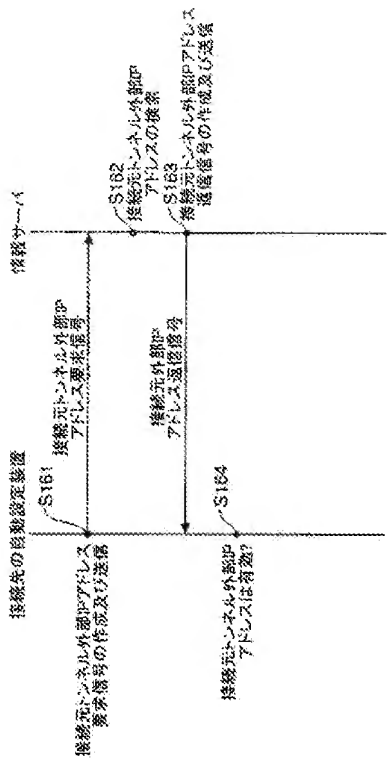
[Drawing 28]



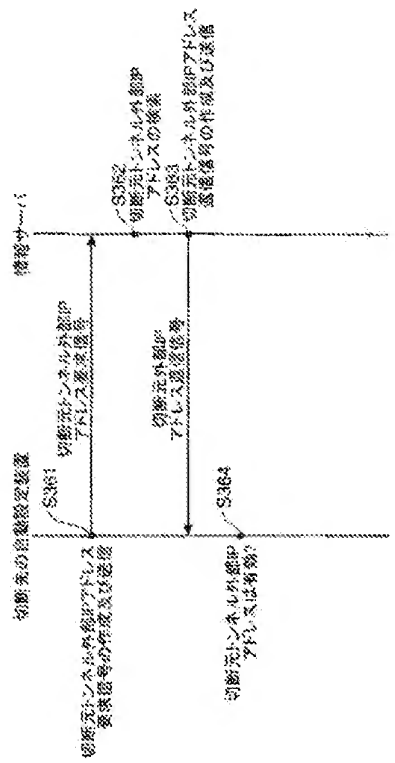
[Drawing 29]



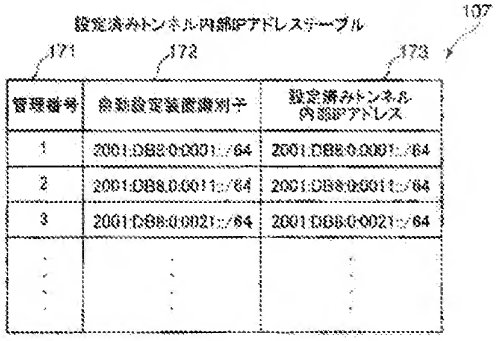
[Drawing 30]


接続先の自動設定装置
S161
接続元トンネル外部IPアドレス要求信号
接続元トンネル外部IPアドレス及び送信
S162
接続元トンネル外部IPアドレスの探索
S163
接続元外部IPアドレス通知信号
S164
接続元トンネル外部IPアドレスは有効?

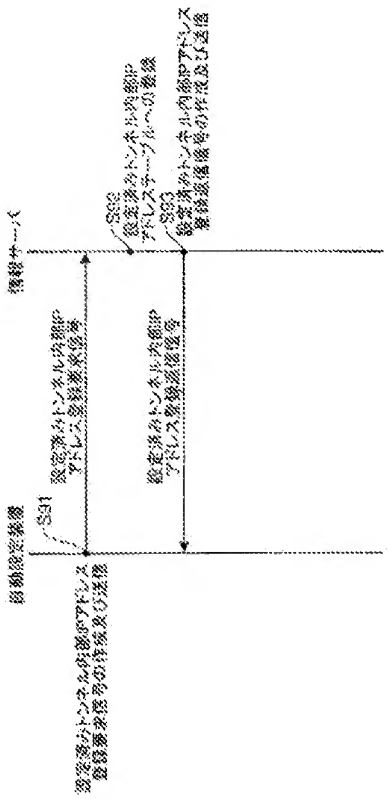
[Drawing 31]



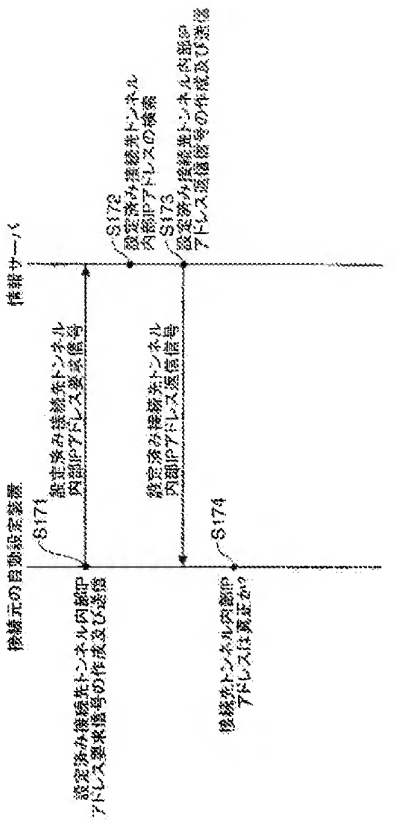
[Drawing 32]



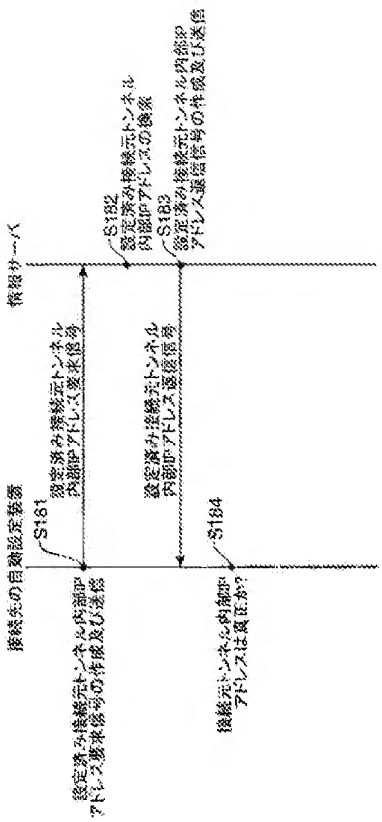
[Drawing 33]



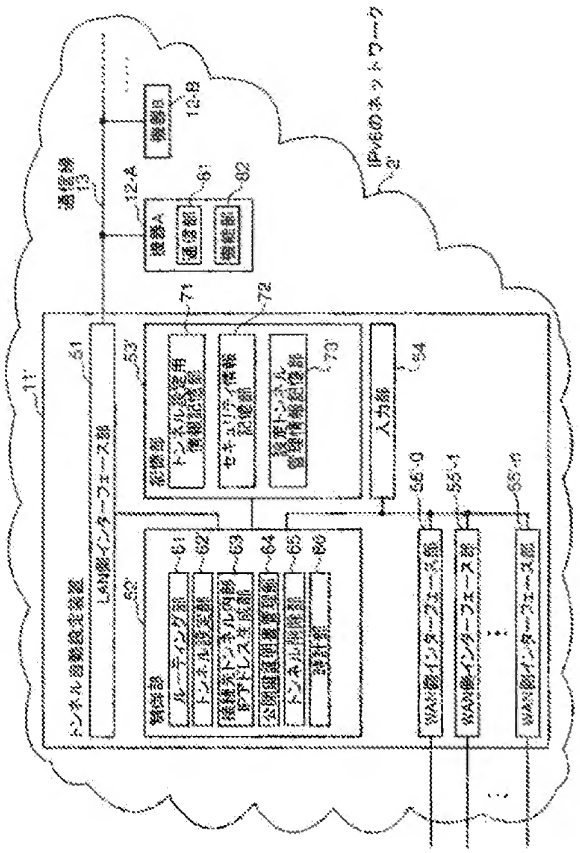
[Drawing 34]


接続元の自動設定装置
情報サーバ
S171
設定済み接続先トンネル
内部IPアドレス要求信号
S172
設定済み接続先トンネル
内部IPアドレスの検索
S173
設定済み接続先トンネル
内部IPアドレス返信信号
S174
設定済み接続先トンネル内部IP
アドレス要求信号の作成及び送信
接続先トンネル内部IP
アドレスは真正か？
設定済み接続先トンネル内部IP
アドレス返信信号の作成及び送信

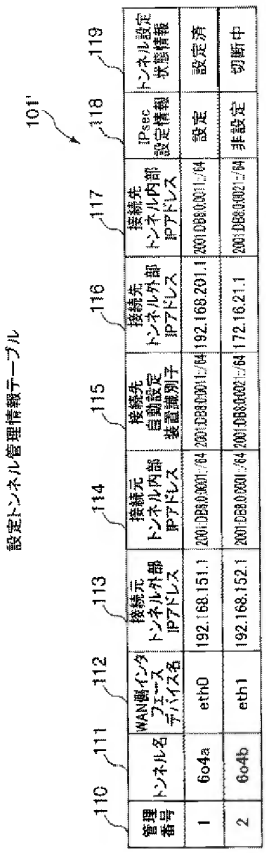
[Drawing 35]


接続先の自動設定装置
情報サーバ
S181
設定済み接続元トンネル
内部IPアドレス要求信号
S182
設定済み接続元トンネル
内部IPアドレスの検索
S183
設定済み接続元トンネル内部IP
アドレス通信信号の作成及び送信
設定済み接続元トンネル
内部IPアドレス通信信号
S184
接続元トンネル内部IP
アドレスは適正か?
設定済み接続元トンネル内部IP
アドレス要求信号の作成及び送信

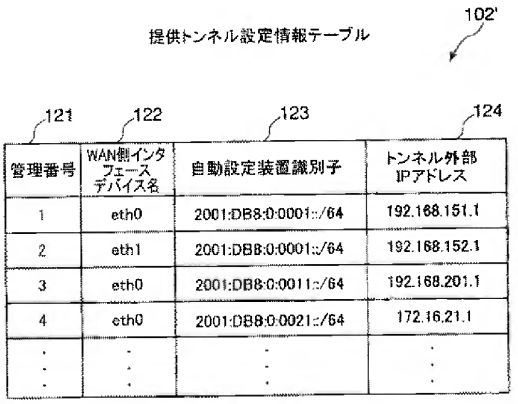
[Drawing 36]



[Drawing 37]



[Drawing 38]



[Translation done.]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-174152
(P2006-174152A)
(43)公開日　平成18年6月29日(2006.6.29)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04Q	7/38	(2006.01)	H04B	7/26	109M	5K067
H04L	9/08	(2006.01)	H04L	9/00	601F	

審査請求 未請求　請求項の数 12　OL　（全 52 頁）

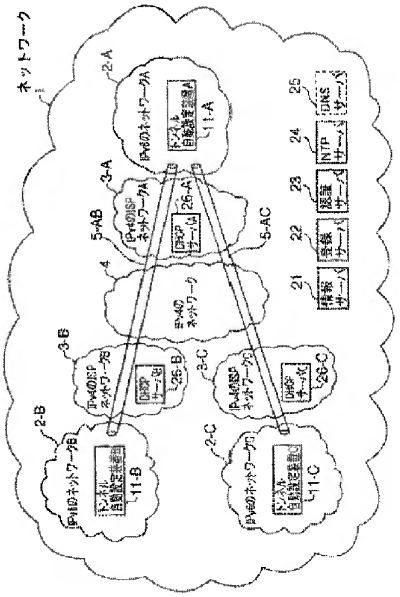
(21)出願番号　特願2004-364591 (P2004-364591)
(22)出願日　平成16年12月16日 (2004.12.16)

(71)出願人　000005832
松下電工株式会社
大阪府門真市大字門真１０４８番地
(71)出願人　503056997
株式会社インターネット総合研究所
東京都新宿区西新宿１－２６－２
(74)代理人　100067828
弁理士　小谷　悦司
(74)代理人　100096150
弁理士　伊藤　孝夫
(74)代理人　100099955
弁理士　樋口　次郎
(72)発明者　藏前　健治
大阪府門真市大字門真１０４８番地　松下電工株式会社内

最終頁に続く

(54)【発明の名称】トンネル自動設定装置、トンネル自動設定方法及びトンネル自動設定プログラム

(57)【要約】
【課題】　本発明は、第三者機関を介した相互認証を行ってセキュリティを向上させつつ自動的にトンネルを構築するトンネル自動設定装置、トンネル自動設定方法及びトンネル自動設定プログラムを提供する。
【解決手段】　本発明に係る、ネットワークに６０４トンネル５を自動的に設定するトンネル自動設定装置１１は、６０４トンネル５における接続先のトンネル自動設定装置１１との間で公開鍵証明書を用いて相互認証を行った後に６０４トンネル５を設定するトンネル設定部を備える。
【選択図】　図１



【特許請求の範囲】
【請求項1】
ネットワークにトンネルを自動的に設定するトンネル自動設定装置において、
前記トンネルにおける接続先のトンネル自動設定装置との間で公開鍵証明書を用いて相互認証を行った後に前記トンネルを設定するトンネル設定部を備えること
を特徴とするトンネル自動設定装置。
【請求項2】
前記トンネルにＩＰｓｅｃを適用するか否かの設定を表すＩＰｓｅｃ設定情報を入力する入力部をさらに備え、
前記トンネル設定部は、前記ＩＰｓｅｃ設定情報に応じて前記トンネルを設定すること
を特徴とする請求項１に記載のトンネル自動設定装置。
【請求項3】
前記接続先のトンネル自動設定装置と公開鍵証明書を用いて相互認証を行った後に前記トンネルを削除するトンネル削除部をさらに備えること
を特徴とする請求項１に記載のトンネル自動設定装置。
【請求項4】
日付と時刻とを計る時計部をさらに備え、
前記トンネル設定部は、前記公開鍵証明書を用いる前に公開鍵証明書の失効リスト及び前記時計部から取得した日付と時刻に基づいて前記公開鍵証明書が有効であるか否かを判断し、有効ではない場合に前記公開鍵証明書を更新すること
を特徴とする請求項１に記載のトンネル自動設定装置。
【請求項5】
日付と時刻とを計る時計部をさらに備え、
前記トンネル削除部は、前記公開鍵証明書を用いる前に公開鍵証明書の失効リスト及び前記時計部から取得した日付と時刻に基づいて前記公開鍵証明書が有効であるか否かを判断し、有効ではない場合に前記公開鍵証明書を更新すること
を特徴とする請求項３に記載のトンネル自動設定装置。
【請求項6】
前記時計部は、ネットワーク内のＮＴＰサーバから現在の日付及び時刻を取得し、前記取得した日付及び時刻と同期をとること
を特徴とする請求項４又は請求項５に記載のトンネル自動設定装置。
【請求項7】
前記トンネル設定部は、起動時に公開鍵証明書を更新すること
を特徴とする請求項１に記載のトンネル自動設定装置。
【請求項8】
前記トンネル削除部は、前記トンネルに障害が発生した場合に前記トンネルを削除すること
を特徴とする請求項３に記載のトンネル自動設定装置。
【請求項9】
前記トンネル削除部は、前記トンネルを削除した後に、前記トンネルを前記トンネル設定部に再設定させること
を特徴とする請求項８に記載のトンネル自動設定装置。
【請求項10】
前記トンネル設定部は、複数個のトンネルを設定可能であること
を特徴とする請求項１に記載のトンネル自動設定装置。
【請求項11】
トンネル自動設定装置を識別する自己の自動設定装置識別子とトンネルの接続先のトンネル自動設定装置における自動設定装置識別子と自己のトンネル内部アドレスとを記憶するトンネル自動設定装置がネットワークに前記トンネルを自動的に設定するトンネル自動

設定方法において、
前記ネットワークへの接続に伴って割り当てられたＩＰアドレスを前記トンネルの接続元のトンネル外部ＩＰアドレスとして取得するステップと、
トンネル外部ＩＰアドレスを自動設定装置識別子に対応付けて管理する情報サーバへ前記割り当てられたＩＰアドレスと前記自己の自動設定装置識別子とを送信するステップと、
前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を前記情報サーバに送信し、前記トンネルの接続先のトンネル外部ＩＰアドレスを取得するステップと、
トンネル自動設定装置の公開鍵証明書を自動設定装置識別子に対応付けて管理しトンネル自動設定装置の公開鍵証明書を発行する認証サーバに、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を送信し、前記トンネルの接続先のトンネル自動設定装置における公開鍵証明書を取得するステップと、
前記トンネルの接続先のトンネル自動設定装置が生成した第１種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、
前記第１種類のチェレンジ文字列を所定の演算方法で演算した演算結果を自己の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第１種類のレスポンス文字列を生成し、前記生成した第１種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、
第２種類のチャレンジ文字列を生成し、前記生成した第２種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、
前記トンネルの接続先のトンネル自動設定装置が前記第２種類のチャレンジ文字列を所定の演算方法で演算した演算結果を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第２種類のレスポンス文字列を生成し、前記生成した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、
前記トンネルの接続先のトンネル自動設定装置から受信した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵で復号した復号結果と、前記第２種類のチャレンジ文字列を前記所定の演算方法で演算した演算結果とが一致するか否かを判断するステップと、
一致する場合に、前記トンネルの接続先のトンネル自動設定装置と前記トンネルを設定するために必要なトンネル内部アドレス及びその他の設定情報を交換し、前記設定情報を用いて前記トンネルを設定するステップとを備えること
を特徴とするトンネル自動設定方法。
【請求項12】
トンネル自動設定装置を識別する自己の自動設定装置識別子とトンネルの接続先のトンネル自動設定装置における自動設定装置識別子と自己のトンネル内部アドレスとを記憶するトンネル自動設定装置に実行させるための、ネットワークに前記トンネルを自動的に設定するトンネル自動設定プログラムにおいて、
前記ネットワークへの接続に伴って割り当てられたＩＰアドレスを前記トンネルの接続元のトンネル外部ＩＰアドレスとして取得するステップと、
トンネル外部ＩＰアドレスを自動設定装置識別子に対応付けて管理する情報サーバへ前記割り当てられたＩＰアドレスと前記自己の自動設定装置識別子とを送信するステップと、
前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を前記情報サーバに送信し、前記トンネルの接続先のトンネル外部ＩＰアドレスを取得するステップと、
トンネル自動設定装置の公開鍵証明書を自動設定装置識別子に対応付けて管理しトンネル自動設定装置の公開鍵証明書を発行する認証サーバに、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を送信し、前記トンネルの接続先のトンネル

自動設定装置における公開鍵証明書を取得するステップと、
前記トンネルの接続先のトンネル自動設定装置が生成した第１種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、
前記第１種類のチェレンジ文字列を所定の演算方法で演算した演算結果を自己の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第１種類のレスポンス文字列を生成し、前記生成した第１種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、
第２種類のチャレンジ文字列を生成し、前記生成した第２種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、
前記トンネルの接続先のトンネル自動設定装置が前記第２種類のチャレンジ文字列を所定の演算方法で演算した演算結果を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第２種類のレスポンス文字列を生成し、前記生成した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、
前記トンネルの接続先のトンネル自動設定装置から受信した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵で復号した復号結果と、前記第２種類のチャレンジ文字列を前記所定の演算方法で演算した演算結果とが一致するか否かを判断するステップと、
一致する場合に、前記トンネルの接続先のトンネル自動設定装置と前記トンネルを設定するために必要なトンネル内部アドレス及びその他の設定情報を交換し、前記設定情報を用いて前記トンネルを設定するステップとを備えること
を特徴とするトンネル自動設定プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ノード間に仮想的なリンク（トンネル）を自動的に設定するトンネル自動設定装置及びトンネル自動設定方法に関する。

【背景技術】

【0002】

１９６９年に米国のＡＲＰＡＮＥＴ（Advanced Research Projects Agency Network）から始まったインターネットは、１９７０年代から１９８０年代にかけてインターネットの基幹技術であるＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）が開発・導入され、１９９０年代の商用サービスの開始とWWW（World Wide Web）技術の開発とをきっかけに爆発的に利用が拡大した。インターネットではネットワーク層のプロトコルとして現在主にＩＰｖ４（Internet Protocol Version 4）が使用されているが、ＩＰｖ４のＩＰアドレス（Internet Protocol Address）（以下、「ＩＰｖ４アドレス」と略記する。）は、３２ビットで構成されているため、利用が拡大した結果ＩＰアドレスの枯渇が一つの問題になった。この問題を解決するために、ＩＰアドレスを１２８ビットに拡大するＩＰｖ６（Internet Protocol Version 6）が開発されている。ＩＰｖ６は、ＩＰｖ４に較べて、ＩＰアドレスを１２８ビットに拡大しただけでなく、集約可能な階層的アドレス体系、マルチキャスト機能、モビリティ機能及びセキュリティ機能等の標準装備、並びに、ＮＤＰ（Neighbor Discovery Protocol、近隣発見プロトコル）によるアドレス解決等の特徴を有し、利便性が向上している。
このような特徴を有するＩＰｖ６のインターネットへの移行が望まれるが、現在普及しているＩＰｖ４を使用した膨大なホストコンピュータやサーバコンピュータやルータ装置等の各ノードを一気にＩＰｖ６に移行することは困難である。このため、ＩＰｖ４からＩＰｖ６への移行期間においては、ＩＰｖ４のネットワークとＩＰｖ６のネットワークとが共存することとなる。この共存環境においては、同一のプロトコルのネットワーク同士を他のプロトコルのネットワークを介して通信を行う技術が必要となる。その一つとして、トンネリングを応用するものがある。

【0003】

このトンネリングは、送信元の装置が接続するネットワークの出口におけるノードで送信情報を別のプロトコルのフレームまたはパケットでカプセル化し、別のプロトコルのネットワークを通過して、宛先の装置が接続するネットワークの入口におけるノードでカプセルを解いて元の送信情報に戻す技術である。このようなトンネリングの技術には、例えば、６ｔｏ４、ＩＳＡＴＡＰ及びＤＴＣＰ等がある（例えば、非特許文献１及び２参照）

【非特許文献1】“ＲＦＣ２４７３　Ｇｅｎｅｒｉｃ　Ｐａｃｋｅｔ　Ｔｕｎｎｅｌｉｎｇ　ｉｎ　ＩＰｖ６　Ｓｐｅｃｉｆｉｃａｔｉｏｎ”，［ｏｎｌｉｎｅ］，ＪＰ－ＮＩＣ，［平成１５年１月２２日検索］、インターネット<http://ｒｆｃ－ｊｐ．ｎｉｃ．ａｄ．ｊｐ／ｒｆｃ／ｒｆｃ２４７３．ｔｘｔ>

【非特許文献2】屏雄一郎、“６ｔｏ４オープンリレールータ運用実験”、ＫＤＤＩ研究所、［平成１６年３月３日検索］、インターネット<ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．６ｔｏ４．ｊｐ／>

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところで、オープンなネットワークを利用した通信では、第三者機関を利用した本人認証、データの完全性及びデータの秘密性（機密性、秘匿性）等の高度なセキュリティを確保する必要があるが、上述したトンネリングの諸技術は、セキュリティが充分とは言えない。即ち、上述の６ｔｏ４及びＩＳＡＴＡＰは、セキュリティを確保する手段自体が備わっていない。ＤＴＣＰは、トンネルを構築する際にＡＰＯＰ（Authenticated Post Office Protocol）を利用していることからパスワードを用いた本人確認を行っているだけで、第三者機関を利用した厳格な本人認証を行っているわけではなく、特にパスワードが漏洩した場合に所謂なりすましが生じ得る。

【0005】

さらに、全てのノードがＩＰｖ６に移行したとしても、コストや性能の点から全てのノードが、特に、エンドノードがセキュリティ機能を備えていない、あるいは、セキュリティ機能の一部しか備えていない場合が生じ得る。このような場合でもセキュアな通信を望む場合がある。

【0006】

本発明は、上述の事情に鑑みて為された発明であり、第三者機関を介した相互認証を行ってセキュリティを向上させつつ自動的にトンネルを構築するトンネル自動設定装置を提供することを目的とする。そして、このようなトンネル自動設定装置に適用されるトンネル自動設定方法を提供することを目的とする。さらに、このようなトンネル自動設定方法のトンネル自動設定プログラムを提供することを目的とする。

【課題を解決するための手段】

【0007】

上述の目的を達成するために、本発明の一態様に係る、ネットワークにトンネルを自動的に設定するトンネル自動設定装置は、前記トンネルにおける接続先のトンネル自動設定装置との間で公開鍵証明書を用いて相互認証を行った後に前記トンネルを設定するトンネル設定部を備えることを特徴とする。

【0008】

そして、上述のトンネル自動設定装置において、前記トンネルにＩＰｓｅｃを適用するか否かの設定を表すＩＰｓｅｃ設定情報を入力する入力部をさらに備え、前記トンネル設定部は、前記ＩＰｓｅｃ設定情報に応じて前記トンネルを設定することを特徴とする。

【0009】

また、上述のトンネル自動設定装置において、前記接続先のトンネル自動設定装置と公開鍵証明書を用いて相互認証を行った後に前記トンネルを削除するトンネル削除部をさらに備えることを特徴とする。

【0010】

さらに、上述のトンネル自動設定装置において、日付と時刻とを計る時計部をさらに備

え、前記トンネル設定部は、前記公開鍵証明書を用いる前に公開鍵証明書の失効リスト及び前記時計部から取得した日付と時刻に基づいて前記公開鍵証明書が有効であるか否かを判断し、有効ではない場合に前記公開鍵証明書を更新することを特徴とする。

【0011】

そして、上述のトンネル自動設定装置において、日付と時刻とを計る時計部をさらに備え、前記トンネル削除部は、前記公開鍵証明書を用いる前に公開鍵証明書の失効リスト及び前記時計部から取得した日付と時刻に基づいて前記公開鍵証明書が有効であるか否かを判断し、有効ではない場合に前記公開鍵証明書を更新することを特徴とする。

【0012】

また、上述のトンネル自動設定装置において、前記時計部は、ネットワーク内のＮＴＰサーバから現在の日付及び時刻を取得し、この取得した日付及び時刻と同期をとることを特徴とする。

【0013】

さらに、上述のトンネル自動設定装置において、前記トンネル設定部は、起動時に公開鍵証明書を更新することを特徴とする。

【0014】

そして、上述のトンネル自動設定装置において、前記トンネル削除部は、前記トンネルに障害が発生した場合に前記トンネルを削除することを特徴とする。

【0015】

また、上述のトンネル自動設定装置において、前記トンネル削除部は、前記トンネルを削除した後に、前記トンネルを前記トンネル設定部に再設定させることを特徴とする。

【0016】

さらに、上述のトンネル自動設定装置において、前記トンネル設定部は、複数個のトンネルを設定可能であることを特徴とする。

【0017】

そして、上述の目的を達成するために、本発明の一態様に係る、トンネル自動設定装置を識別する自己の自動設定装置識別子とトンネルの接続先のトンネル自動設定装置における自動設定装置識別子と自己のトンネル内部アドレスとを記憶するトンネル自動設定装置がネットワークに前記トンネルを自動的に設定するトンネル自動設定方法は、前記ネットワークへの接続に伴って割り当てられたＩＰアドレスを前記トンネルの接続元のトンネル外部ＩＰアドレスとして取得するステップと、トンネル外部ＩＰアドレスを自動設定装置識別子に対応付けて管理する情報サーバへ前記割り当てられたＩＰアドレスと前記自己の自動設定装置識別子とを送信するステップと、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を前記情報サーバに送信し、前記トンネルの接続先のトンネル外部ＩＰアドレスを取得するステップと、トンネル自動設定装置の公開鍵証明書を自動設定装置識別子に対応付けて管理しトンネル自動設定装置の公開鍵証明書を発行する認証サーバに、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を送信し、前記トンネルの接続先のトンネル自動設定装置における公開鍵証明書を取得するステップと、前記トンネルの接続先のトンネル自動設定装置が生成した第１種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、前記第１種類のチェレンジ文字列を所定の演算方法で演算した演算結果を自己の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第１種類のレスポンス文字列を生成し、前記生成した第１種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、第２種類のチャレンジ文字列を生成し、前記生成した第２種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、前記トンネルの接続先のトンネル自動設定装置が前記第２種類のチャレンジ文字列を所定の演算方法で演算した演算結果を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第２種類のレスポンス文字列を生成し、前記生成した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置か

ら受信するステップと、前記トンネルの接続先のトンネル自動設定装置から受信した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵で復号した復号結果と、前記第２種類のチャレンジ文字列を前記所定の演算方法で演算した演算結果とが一致するか否かを判断するステップと、一致する場合に、前記トンネルの接続先のトンネル自動設定装置と前記トンネルを設定するために必要なトンネル内部アドレス及びその他の設定情報を交換し、前記設定情報を用いて前記トンネルを設定するステップとを備えることを特徴とする。

【0018】

また、上述の目的を達成するために、本発明の一態様に係る、トンネル自動設定装置を識別する自己の自動設定装置識別子とトンネルの接続先のトンネル自動設定装置における自動設定装置識別子と自己のトンネル内部アドレスとを記憶するトンネル自動設定装置に実行させるための、ネットワークに前記トンネルを自動的に設定するトンネル自動設定プログラムは、前記ネットワークへの接続に伴って割り当てられたＩＰアドレスを前記トンネルの接続元のトンネル外部ＩＰアドレスとして取得するステップと、トンネル外部ＩＰアドレスを自動設定装置識別子に対応付けて管理する情報サーバへ前記割り当てられたＩＰアドレスと前記自己の自動設定装置識別子とを送信するステップと、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を前記情報サーバに送信し、前記トンネルの接続先のトンネル外部ＩＰアドレスを取得するステップと、トンネル自動設定装置の公開鍵証明書を自動設定装置識別子に対応付けて管理しトンネル自動設定装置の公開鍵証明書を発行する認証サーバに、前記トンネルの接続先のトンネル自動設定装置における自動設定装置識別子を送信し、前記トンネルの接続先のトンネル自動設定装置における公開鍵証明書を取得するステップと、前記トンネルの接続先のトンネル自動設定装置が生成した第１種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、前記第１種類のチェレンジ文字列を所定の演算方法で演算した演算結果を自己の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第１種類のレスポンス文字列を生成し、前記生成した第１種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、第２種類のチャレンジ文字列を生成し、前記生成した第２種類のチャレンジ文字列を前記トンネルの接続先のトンネル自動設定装置に送信するステップと、前記トンネルの接続先のトンネル自動設定装置が前記第２種類のチャレンジ文字列を所定の演算方法で演算した演算結果を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵と暗号鍵ペアを構成する秘密鍵で暗号化することによって第２種類のレスポンス文字列を生成し、前記生成した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置から受信するステップと、前記トンネルの接続先のトンネル自動設定装置から受信した第２種類のレスポンス文字列を前記トンネルの接続先のトンネル自動設定装置におけるトンネル自動設定装置の公開鍵証明書の公開鍵で復号した復号結果と、前記第２種類のチャレンジ文字列を前記所定の演算方法で演算した演算結果とが一致するか否かを判断するステップと、一致する場合に、前記トンネルの接続先のトンネル自動設定装置と前記トンネルを設定するために必要なトンネル内部アドレス及びその他の設定情報を交換し、前記設定情報を用いて前記トンネルを設定するステップとを備えることを特徴とする。

【発明の効果】

【0019】

本発明に係るトンネル自動設定装置、トンネル自動設定方法及びトンネル自動設定プログラムは、トンネルを設定する接続元及び接続先のトンネル自動設定装置にとって第三者機関である公開鍵基盤の認証局が発行する公開鍵証明書を用いて相互認証を行うので、トンネルを設定しようと意図した真正なトンネル自動設定装置との間でトンネルを設定することができる。

【発明を実施するための最良の形態】

【0020】

以下、本発明に係る実施形態を図面に基づいて説明する。なお、各図において同一の符号を付した構成は、同一の構成であることを示し、その説明を省略する。また、総称する場合にはアルファベットの添え字を省略した参照符合で示し、個別の構成を示す場合にはアルファベットの添え字を付した参照符合で示す。

（実施形態の構成）

本実施形態は、２個のＩＰｖ６のネットワーク内におけるトンネル自動設定装置相互間にＩＰｖ４ネットワーク上のトンネルを自動的に設定し得るトンネル自動設定装置の実施形態である。このようにＩＰｖ６のノード間における通信を可能とするためにＩＰｖ４のネットワークに設定されるトンネルをＩＰｖ６ｏｖｅｒＩＰｖ４トンネル（Tunnel）（以下、「６ｏ４トンネル」と略記する。）と呼ぶ。

【0021】

図１は、実施形態におけるネットワークの全体構成を示す図である。図２は、トンネル自動設定装置を含むネットワークの構成を示すブロック図である。図３は、トンネル自動設定装置における設定トンネル管理情報テーブルの構成を示す図である。図４は、情報サーバにおける提供トンネル設定情報テーブルの構成を示す図である。図５は、登録サーバにおけるログイン認証情報登録テーブルの構成を示す図である。図６は、登録サーバにおける自動設定装置本人情報登録テーブルの構成を示す図である。図７は、認証サーバにおけるリポジトリの構成を示す図である。

【0022】

図１において、ネットワーク１は、複数のＩＰｖ６のネットワークと、複数のＩＰｖ４のネットワークとが共存する通信網である。

【0023】

ネットワーク１を構成するＩＰｖ６のネットワークの中には、第三者機関を利用した相互認証を行って６ｏ４トンネルを自動的に設定するトンネル自動設定装置（以下、「自動設定装置」と略記する。）１１を含むＩＰｖ６のネットワーク２がある。ＩＰｖ６のネットワーク２は、例えば、１又は複数の機器等が通信線によって接続されたローカル・エリア・ネットワーク（Local Area Network、ＬＡＮ）、及び、これら機器を遠隔に監視及び制御する遠隔監視制御装置を含むＬＡＮ等である。図１では、３個のＩＰｖ６のネットワーク２－Ａ、２－Ｂ、２－Ｃが示されており、各ＩＰｖ６のネットワーク２－Ａ、２－Ｂ、２－Ｃは、各自動設定装置１１－Ａ、１１－Ｂ、１１－Ｃをそれぞれ含む。

【0024】

ネットワーク１を構成するＩＰｖ４のネットワークの中には、自動設定装置１１が接続すべきインターネット・サービス・プロバイダ（以下、「ＩＳＰ」と略記する。）が構築するＩＳＰネットワーク３、及び、ＩＳＰネットワーク３が接続するネットワーク４がある。ＩＳＰネットワーク３は、図１では、３個のＩＰｖ４のＩＳＰネットワーク３－Ａ、３－Ｂ、３－Ｃが示されており、各ＩＳＰネットワーク３－Ａ、３－Ｂ、３－Ｃは、各自動設定装置１１－Ａ、１１－Ｂ、１１－Ｃに対しインターネットに接続するサービスをそれぞれ提供する。各ＩＳＰネットワーク３－Ａ、３－Ｂ、３－Ｃには、インターネットに接続するサービスを受けるべく接続を要求するクライアントに未割り振りのＩＰアドレスを自動的に割り振るＤＨＣＰ（Dynamic Host Configuration Protocol）サーバ２６－Ａ、２６－Ｂ、２６－Ｃがそれぞれ含まれ、そして、インターネットに接続するサービスを提供する通信可能なコンピュータ（ＩＳＰコンピュータ、不図示）がそれぞれ含まれる。ネットワーク４は、ＩＰｖ４を使用するルータ装置、ゲートウェイ装置、サーバコンピュータ、ホストコンピュータ等のノードで構成されるネットワークである。

【0025】

そして、ネットワーク１は、自動設定装置１１が６ｏ４トンネルを自動的に設定する場合に６ｏ４トンネルの設定に必要な情報を提供する情報サーバ２１と、自動設定装置１１の公開鍵に対する公開鍵証明書の発行に関し本人認証を行うと共に本人（自動設定装置１１）に関する情報を登録し管理する登録サーバ２２と、登録サーバ２２が本人認証を行って真正であると認めた自動設定装置１１の公開鍵に対し公開鍵証明書を発行する認証サー

バ２３と、クライアント（自動設定装置１１及び認証サーバ２３を含む）からの要求に応じて時刻を返信するＮＴＰ（Network Time Protocol）サーバ２４とを含む。

【0026】

登録サーバ２２及び認証サーバ２３は、所謂公開鍵基盤（Public Key Infrastructur、ＰＫＩ）における登録局（Registration Authority）及び認証局（Certification Authority）の役割をそれぞれ担う。このように登録サーバ２２と認証サーバ２３とを分けることによって認証サーバ２３は、公開鍵証明書の発行にハードウェア資源及びソフトウェア資源を集中することができ、負担を軽減することができる。なお、登録サーバ２２と認証サーバ２３とを同一のコンピュータによって実現してもよい。

【0027】

また、ネットワーク１は、例えば、電話網、ディジタル通信網及び無線通信網等であり、所定の通信プロトコルを用いて情報を収容した通信信号が伝送される。本実施形態では、ネットワーク１は、通信プロトコルにＨＴＴＰ（Hyper Text Transfer Protocol）、ＦＴＰ（File Transfer Protocol）、ＰＯＰ３（Post Office Protocol ver.3）、ＳＭＴＰ（Simple Mail Transfer Protocol）、Ｔｅｌｎｅｔ、ＴＣＰ（Transmission Control Protocol）、ＵＤＰ（User Datagram Protocol）及びＩＰ（Internet Protocol）等のインターネットプロトコル群が用いられてインターネットを構成する。なお、ＩＰは、複数のバージョン、本実施形態ではバージョン４とバージョン６とが使用されている。

【0028】

ＩＰｖ６のネットワーク２に含まれる自動設定装置１１は、本実施形態では、例えば、ＩＰｖ６のネットワーク２とネットワーク１を構成する他のネットワークとの境界に配置されるルータ装置に組み込まれ、ネットワーク１を構成する他のネットワークから送信されてきた通信パケット、当該自動設定装置１１が属するＩＰｖ６のネットワーク２から送信されてきた通信パケット、及び、当該自動設定装置１１自身が送信する通信パケット等をルーティング（経路選択）すると共に、他のＩＰｖ６のネットワーク内に在る自動設定装置１１との間に６ｏ４トンネルを自動的に設定する。図１に示す例では、ＩＰｖ６のネットワーク２－Ａ内の自動設定装置１１－Ａは、ＩＰｖ６のネットワーク２－Ｂ内の自動設定装置１１－Ｂとの間、及び、ＩＰｖ６のネットワーク２－Ｃ内の自動設定装置１１－Ｃとの間にそれぞれＩＰｖ６ｏｖｅｒＩＰｖ４トンネル５－ＡＢ、５－ＡＣを自動的に設定する。

【0029】

例えば、図２に示す例では、自動設定装置１１は、一戸建て住宅、集合住宅、公共施設、オフィスビル等の建造物に設置されるＩＰｖ６のネットワーク２のルータ装置に組み込まれている。ＩＰｖ６のネットワーク２は、自動設定装置１１、電気をエネルギー源として稼動する１又は複数の機器１２（１２－Ａ、１２－Ｂ、・・・）、自動設定装置１１と機器１２とを接続する通信線１３、例えば、イーサネット（Ethernet、登録商標）を備え、イントラネットを構成している。

【0030】

機器１２は、自動設定装置１１と通信線１３を介して通信を行う通信部８１と、機器１２の機能を実行する機能部８２とを備えて構成され、機能部８２の状態（例えば、電源のオン・オフ、稼動状態、故障状態等）を他のネットワーク内の遠隔監視制御装置等に通信線１３及び自動設定装置１１を介して通信部８１を用いて送信すると共に、機能部８２の状態を制御する制御命令を他のネットワーク内の遠隔監視制御装置等から自動設定装置１１及び通信線１３を介して通信部８１を用いて受信し制御命令の通りに制御するものである。制御命令は、例えば、遠隔監視制御装置等にアクセスする携帯電話やＰＤＡ（Personal Digital Assistants）やパーソナルコンピュータ等の端末装置から送信される。機能部８２は、機器１２が、例えば、ガスの使用量を計量するガスメータである場合には、ガスの使用量を計量する計量機能である。機器１２は、ガスメータの他に、例えば、電気の使用量を計量する電気メータ、及び、水道の使用量を計量する水道メータ等の計量メータ、照明器具及び空調装置等の住戸環境やオフィス環境等を調整する装置、煙センサ、温度

センサ及び湿度センサ等のセンサ、電子錠装置等の住戸設備、テレビジョン、ビデオテープレコーダ、ＤＶＤレコーダ及び洗濯機等の家電製品、コンピュータ等の情報処理装置、電話機及びファクシミリ装置等の通信機器、そして、脈拍計、体温計、血中酸素濃度計及び心電図計等の医療機器等である。

【0031】

自動設定装置１１は、図２に示すように、ローカル・エリア・ネットワーク側インターフェース部（以下、「ＬＡＮ側インターフェース部」と略記する。）５１と、制御部５２と、記憶部５３と、入力部５４と、ワイド・エリア・ネットワーク側インターフェース部（以下、「ＷＡＮ側インターフェース部」と略記する。）５５とを備えて構成される。

【0032】

ＬＡＮ側インターフェース部５１は、当該自動設定装置１１が属するＩＰｖ６のネットワーク２内における機器１２との間で通信線１３を介して通信信号を送受信するインターフェース回路であり、例えば、イーサネットカード等のネットワークカードである。入力部５４は、６ｏ４トンネルにＩＰｓｅｃを適用するか否かの設定を表すＩＰｓｅｃ（IPsecurity）設定情報、６ｏ４トンネルを設定する接続先の自動設定装置１１における自動設定装置識別子等の各種情報を当該自動設定装置１１に入力する装置であり、例えば、ディップスイッチやジャンパースイッチやテンキーパッド等である。なお、入力部５４がテンキーパッドやキーボード等の入力装置である場合には、入力内容を確認するために液晶表示装置等の表示部をさらに備えることが好ましい。ＷＡＮ側インターフェース部５５は、ネットワーク１を構成する他のネットワークとの間で通信信号を送受信するインターフェース回路であり、例えば５６ＫモデムやターミナルアダプタやＡＤＳＬモデム等のモデムである。

【0033】

記憶部５３は、トンネル設定用情報を記憶するトンネル設定用情報記憶部７１、セキュリティ情報を記憶するセキュリティ情報記憶部７２及び設定トンネル管理情報を記憶する設定トンネル管理情報記憶部７３を備え、トンネルを自動的に設定するためのトンネル自動設定プログラム、インターネットを利用するためのプログラム、通信パケットのルーティングを行うルーティングプログラム等の各種プログラム、及び、トンネルの設定に係る情報や各種プログラムの実行中に生じる情報等の各種情報を記憶する。記憶部５３は、例えば、ＲＡＭ（Random Access Memory）等の揮発性のメモリ、及び、ＲＯＭ（Read Only Memory）や書換え可能なＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）等の不揮発性のメモリを備えて構成される。

【0034】

トンネル設定用情報は、トンネルを自動的に設定するために必要な予め記憶される情報であり、本実施形態では、情報サーバ２１のＩＰアドレス、及び、自動設定装置１１を識別するために予め割り当てられた固有な（ユニークな）識別子（自動設定装置識別子）である。自動設定装置識別子は、例えば、１又は複数の記号からなる記号列であり、本実施形態では、当該自動設定装置１１のＩＰｖ６アドレスの生成情報（プレフィックス等を含む。）と兼用されている。このため、自動設定装置１１のＩＰｖ６アドレスの生成情報は、製造段階や出荷段階等において記憶されるので、製造企業は、自動設定装置１１のＩＰｖ６アドレスの生成情報を管理することができる。

【0035】

６ｏ４トンネルを自動的に設定する場合には、６ｏ４トンネルを設定する接続元のトンネル内部ＩＰアドレス（複数のＩＰアドレスを含むネットワークの場合は、ＩＰアドレス及びプレフィックス長などのネットワークに関する付帯情報である。以下、ネットワークの場合もトンネル内部ＩＰアドレスと呼ぶことにする。）及びトンネル外部ＩＰアドレスと接続先のトンネル内部ＩＰアドレス及びトンネル外部ＩＰアドレスとが必要である。トンネル内部ＩＰアドレスは、カプセル化（カプセリング）される通信パケットにおけるＩＰヘッダのＩＰアドレス、即ち、カプセリング後の通信パケットにおけるペイロードに収容される通信パケットにおけるＩＰヘッダのＩＰアドレスが対応し、トンネル外部ＩＰア

ドレスは、カプセリング後の通信パケットにおけるＩＰヘッダのＩＰアドレスが対応する。本実施形態では、ＩＰｖ６ｏｖｅｒＩＰｖ４トンネルを自動的に設定するので、接続元のＩＰｖ６アドレス（トンネル内部ＩＰアドレスに対応）及びＩＰｖ４アドレス（トンネル外部ＩＰアドレスに対応）と接続先のＩＰｖ６アドレス（トンネル内部ＩＰアドレスに対応）及びＩＰｖ４アドレス（トンネル外部ＩＰアドレスに対応）とが必要である。接続元のＩＰｖ６アドレスは、接続元の自動設定装置識別子から生成され、後述するように、接続元のＩＰｖ４アドレスは、接続元の自動設定装置がＩＳＰネットワーク３に接続した時に、ＩＳＰネットワーク３内のＤＨＣＰサーバによって割り当てられる。同様に、接続先のＩＰｖ６アドレスは、接続先の自動設定装置識別子から生成され、後述するように、接続先のＩＰｖ４アドレスは、接続先の自動設定装置がＩＳＰネットワーク３に接続した時に、ＩＳＰネットワーク３内のＤＨＣＰサーバによって割り当てられる。そして、接続元の自動設定装置は、情報サーバ２１から接続先のＩＰｖ４アドレスを取得する。

【0036】

セキュリティ情報は、第三者機関を利用した本人認証を行うために必要な情報であり、予め記憶される情報と後述の動作によって記憶される情報とがある。予め記憶される情報は、登録サーバ２２のＩＰアドレス、認証サーバ２３のＩＰアドレス、ＮＴＰサーバ２４のＩＰアドレス、登録サーバ２２にログインするためのＩＤとパスワードとの組、及び、ＩＰｓｅｃが設定された場合に必要となるＩＰｓｅｃ関連情報であり、そして、後述の動作によって記憶される情報は、自動設定装置１１の暗号鍵ペア、自動設定装置１１の公開鍵証明書、認証サーバ２３の公開鍵証明書及び接続先の自動設定装置１１の公開鍵証明書である。ＩＰｓｅｃ関連情報は、後述するように、本実施形態では、送信元ポート番号、宛先ポート番号、トランスポート層プロトコル、アクション、セキュリティプロトコル、カプセル化モード、暗号化アルゴリズム及び認証アルゴリズムである。

【0037】

設定トンネル管理情報は、対向する接続先の自動設定装置１１との間に設定した６ｏ４トンネルに関する情報であり、接続元のトンネル内部ＩＰアドレス及びトンネル外部ＩＰアドレスと接続先のトンネル内部ＩＰアドレス及びトンネル外部ＩＰアドレスとが少なくとも含まれる。

【0038】

本実施形態では、設定トンネル管理情報は、６ｏ４トンネルを識別するためのトンネル名と、接続元の自動設定装置１１におけるトンネル内部ＩＰアドレス及びトンネル外部ＩＰアドレスと、接続先の自動設定装置１１における自動設定装置識別子、トンネル内部ＩＰアドレス及びトンネル外部ＩＰアドレスと、ＩＰｓｅｃ設定情報と、６ｏ４トンネルが設定済みであるか削除中であるかの６ｏ４トンネルの設定状態を示すトンネル設定状態情報とである。これら設定トンネル管理情報は、例えば、図３に示すように、テーブル形式で記憶され、設定トンネル管理情報を登録する設定トンネル管理情報テーブル１０１は、各レコードを識別する管理番号を登録する管理番号フィールド１１０と、トンネル名を登録するトンネル名フィールド１１１と、接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスを登録する接続元トンネル外部ＩＰアドレスフィールド１１３と、接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスを登録する接続元トンネル内部ＩＰアドレスフィールド１１４と、接続先の自動設定装置１１における自動設定装置識別子を登録する接続先自動設定装置識別子フィールド１１５と、接続先の自動設定装置１１におけるトンネル外部ＩＰアドレスを登録する接続先トンネル外部ＩＰアドレスフィールド１１６と、接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスを登録する接続元トンネル内部ＩＰアドレスフィールド１１７と、ＩＰｓｅｃ設定情報を登録するＩＰｓｅｃ設定情報フィールド１１８と、トンネル設定状態情報を登録するトンネル設定状態情報フィールド１１９とを備えて構成され、トンネル名ごとに、即ち、設定されている６ｏ４トンネルごとにレコードが作成される。

【0039】

このように自動設定装置１１が設定トンネル管理情報テーブル１０１を備え、６ｏ４ト

ンネルごとに管理することによって複数の他の自動設定装置１１へ複数の６０４トンネルをそれぞれ同時に設定することができる。そして、制御部５２は、同時に設定された複数の６０４トンネルを時分割で運用する。また、設定トンネル管理情報テーブル１０１にトンネル設定状態情報フィールド１１９を備えることによって、このトンネル設定状態情報フィールド１１９の情報を例えば端末装置からネットワーク１を介して参照することで６０４トンネルが設定済みであるか削除中であるかを知ることができる。

【0040】

なお、各種情報や各種プログラムが記憶部５３に記憶されていない場合には、これら各種情報や各種プログラムは、これらを記録したＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の記録媒体を用いて図略のドライブ装置を介してインストールしたり、これら各種情報や各種プログラムを管理するサーバからネットワーク１を介してダウンロードすることによってインストールしたりしてもよい。

【0041】

制御部５２は、各種プログラムを実行することによって通信パケットのルーティングや６０４トンネルの自動設定等を行って自動設定装置１１全体を制御するものであり、機能的に、通信パケットのルーティングを行うルーティング部６１、１又は複数の６０４トンネルを設定するトンネル設定部６２、接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスを生成する接続先トンネル内部ＩＰアドレス生成部６３、公開鍵証明書を管理する公開鍵証明書管理部６４、設定した６０４トンネルを削除するトンネル削除部６５、及び、日付と時刻とを計る時計部６６を備える。制御部５２は、例えば、マイクロプロセッサ等を備えて構成される。

【0042】

情報サーバ２１は、自動設定装置１１が６０４トンネルを自動的に設定する場合にトンネルの設定に必要な情報を提供する通信可能なサーバコンピュータであり、その記憶部に、提供する６０４トンネルの設定に必要な情報（提供トンネル設定情報）を自動設定装置識別子に対応付けて記憶する提供トンネル設定情報記憶部を備える。

【0043】

提供トンネル設定情報は、少なくともトンネル外部アドレスである。例えば、図４に示すように、テーブル形式で記憶され、提供トンネル設定情報を登録する提供トンネル設定情報テーブル１０２は、各レコードを識別する管理番号を登録する管理番号フィールド１２１と、自動設定装置識別子を登録する自動設定装置識別子フィールド１２３と、トンネル外部ＩＰアドレスを登録するトンネル外部ＩＰアドレスフィールド１２４とを備えて構成され、自動設定装置識別子ごとにレコードが作成される。

【0044】

登録サーバ２２は、自動設定装置１１の公開鍵に対する公開鍵証明書の発行に関し本人認証を行うと共に本人（自動設定装置１１）に関する情報を登録し管理する通信可能なサーバコンピュータであり、その記憶部に、ログイン認証情報登録テーブルを予め記憶するログイン認証情報登録テーブル記憶部、及び、自動設定装置本人情報登録テーブルを記憶する自動設定装置本人情報登録テーブル記憶部を備える。

【0045】

ログイン認証情報登録テーブルは、当該登録サーバ２２にログインを許可する自動設定装置１１に設定されている自動設定装置１１のＩＤ及びパスワードを予め登録する。ログイン認証情報登録テーブル１０３は、例えば、図５に示すように、各レコードを管理するための管理番号を登録する管理番号フィールド１３１、自動設定装置１１を特定するＩＤ（Identification）を登録するＩＤフィールド１３２、及び、ＩＤと組み合わされて正規な利用者であるかどうかの識別に用いられるパスワードを登録するパスワードフィールド１３３の各フィールドを備えて構成され、ＩＤごとにレコードが作成される。

【0046】

自動設定装置本人情報登録テーブルは、認証サーバ２３が公開鍵証明書を発行するために登録サーバ２２が本人認証した自動設定装置１１に関する情報（自動設定装置本人情報

）を登録するテーブルであり、本実施形態では、自動設定装置１１のデジタル署名を検証するための公開鍵（自動設定装置１１の公開鍵）、及び、自動設定装置１１に関する情報（自動設定装置本人情報）である。自動設定装置本人情報は、例えば、本実施形態では、自動設定装置１１の自動設定装置識別子、設置場所の住所、取り扱い責任者の氏名、及び、責任者の連絡先である。このため、本実施形態では、例えば、図６に示すように、自動設定装置本人情報登録テーブル１０４は、各レコードを管理するための管理番号を登録する管理願号フィールド１４１、自動設定装置１１の公開鍵を登録する公開鍵フィールド１４２、及び、自動設定装置本人情報を登録する自動設定装置本人情報フィールド１４３の各フィールドを備えて構成され、自動設定装置１１の公開鍵ごとにレコードが作成される。そして、自動設定装置本人情報フィールド１４３は、自動設定装置１１の自動設定装置識別子を登録する自動設定装置識別子フィールド１４３１、自動設定装置１１の設置場所の住所を登録する設置場所住所フィールド１４３２、自動設定装置１１を取り扱う責任者の氏名（管理企業の企業名を含む）を登録する責任者名フィールド１４３３、及び、当該責任者の連絡先を登録する連絡先フィールド１４３４の各サブフィールドを備えて構成される。ここで、連絡先は、電話番号、ファクシミリ番号及び電子メールアドレス等のネットワーク１を利用する通信手段の宛先である。

【0047】

認証サーバ２３は、登録サーバ２２が本人認証を行って真正であると認めた自動設定装置１１の公開鍵に対し公開鍵証明書を発行する通信可能なサーバコンピュータであり、その記憶部に、認証サーバ２３の公開鍵証明書に関する情報、即ち、認証サーバ２３の公開鍵証明書と有効期限とを記憶する認証サーバ公開鍵証明書記憶部、リポジトリを記憶するリポジトリ記憶部、証明書破棄リストを記憶する証明書破棄リスト記憶部、及び、後述のセルフ署名用の暗号鍵ペアを記憶するセルフ署名用暗号鍵ペア記憶部を備える。そして、認証サーバ２３は、ＮＴＰサーバ２４から現在の時刻を取得してこの時刻に内部の時計を合わせる時計部を備える。

【0048】

リポジトリは、自動設定装置１１の公開鍵証明書を当該自動設定装置１１の自動設定装置識別子に対応付けて登録するテーブルである。公開鍵証明書の形式は、ＰＫＣＳ＃６（Extended-Certificate Syntax Standard）やＩＴＵ（International Telecommunication Union、国際電気通信連合）のＸ．５０９等種々あるが、例えばＸ．５０９の規格に従う場合には、例えば、図７に示すように、リポジトリ１０５は、各レコードを管理するための管理番号を登録する管理番号フィールド１５１、自動設定装置識別子（公開鍵の所有者に対応する）を登録する自動設定装置識別子フィールド１５２、及び、自動設定装置１１の公開鍵証明書を登録する公開鍵証明書フィールド１５３を備え、自動設定装置１１ごとにレコードが作成される。ここで、Ｘ．５０９に従う公開鍵証明書には、公開鍵証明書のシリアル番号、デジタル証明書のアルゴリズム、公開鍵におけるアルゴリズム、年月日時分秒で表される有効期間の開始時期、年月日時分秒で表される有効期間の終了時期、公開鍵、公開鍵証明書の規格のバージョン、証明書の発行者、証明書の所有者、認証サーバ２３よる署名が含まれる。

【0049】

証明書破棄リスト（失効リスト、Certificate Revocation List、ＣＲＬ）は、破棄（失効）した公開鍵証明書の一覧であり、より具体的には、破棄した公開鍵証明書のシリアル番号の一覧に対し、当該破棄した公開鍵証明書を発行した認証局がデジタル署名を付したものである。

【0050】

認証サーバ２３は、自動設定装置１１の公開鍵に対しデジタル署名を行った公開鍵証明書を発行するが、そのデジタル署名を行うために認証サーバ２３の秘密鍵が必要であり、当該認証サーバ２３の秘密鍵と暗号鍵ペアを構成する認証サーバ２３の公開鍵を自動設定装置１１に配布する必要がある。これは、或る自動設定装置１１が他の自動設定装置１１の公開鍵証明書を検証するために必要となるからである。この認証サーバ２３の公開鍵を

配布の際に、自動設定装置１１は、配布された認証サーバ２３の公開鍵が真正であるか否かを判断する必要があるが、この真正であることの確認に、本実施形態では、認証サーバ２３自身が認証サーバ２３の公開鍵にデジタル署名を行うセルフ署名（self-signature）を採用している。この認証サーバ２３自身が認証サーバ２３の公開鍵にデジタル署名を行った公開鍵証明書が認証サーバ２３の公開鍵証明書である。ここで、セルフ署名を行うための暗号鍵ペアをセルフ署名用暗号鍵ペアと呼称することとし、その秘密鍵及び公開鍵をセルフ署名用秘密鍵及びセルフ署名用公開鍵とそれぞれ呼称することとする。このセルフ署名用公開鍵は、認証サーバ２３の公開鍵証明書を検証するための公開鍵となる。また、本実施形態では、セルフ署名を採用しているが、他の公開鍵基盤の認証局、例えば、政府公開鍵基盤（Government Public Key Infrastructure、ＧＰＫＩ）の認証局によって認証サーバ２３の公開鍵を認証するように構成してもよい。

【0051】

ＮＴＰサーバ２４は、クライアントからの要求に応じて時刻を返信する通信可能なサーバコンピュータである。ＮＴＰは、一般に、他のＮＴＰサーバやホストコンピュータとＮＴＰサーバが最上位となる階層構造を持ち、最上位であるＮＴＰサーバが原子時計やＧＰＳ等の正確な時計から標準時を取得し、下位のホストコンピュータ（下位のＮＴＰサーバを含む）がそれを参照してその時刻で自己の時計における時刻を合わせることによって、ネットワーク内のノード間において同期をとるものである。自動設定装置１１や認証サーバ２３は、ＮＴＰサーバ２４から日付と時刻とを取得し、この取得した日付と時刻とに自己の内部に備える時計、例えばソフトウェア時計を合わせることによって同期をとることができる。

【0052】

次に、本実施形態の動作について説明する。

（実施形態の動作）

まず、自動設定装置１１が認証サーバ２３に公開鍵証明書を発行してもらうための公開鍵証明書取得処理について説明する。この公開鍵証明書取得処理は、自動設定装置１１が６ｏ４トンネルを自動的に設定する前に事前に行う処理である。公開鍵証明書は、認証サーバ２３が発行するデータであって、デジタル署名検証用の自動設定装置１１の公開鍵が真正であることを証明するデータである。

【0053】

図８は、公開鍵証明書取得処理の動作を示すシーケンス図である。図９は、自動設定装置の公開鍵証明書の発行処理における動作を示すフローチャートである。図１０は、自動設定装置の公開鍵証明書の記憶処理における動作を示すフローチャートである。

【0054】

図８において、自動設定装置１１の制御部５２における公開鍵証明書管理部６４は、公開鍵暗号における公開鍵（自動設定装置１１の公開鍵）と秘密鍵（自動設定装置１１の秘密鍵）との暗号鍵ペアを生成する（Ｓ１１）。

【0055】

公開鍵暗号（非対称鍵暗号）は、秘密鍵で暗号化されたデータが、対応する公開鍵（秘密鍵と暗号鍵ペアを構成する公開鍵）でしか復号することができず、公開鍵で暗号化されたデータが、対応する秘密鍵（公開鍵と暗号鍵ペアを構成する秘密鍵）でしか復号することができない暗号方式である。通常、公開鍵は、暗号鍵ペアのうち広く公開される鍵であり、秘密鍵は、暗号鍵ペアのうち本人だけが分かるように厳重に管理され秘匿される鍵である。公開鍵暗号は、鍵を安全な経路で輸送する必要がないため、暗号化と復号化とを同じ鍵で行う共通鍵暗号（対称暗号、秘密鍵暗号）に比べて鍵の管理が容易であり安全性が高い。

【0056】

公開鍵暗号は、種々のアルゴリズムによる各種方式があるが、例えば、ＲＳＡ（Rivest-Shamir-Adleman）方式、ＥｌＧａｍａｌ方式、Ｒａｂｉｎ方式及び楕円曲線暗号等がある。公開鍵暗号において、データの秘密性を確保するためにデータを暗号化する場合では

、送信者が公開鍵でデータを暗号化し、受信者が秘密鍵で復号化することになるが、本人認証を行うためのデジタル署名の場合では、署名者がデータを秘密鍵で暗号化し（署名の作成に相当）、検証者が公開鍵で復号化する（署名の検証に相当）ことになる。そして、署名者の公開鍵を信頼し得る認証局で認証すること（公開鍵証明書の発行）によって、公開鍵証明書付きの公開鍵を受信した装置側は、当該公開鍵を真正な署名者本人の公開鍵であると信頼することができる。

【0057】

次に、自動設定装置１１の公開鍵証明書管理部６４は、登録サーバ２２に本人認証を行わせ認証サーバ２３に公開鍵証明書を発行させるために、処理Ｓ１１で作成した自動設定装置１１の公開鍵、及び、当該自動設定装置１１の自動設定装置本人情報を収容する通信信号（公開鍵証明書発行要求信号）を作成する（Ｓ１２）。

【0058】

そして、自動設定装置１１の公開鍵証明書管理部６４は、ＩＳＰネットワーク３に接続してインターネット接続サービスを受け、セキュリティ情報記憶部７２の登録サーバ２２のＩＰアドレスを用いて登録サーバ２２にアクセスし、予め設定され記憶されているＩＤとパスワードとを登録サーバ２２に送信し、登録サーバ２２にログインする（Ｓ１３）。登録サーバ２２は、ログイン認証情報登録テーブル１０３を参照し、自動設定装置１１から送信されたＩＤとパスワードとの組がログイン認証情報登録テーブル１０３に登録されているか否かを判断し、登録されいる場合には正当な自動設定装置１１であると認め、自動設定装置１１のログインを許可する。なお、登録されていない場合には、ログインを拒否し、切断する。

【0059】

次に、自動設定装置１１は、ログインに成功すると、自動設定装置１１の公開鍵に対する公開鍵証明書を得るべく、公開鍵証明書発行要求信号を登録サーバ２２に送信する（Ｓ１４）。登録サーバ２２は、公開鍵証明書発行要求信号を受信すると、自動設定装置本人情報登録テーブル１０４に新たな管理番号を付して新たなレコードを追加し、公開鍵証明書発行要求信号に収容されている自動設定装置１１の公開鍵及び自動設定装置本人情報を新たに追加したレコードにおける公開鍵フィールド１４２及び自動設定装置本人情報フィールド１４３にそれぞれに登録する（Ｓ１５）。

【0060】

本実施形態では、デジタル署名の発行を要求する自動設定装置１１が真正な自動設定装置１１であること（所謂本人確認）は、上述のように、当該自動設定装置１１が登録サーバ２２にログインが可能であることによって判断している。公開鍵証明書の信頼性は、認証サーバ２３の信頼性に依存し、特に本人確認の信頼性が重要となるが、本実施形態では自動設定装置１１の製造企業や販売企業が自動設定装置１１のＩＤ及びパスワードの組を販売前に予め自動設定装置１１に組み込む、あるいは、郵送や電話によって購買者に配布するように構成することでこの本人確認の信頼性を確保している。なお、郵送や電話による場合には、ＩＤ及びパスワードは、入力部５４から自動設定装置１１に記憶される。

【0061】

また、パスワードの漏洩を防止しさらに本人確認の信頼性を向上させる観点から、処理Ｓ１３の処理に、ワンタイム・パスワード（One-Time Password）技術を用いてもよい。このワンタイム・パスワード技術は、まずサーバ（本実施形態では登録サーバ２２）がクライアント（本実施形態では自動設定装置１１）に認証文字列の「種」となるランダムな文字列（チャレンジ文字列）を生成してこのチャレンジ文字列を送信し、クライアントがチャレンジ文字列とパスワードとを用いて所定の手順に従って演算し、演算結果（認証文字列、レスポンス文字列）をサーバに返信し、サーバが生成したチャレンジ文字列と記憶しているパスワードとを用いてクライアントから返信されたレスポンス文字列を検証することによって、正規のクライアントであるか判別する技術である。さらに本人確認の信頼性を向上させる観点から、ログイン認証情報登録テーブル１０３に自動設定装置１１のＩＰアドレスをＩＤに対応付けてさらに登録し、公開鍵証明書発行要求信号を受信した場合

に、処理Ｓ１３でログインを許可したＩＤに対応するＩＰアドレスをログイン認証情報登録テーブル１０３から検索し、検索したＩＰアドレスを宛先とした公開鍵証明書発行要求信号を送信したか否かを問う通信信号（本人確認信号）を送信し、公開鍵証明書発行要求信号を送信した旨の返信を受けることによって本人確認を行ってもよい。

【0062】

次に、登録サーバ２２は、公開鍵証明書発行要求信号を送信した自動設定装置１１に対し公開鍵証明書を発行するように認証サーバ２３に要求する旨の情報、当該自動設定装置１１の自動設定装置識別子、及び、当該自動設定装置１１の公開鍵を収容した通信信号（発行要求信号）を作成し、認証サーバ２３に送信する（Ｓ１６）。本実施形態では、登録サーバ２２は、公開鍵証明書発行要求信号を受信した場合に、無条件に発行要求信号を認証サーバ２２に送信するように構成しているが、発行要求信号の送信を明示するために、公開鍵証明書発行要求信号にさらに認証サーバ２３に公開鍵証明書の発行を要求する旨の情報を収容し、登録サーバ２２は、公開鍵証明書発行要求信号にこの情報が収容されている場合に、認証サーバ２２に発行要求信号を送信するように構成してもよい。

【0063】

認証サーバ２３は、登録サーバ２２から発行要求信号を受信すると、登録サーバ２２の自動設定装置１１に対する本人認証を信頼し、直ちに自動設定装置１１の公開鍵に対し公開鍵証明書の発行処理を行う（Ｓ１７）。

【0064】

この公開鍵証明書の発行処理についてより詳細に説明すると、図９において、認証サーバ２３は、まず、認証サーバ公開鍵証明書記憶部を参照することによって、認証サーバ２３の公開鍵証明書が存在するか否か及び有効であるか否かを判断する（Ｓ２１）。有効であるか否かの判断は、認証サーバ２３の公開鍵証明書が存在する場合において、当該認証サーバ２３の公開鍵証明書が有効期限内であるか否か、及び、証明書破棄リストに載っているか否かを判断することによって行われる。有効期限内であって証明書破棄リストに載っていない場合には、有効と判断され、有効期限外である、または、証明書破棄リストに載っている場合には、有効ではないと判断される。

【0065】

判断の結果、認証サーバ２３の公開鍵証明書が存在しない、または、有効ではない場合（Ｎｏ）には、認証サーバ２３は、自動設定装置１１の公開鍵証明書を作成するために必要な暗号鍵ペア（認証サーバ２３の公開鍵及び秘密鍵）を生成し（Ｓ２２）、セルフ署名用秘密鍵を用いて処理Ｓ２２で新たに生成した認証サーバ２３の公開鍵にデジタル署名を行うことによって認証サーバ２３の公開鍵証明書を作成し（Ｓ２３）、作成した認証サーバ２３の公開鍵証明書を認証サーバ公開鍵証明書記憶部に記憶し（Ｓ２４）、そして、新たに作成した認証サーバ２３の公開鍵証明書を全ての自動設定装置１１に配布する（Ｓ２５）。この配布は、例えば、自動設定装置１１が認証サーバ２３から認証サーバ２３の公開鍵証明書を取得することが可能な状態とすることによって配布する。この取得可能な状態は、例えば、ＷｅｂサーバやＬＤＡＰサーバなどを介して認証を伴わずにアクセスできる箇所に、認証サーバ２３の公開鍵証明書を設置することによって実現される。なお、本実施形態では、セルフ署名であるため、認証サーバ２３が処理Ｓ２３において認証サーバ２３の公開鍵証明書を作成したが、他の認証局がデジタル署名を行う場合には、処理Ｓ２３において、この他の認証局に処理Ｓ２２で生成した公開鍵に対する公開鍵証明書の発行を要求することになる。また、図９に示す動作では、セルフ署名用暗号鍵ペアは、有効なものとしたが、このセルフ署名用暗号鍵ペアの有効性をチェックする処理をさらに追加してもよい。

【0066】

一方、チェックの結果、認証サーバ２３の公開鍵証明書が存在し有効である場合（Ｙｅｓ）、及び、処理Ｓ２２乃至処理Ｓ２５を実行することによって新たに認証サーバ２３の公開鍵証明書を作成した場合には、認証サーバ２３は、認証サーバ２３の暗号鍵ペアを用いて自動設定装置１１の公開鍵証明書を作成する。即ち、認証サーバ２３は、認証サーバ

２３の秘密鍵を用いて自動設定装置の公開鍵にデジタル署名を行う。さらに、言い換えれば、認証サーバ２３は、認証サーバ２３の秘密鍵で自動設定装置１１の公開鍵に認証サーバ２３の署名を付加する（Ｓ２６）。次に、認証サーバ２３は、作成した自動設定装置１１の公開鍵証明書を自動設定装置識別子に対応付けてリポジトリ１０５に登録する（Ｓ２７）。即ち、自動設定装置１１の公開鍵証明書におけるシリアル番号、デジタル証明書のアルゴリズム、公開鍵におけるアルゴリズム、年月日時分秒で表される有効期間の開始時期、年月日時分秒で表される有効期間の終了時期、公開鍵、公開鍵証明書の規格のバージョン、証明書の発行者、証明書の所有者、認証サーバ２３よる署名が含まれた公開鍵証明書を自動設定装置識別子（暗号鍵ペア所有者）に対応付けてリポジトリ１０５に登録する。

【0067】

このように自動設定装置１１、登録サーバ２２及び認証サーバ２３が動作することによって、自動設定装置１１が生成した暗号鍵ペアの公開鍵に対し、認証サーバ２３による公開鍵証明書が発行される。

【0068】

そして、図８に戻って、自動設定装置１１がその公開鍵証明書の交付を望む場合には、自動設定装置１１が当該自動設定装置１１の自動設定装置識別子、及び、自動設定装置１１の公開鍵証明書の交付を要求する旨の情報を収容した通信信号（交付要求信号）を認証サーバ２３に送信し（Ｓ１８）、この交付要求信号を認証サーバ２３が受信すると、認証サーバ２３は、交付要求信号に収容されている自動設定装置識別子に基づいてリポジトリ１０５を検索し、検索結果に基づいて、自動設定装置１１の公開鍵証明書を収容した通信信号（交付信号）を自動設定装置１１に送信する（Ｓ１９）。自動設定装置１１の公開鍵証明書管理部６４は、認証サーバ２３から自動設定装置１１の公開鍵証明書を収容するこの通信信号を受信すると、自動設定装置１１の公開鍵証明書の記憶処理を行う（Ｓ２０）。

【0069】

この自動設定装置の公開鍵証明書の記憶処理についてより詳細に説明すると、図１０において、自動設定装置１１の公開鍵証明書管理部６４は、認証サーバ２３の公開鍵で自動設定装置１１の公開鍵証明書を検証する（Ｓ３１）。自動設定装置１１の公開鍵証明書管理部６４は、この処理Ｓ３１の検証で得られた自動設定装置１１の公開鍵と図８の処理Ｓ１１で生成した自動設定装置の公開鍵とを比較し、一致するか否かを判断する（Ｓ３２）。判断の結果、自動設定装置１１の公開鍵証明書管理部６４は、一致しない場合（不一致）には、図８の処理Ｓ１１からの公開鍵証明書取得処理をやり直し（Ｓ３４）、一致する場合（一致）には、この自動設定装置１１の公開鍵証明書が有効であるか否かを判断する（Ｓ３３）。判断の結果、自動設定装置１１の公開鍵証明書管理部６４は、有効ではない場合（Ｎｏ）には処理Ｓ３４を実行し、一方、有効である場合（Ｙｅｓ）には自身の自動設定装置１１の公開鍵証明書を記憶する（Ｓ３５）。

【0070】

このような動作を行うことによって、自動設定装置１１は、自動設定装置１１の公開鍵証明書を認証サーバ２３から取得することができる。ここで、このような公開鍵証明書取得処理を自動設定装置１１の起動時に行うように構成することによって、暗号鍵ペアの生成がその都度行われることになるから、セキュリティを向上させることができる。なお、本実施形態では、自動設定装置１１から交付要求信号の受信を待って認証サーバ２３は、自動設定装置１１の公開鍵証明書を交付しているが、自動設定装置１１の公開鍵証明書を発行した場合に直ちに交付するように構成してもよい。

【0071】

ここで、認証サーバ２３は、登録サーバ２２から発行要求信号を受信することによって実行される自動設定装置１１の公開鍵に対する公開鍵証明書の発行処理において、認証サーバ２３の公開鍵証明書の存在や有効性をチェックしているが、認証サーバ２３の公開鍵証明書における有効性のチェックは、定期的にも行われており、有効ではない場合には認

証サーバ２３の公開鍵証明書を更新している。このような定期的に行われる認証サーバ２３の公開鍵証明書を更新する認証サーバの公開鍵証明書に対する更新処理について説明する。

【0072】

図１１は、認証サーバの公開鍵証明書に対する更新処理における動作を示すシーケンス図である。図１２は、認証サーバの公開鍵証明書に対する更新処理における動作を示すフローチャートである。

【0073】

図１１において、認証サーバ２３の公開鍵証明書に対する更新処理を行う時期になると、認証サーバ２３は、同期をとるべく、ＮＴＰサーバ２４に日付と時刻とを要求する旨の情報を収容する通信信号（時刻要求信号）を送信する（Ｓ４１）。ＮＴＰサーバ２４は、時刻要求信号を受信すると、現在の日付と時刻とを収容した通信信号（時刻返信信号）を認証サーバ２３に返信する（Ｓ４２）。

【0074】

認証サーバ２３は、時刻返信信号を受信すると、この信号に収容されている日付と時刻とで内部の時計を合わせて同期をとり、認証サーバ２３の公開鍵証明書に対する更新処理を行う（Ｓ４３）。

【0075】

この認証サーバ２３の公開鍵証明書に対する更新処理についてさらに詳細に説明すると、図１２において、認証サーバ２３は、まず、認証サーバ公開鍵証明書記憶部を参照することによって、認証サーバ２３の公開鍵証明書が有効か否かを判断する（Ｓ５１）。この有効性のチェックは、当該認証サーバ２３の公開鍵証明書が有効期限内であるか否か、及び、証明書破棄リストに載っているか否かを判断することによって行われる。

【0076】

判断の結果、有効ではない場合（Ｎｏ）には、認証サーバ２３は、暗号鍵ペアの生成処理を行い（Ｓ５２）、認証サーバ２３の公開鍵証明書の作成処理を行い（Ｓ５３）、認証サーバ２３の公開鍵証明書の記憶処理を行い（Ｓ５４）、新たに作成した認証サーバ２３の公開鍵の配布処理を行って（Ｓ５５）、処理を終了する。これら処理Ｓ５２乃至処理Ｓ５５は、図９を用いて説明した処理Ｓ２２乃至処理Ｓ２５と同様であるので、その説明を省略する。一方、判断の結果、有効である場合（Ｙｅｓ）には、認証サーバ２３は、処理を終了する。

【0077】

このように動作することによって、認証サーバ２３は、ＮＴＰサーバ２４の時刻と同期をとってネットワーク１内の各ノードと同期をとることにより、認証サーバ２３の公開鍵証明書の有効性を適切に判断することができる。また、認証サーバ２３は、認証サーバ２３の公開鍵証明書が有効ではない場合には、新たな認証サーバ２３の公開鍵証明書を取得して認証サーバ２３の公開鍵証明書に対する更新が行われる。

【0078】

次に、認証サーバ２３を用いたトンネルを自動的に設定するトンネル自動設定処理について説明する。トンネル自動設定処理は、他の自動設定装置１１と情報交換するためにトンネルを自動的に設定するために必要な情報を情報サーバ２１に登録する初期処理、トンネルを自動的に設定するトンネル構築処理、及び、トンネルを自動的に削除するトンネル削除処理から構成される。

【0079】

図１３は、トンネル自動設定処理における初期処理の動作を示すシーケンス図である。図１４乃至図１８は、トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その１乃至その５）である。図１９は、トンネル自動設定処理におけるトンネル構築処理の動作を示すフローチャートである。図２０は、自動設定装置の公開鍵証明書に対する更新処理における動作を示すシーケンス図である。図２１は、自動設定装置の公開鍵証明書における使用可能性判断処理の動作を示すフローチャートである。

【0080】
まず、トンネル自動設定処理の初期処理について説明する。図１３において、例えば、自動設定装置１１の電源が投入され、ＩＰｓｅｃ設定情報及び６ｏ４トンネルの接続先の自動設定装置１１における自動設定装置識別子が入力部５４から入力されると、自動設定装置１１の制御部５２におけるトンネル設定部６２は、ＩＳＰネットワーク３に接続要求を送信する（Ｓ６１）。ＩＳＰネットワーク３において、ＩＳＰコンピュータは、接続要求を受けると、ＤＨＣＰサーバ２６を用いて自動設定装置１１にＩＰｖ４アドレスを割り振り、この割り振ったＩＰｖ４アドレスやデフォルト経路情報等のインターネット接続サービスを提供するために必要な情報を自動設定装置１１に送信し、インターネット接続サービスを開始する（Ｓ６２）。
【0081】
次に、自動設定装置１１のトンネル設定部６２は、ＩＳＰネットワーク３のインターネット接続サービスを利用し、トンネル設定用情報記憶部７１における情報サーバ２１のＩＰアドレスを用いて情報サーバ２１にアクセスし、自動設定装置識別子、トンネル外部ＩＰアドレス、及び、これら情報を提供トンネル設定情報テーブル１０２に登録を要求する旨の情報を収容する通信信号（トンネル外部ＩＰアドレス設定情報信号）を作成して情報サーバ２１に送信する（Ｓ６３）。トンネル外部ＩＰアドレスは、処理Ｓ６２でＤＨＣＰサーバ２６によって割り振られたＩＰｖ４アドレスである。情報サーバ２１は、トンネル設定情報信号を受信すると、新たなレコードを作成し、トンネル外部ＩＰアドレス設定情報信号に収容されている自動設定装置識別子及びトンネル外部ＩＰアドレスを提供トンネル設定情報テーブル１０２に登録する（Ｓ６４）。
【0082】
このように動作することによって６ｏ４トンネルの設定に必要なトンネル外部ＩＰアドレスが割り当てられ、割り当てられたトンネル外部ＩＰアドレスが情報サーバ２１に登録され、集中的に一括管理される。特に、ダイヤルアップ接続等の場合のように、６ｏ４トンネルを設定するたびにトンネル外部ＩＰアドレスが変更される場合にも対応することができる。
【0083】
次に、自動設定装置１１のトンネル設定部６２は、当該自動設定装置１１におけるＬＡＮ側インターフェース部５１のＩＰｖ６アドレスを割り振るべく、トンネル内部ＩＰアドレス生成部６３を用いて所定の手順に従って自動設定装置識別子よりＩＰｖ６アドレス（トンネル内部ＩＰアドレス）を作成する（Ｓ６５）。
【0084】
ＩＰｖ６アドレスを生成する所定の手順は、重複しないグローバル・アドレスであればどのような手順でもよいが、本実施形態では、自動設定装置識別子がＩＰｖ６アドレス生成情報であるので、ＩＰｖ６アドレスの作成は、例えば、生成するＩＰｖ６アドレスのネットワーク・プレフィックスに自動設定装置識別子に含まれるＩＰｖ６アドレス生成情報のネットワーク・プレフィックスをそのまま使用し、さらにインターフェースＩＤ付加することよってＩＰｖ６アドレスを生成する。インタフェースＩＤはネットワーク２に繋がる他の機器のインターフェースＩＤと重複しなければどのようなインターフェースＩＤを用いても良いが、本実施形態では、ＬＡＮ側インターフェース部５１に割り振るＩＰｖ６アドレスに含まれるインターフェースＩＤは、全て０としている。
【0085】
次に、自動設定装置１１のトンネル設定部６２は、トンネル内部ＩＰアドレス生成部６３により生成されたＩＰｖ６アドレスをＬＡＮ側インターフェース部５１のＩＰアドレス（トンネル内部ＩＰアドレス）として設定する（Ｓ６６）。
【0086】
次に、自動設定装置１１のトンネル設定部６２は、ルータ装置（本実施形態では自動設定装置１１）が配下のホストコンピュータにネットワーク・プレフィックスを通知するルータ広告（Router Advertisement）を行うＲＡデーモンを起動する（Ｓ６７）。次に、自

動設定装置１１のトンネル設定部６２は、ＩＫＥ（Internet Key Exchange）を行うＩＫＥデーモンを起動する（Ｓ６８）。ＩＫＥは、ＩＰｓｅｃの設定に用いられ、ＳＡ（Security Association）の生成と管理を行うプロトコルである。そして、自動設定装置１１のトンネル設定部６２は、トンネル構築処理を行う（Ｓ６９）。

【0087】

次に、トンネル自動設定処理のトンネル構築処理について説明する。図１４乃至図１８において、接続元の自動設定装置１１の制御部５２におけるトンネル設定部６２は、自動設定装置１１の公開鍵証明書を更新する更新処理を行う（Ｓ１０１）。このように自動設定装置１１は、更新処理を行うので、セキュリティを向上させることができ、また、有効な公開鍵証明書によって６０４トンネルの自動設定を続行することができる。

【0088】

この自動設定装置１１の公開鍵証明書に対する更新処理についてより詳細に説明する。図２０において、自動設定装置１１のトンネル設定部６２は、制御部５２における時計部６６を用いて、同期をとるべく、ＮＴＰサーバ２４に日付と時刻とを要求する旨の情報を収容した時刻要求信号を送信する（Ｓ２０１）。ＮＴＰサーバ２４は、時刻要求信号を受信すると、現在の日付と時刻とを収容した時刻返信信号を自動設定装置１１に返信する（Ｓ２０２）。自動設定装置１１の時計部６６は、時刻返信信号を受信すると、この信号に収容されている日付と時刻とで内部の時計を合わせる（Ｓ２０３）。

【0089】

このように動作することによって自動設定装置１１は、時計部６６の時計をＮＴＰサーバ２４の日付及び時刻に合わせるので、例えば、バックアップ電源を持たない自動設定装置１１の電源が落とされたり、時計の精度が悪かったりしたために、自動設定装置１１の時計が狂っている場合でも、自動設定装置１１は、認証サーバ２３と現在時刻の同期をとることができる。このため、認証サーバ２３の公開鍵証明書の有効性や自動設定装置１１の公開鍵証明書の有効性を適切に判断することができる。

【0090】

次に、自動設定装置１１のトンネル設定部６２は、認証サーバ２３の公開鍵証明書の交付を要求する旨の情報を収容した通信信号（認証サーバ公開鍵証明書交付要求信号）を作成して認証サーバ２３に送信する（Ｓ２０４）。認証サーバ２３は、認証サーバ公開鍵証明書交付要求信号を受信すると、認証サーバ公開鍵証明書記憶部に記憶されている認証サーバ２３の公開鍵証明書を収容した通信信号（認証サーバ公開鍵証明書交付信号）を作成して自動設定装置１１に返信する（Ｓ２０５）。

【0091】

自動設定装置１１のトンネル設定部６２は、認証サーバ公開鍵証明書交付信号を受信すると、この信号に収容されている認証サーバ２３の公開鍵証明書が有効か否かを判断する（Ｓ２０６）。この有効か否かの判断は、時計部６６の時刻が、取得した認証サーバ２３の公開鍵証明書に記載されている有効期間内であるか否かを判断することによって行われ、有効期間内である場合に有効と判断される。有効ではない場合には、一定時間経過後、再度処理Ｓ２０１から実施する。

【0092】

次に、自動設定装置１１のトンネル設定部６２は、制御部５２の公開鍵証明書管理部６４を用いて、自動設定装置１１の公開鍵証明書の使用可能性を判断する使用可能性判断処理を行って（Ｓ２０７）、更新処理を終了し、トンネル構築処理における後述の処理Ｓ１０２を行う。

【0093】

この自動設定装置１１の公開鍵証明書における使用可能性判断処理についてより詳細に説明すると、図２１において、自動設定装置１１の公開鍵証明書管理部６４は、セキュリティ情報記憶部７２に自動設定装置１１の公開鍵証明書が存在するか否かを判断する（Ｓ２１１）。

【0094】

判断の結果、自動設定装置１１の公開鍵証明書が存在しない場合（Ｎｏ）には、自動設定装置１１の公開鍵証明書管理部６４は、認証サーバ２３から当該自動設定装置１１の公開鍵証明書を取得すべく、当該自動設定装置１１の自動設定装置識別子及び自動設定装置１１の公開鍵証明書の交付を要求する旨の情報を収容した交付要求信号を認証サーバ２３に送信する（Ｓ２１２）。自動設定装置１１の公開鍵証明書管理部６４は、自動設定装置１１の公開鍵証明書を収容した交付返信信号の返信を認証サーバ２３から受信して交付を受けると（Ｓ２１３）、処理Ｓ２１４を実行する。一方、判断の結果、自動設定装置１１の公開鍵証明書が存在する場合（Ｙｅｓ）も自動設定装置１１の公開鍵証明書管理部６４は、処理Ｓ２１４を実行する。

【0095】

処理Ｓ２１４において、自動設定装置１１の公開鍵証明書管理部６４は、自動設定装置１１の公開鍵証明書が有効か否かを判断する。この有効か否かの判断は、当該自動設定装置１１の公開鍵証明書が有効期限内であるか否か、及び、証明書破棄リストに載っているか否かを判断することによって行われる。

【0096】

判断の結果、有効ではない場合（Ｎｏ）には、自動設定装置１１の公開鍵証明書管理部６４は、図８を用いて説明した上述の公開鍵証明書取得処理を行って（Ｓ２１５）、トンネル構築処理を続行する。一方、判断の結果、有効である場合（Ｙｅｓ）にも自動設定装置１１の公開鍵証明書管理部６４は、トンネル構築処理を続行する（Ｓ２１６）。

【0097】

このように接続元の自動設定装置１１の制御部５２におけるトンネル設定部６２が動作することによって、接続元の自動設定装置１１の公開鍵証明書を更新する更新処理が行われる。

【0098】

図１４乃至図１８に戻って、接続元の自動設定装置１１の制御部５２におけるトンネル設定部６２は、トンネル設定用情報記憶部７１の情報サーバ２１のＩＰアドレスを用いて情報サーバ２１に接続し、接続先の自動設定装置１１の自動設定装置識別子及び接続先の自動設定装置１１のトンネル外部ＩＰアドレスを要求する旨の情報を収容した通信信号（接続先トンネル外部ＩＰアドレス要求信号）を作成して情報サーバ２１に送信する（Ｓ１０２）。情報サーバ２１は、この接続先トンネル外部ＩＰアドレス要求信号を受信すると、この信号に収容されている自動設定装置識別子に基づいて提供トンネル設定情報テーブル１０２からこの自動設定装置識別子に対応するトンネル外部ＩＰアドレスを検索する（Ｓ１０３）。そして、情報サーバ２１は、自動設定装置識別子、及び、検索したこの自動設定装置識別子に対応するトンネル外部ＩＰアドレスを収容した通信信号（接続先トンネル外部ＩＰアドレス返信信号）を作成して自動設定装置１１に返信する（Ｓ１０４）。ここで、情報サーバ２１は、処理Ｓ１０２で、接続先トンネル外部ＩＰアドレス要求信号に収容されていた自動設定装置識別子が提供トンネル設定情報テーブル１０２にない場合には、自動設定装置識別子に対応するトンネル外部ＩＰアドレスがない旨を示す情報（無登録情報）を接続先トンネル外部ＩＰアドレス返信信号に収容して自動設定装置１１に返信する。無登録情報は、例えば、「＊＊＊＊」や「ｖａｃａｎｔ」や「Ｎｕｌｌ」等の記号列によって表される。

【0099】

次に、接続元の自動設定装置１１におけるトンネル設定部６２は、接続先トンネル外部ＩＰアドレス返信信号を受信すると、この信号に収容されていた接続先のトンネル外部ＩＰアドレスが有効であるか否かを判断する（Ｓ１０５）。この有効であるか否かの判断は、接続先のトンネル外部ＩＰアドレスの代わりに無登録情報が接続先トンネル外部ＩＰアドレス返信信号に収容されていたか否かを判断することによって行われ、無登録情報ではない場合には、有効と判断され、無登録情報である場合には有効ではないと判断する。

【0100】

判断の結果、有効ではない場合には、接続先の自動設定装置１１が図１３を用いて説明

した初期処理を実行していないと判断し、一定時間の経過後に、処理Ｓ１０２に処理が戻され、有効である場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、例えばスリーウェイハンドシェイク（Three Way Handshake）によって接続先の自動設定装置１１とコネクションを確立し、接続先の自動設定装置と通信可能に接続する（Ｓ１０６）。スリーウェイハンドシェイクは、送信元のホストコンピュータ（本実施形態では接続元の自動設定装置）が通信開始の要求を送信先のホストコンピュータ（本実施形態では接続先の自動設定装置）に送信し（第１ステップ）、送信先のホストコンピュータが通信がＯＫであれば確認応答を返信し（第２ステップ）、そして、送信元のホストコンピュータがコネクションの確立の通知を送信先のホストコンピュータに送信する（第３ステップ）ことによってコネクションを確立する手順である。

【0101】

接続先の自動設定装置１１の制御部５２におけるトンネル設定部６２は、自動設定装置１１の公開鍵証明書を更新する更新処理を行う（Ｓ１０７）。この更新処理は、図２０及び図２１を用いて説明した上述の更新処理と同様であるので、その説明を省略する。

【0102】

コネクションが確立すると、接続元の自動設定装置１１におけるトンネル設定部６２は、当該自動設定装置１１の自動設定装置識別子を収容する通信信号（自動設定装置識別子通知信号）を作成して接続先の自動設定装置１１に送信する（Ｓ１０８）。

【0103】

接続元の自動設定装置１１からこの自動設定装置識別子通知信号を受信すると、接続先の自動設定装置１１におけるトンネル設定部６２は、自身（接続先の自動設定装置１１）の自動設定装置識別子を収容する通信信号（自動設定装置識別子通知信号）を作成して接続元の自動設定装置１１に送信する（Ｓ１０９）。

【0104】

次に、接続元と接続先の自動設定装置１１はそれぞれ他方の自動設定装置１１の公開鍵証明書を入手し、入手した他方の動設定装置１１の公開鍵証明書が真正であるか否かをチェックするが、この公開鍵証明書の入手方法は、２通りある。

【0105】

まず初めに、接続元と接続先の自動設定装置１１において認証サーバから他方の自動設定装置１１の公開鍵証明書を入手する方法について説明する。

【0106】

接続先の自動設定装置１１におけるトンネル設定部６２は、接続元の自動設定装置１１における自動設定装置識別子、及び、接続元の自動設定装置１１における公開鍵証明書の交付を要求する旨の情報を収容した通信信号（交付要求信号）を作成して認証サーバ２３に送信する（Ｓ１１０）。

【0107】

この交付要求信号を受信すると認証サーバ２３は、受信した交付要求信号の自動設定装置識別子に基づいてリポジトリ１０５を参照し、この接続元の自動設定装置１１における自動設定装置識別子に対応する自動設定装置１１の公開鍵証明書を検索する（Ｓ１１１）。認証サーバ２３は、検索した接続元の自動設定装置１１の公開鍵証明書を収容する通信信号（交付信号）を作成して接続先の自動設定装置１１に返信する（Ｓ１１２）。

【0108】

この交付信号を受信すると、接続先の自動設定装置１１におけるトンネル設定部６２は、認証サーバ２３の公開鍵証明書を用いて接続元の自動設定装置１１の公開鍵証明書が真正であるか否か検証する（Ｓ１１３）。

【0109】

さらに、接続先の自動設定装置１１からこの自動設定装置識別子通知信号を受信する（Ｓ１０９）と、接続元の自動設定装置１１におけるトンネル設定部６２は、接続先の自動設定装置１１における自動設定装置識別子、及び、接続先の自動設定装置１１における公開鍵証明書を要求する旨の情報を収容した通信信号（交付要求信号）を作成して認証サー

バ２３に送信する（Ｓ１１４）。

【0110】

この交付要求信号を受信すると認証サーバ２３は、受信した交付要求信号の自動設定装置識別子に基づいてリポジトリ１０５を参照し、この接続先の自動設定装置１１における自動設定装置識別子に対応する自動設定装置１１の公開鍵証明書を検索する（Ｓ１１５）。認証サーバ２３は、検索した接続先の自動設定装置１１の公開鍵証明書を収容する通信信号（交付信号）を作成して接続元の自動設定装置１１に返信する（Ｓ１１６）。

【0111】

この交付信号を受信すると、接続元の自動設定装置１１におけるトンネル設定部６２は、認証サーバ２３の公開鍵証明書を用いて接続先の自動設定装置１１の公開鍵証明書が真正であるか否か検証する（Ｓ１１７）。

【0112】

次に、接続元と接続先の自動設定装置１１において互いに自動設定装置１１の公開鍵証明書を交換することで他方の公開鍵証明書を入手する方法について説明する。

【0113】

接続元の自動設定装置１１におけるトンネル設定部６２は、自身（接続元の自動設定装置１１）の自動設定装置１１の公開鍵証明書を収容した通信信号（公開鍵証明書通知信号）を作成して接続先の自動設定装置１１に送信する（Ｓ１１８）。

【0114】

この公開鍵証明書通知信号を接続元の自動設定装置１１から受信した接続先の自動設定装置１１におけるトンネル設定部６２は、この受信した公開鍵証明書通知信号に収容されている接続元の自動設定装置１１の公開鍵証明書を認証サーバ２３の公開鍵証明書を用いて真正であるか否か検証する（Ｓ１１９）。そして、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１１８で検証した結果を判断することによって、接続元の自動設定装置１１の公開鍵証明書が真正な自動設定装置１１の公開鍵証明書であるか否かを判断する（Ｓ１２０）。本実施形態では、認証サーバ２３の公開鍵証明書は、セルフ署名であるので、このような処理Ｓ１２０を行うことによって自動設定装置１１の公開鍵の信頼性を向上させている。

【0115】

接続先の自動設定装置１１におけるトンネル設定部６２は、接続元の自動設定装置１１に判断結果を収容した通信信号（判断結果通知信号）を作成して送信し（Ｓ１２１）、判断の結果、真正な公開鍵証明書ではない場合には、接続元の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、真正な公開鍵証明書である場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、自身（接続先の自動設定装置１１）の自動設定装置１１の公開鍵証明書を収容した通信信号（公開鍵証明書通知信号）を接続元の自動設定装置１１に送信する（Ｓ１２２）。

【0116】

この公開鍵証明書通知信号を接続先の自動設定装置１１から受信した接続元の自動設定装置１１におけるトンネル設定部６２は、この受信した公開鍵証明書通知信号に収容されている接続先の自動設定装置１１の公開鍵証明書を認証サーバ２３の公開鍵証明書を用いて真正であるか否か検証する（Ｓ１２３）。そして、接続元の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１２３で検証した結果を判断することによって、接続先の自動設定装置１１の公開鍵証明書が真正な自動設定装置１１の公開鍵証明書であるか否かを判断する（Ｓ１２４）。

【0117】

接続元の自動設定装置１１におけるトンネル設定部６２は、接続先の自動設定装置１１に判断結果を収容した通信信号（判断結果通知信号）を作成して送信し（Ｓ１２５）、判断の結果、真正な公開鍵証明書ではない場合には、接続先の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、真正な公開鍵証明書である場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、ラン

ダムにチャレンジ文字列を生成する（Ｓ１２６）。そして、接続元の自動設定装置１１は、生成したチャレンジ文字列を収容する通信信号（チャレンジ文字列通知信号）を作成して接続先の自動設定装置１１に送信する（Ｓ１２７）。

【0118】

接続先の自動設定装置１１におけるトンネル設定部６２は、チャレンジ文字列通知信号を受信すると、この信号に収容されているチャレンジ文字列を自動設定装置１１との間で予め取り決められた所定の演算方法によって演算し、演算結果を自身（接続先の自動設定装置１１）の自動設定装置１１の秘密鍵（接続先の自動設定装置１１の秘密鍵）で暗号化することによってレスポンス文字列を生成する（Ｓ１２８）。この所定の演算方法は、どのような演算方法でもよいが、例えば、本実施形態では、一方向ハッシュ関数（one-way hash function）である。従って、接続先の自動設定装置１１におけるトンネル設定部６２は、チャレンジ文字列のハッシュ値を求め、求めたハッシュ値を自身の自動設定装置１１の秘密鍵で暗号化することによってレスポンス文字列を生成する。次に、接続先の自動設定装置１１におけるトンネル設定部６２は、レスポンス文字列を収容する通信信号（レスポンス文字列通知信号）を作成して接続元の自動設定装置１１に送信する（Ｓ１２９）。

【0119】

接続元の自動設定装置１１におけるトンネル設定部６２は、レスポンス文字列通知信号を受信すると、処理Ｓ１２６で生成したチャレンジ文字列を上述の所定の演算方法によって演算した演算結果と、この信号に収容されているレスポンス文字列を接続先の自動設定装置１１の公開鍵証明書に含まれる接続先の自動設定装置１１の公開鍵で復号化した復号結果とを比較し、一致するか否かを判断する（Ｓ１３０）。

【0120】

接続元の自動設定装置１１におけるトンネル設定部６２は、接続先の自動設定装置１１に判断結果を収容した通信信号（判断結果通知信号）を作成して送信し（Ｓ１３１）、判断の結果、一致しない場合には、接続先の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、一致する場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、後述の処理を継続する。

【0121】

判断結果通知信号を受信すると、接続先の自動設定装置１１におけるトンネル設定部６２は、ランダムにチャレンジ文字列を生成し（Ｓ１３２）、生成したチャレンジ文字列を収容するチャレンジ文字列通知信号を作成して接続元の自動設定装置１１に送信する（Ｓ１３３）。

【0122】

接続元の自動設定装置１１におけるトンネル設定部６２は、このチャレンジ文字列通知信号を受信すると、この信号に収容されているチャレンジ文字列を上述の所定の演算方法によって演算し、演算結果を自身の自動設定装置１１の秘密鍵（接続先の自動設定装置１１の秘密鍵）で暗号化することによってレスポンス文字列を生成する（Ｓ１３４）。次に、接続元の自動設定装置１１におけるトンネル設定部６２は、レスポンス文字列を収容するレスポンス文字列通知信号を作成して接続先の自動設定装置１１に送信する（Ｓ１３５）。

【0123】

接続先の自動設定装置１１におけるトンネル設定部６２は、レスポンス文字列通知信号を受信すると、処理Ｓ１３２で生成したチャレンジ文字列を上述の所定の演算方法によって演算した演算結果と、この信号に収容されているレスポンス文字列を接続元の自動設定装置１１の公開鍵証明書に含まれる接続元の自動設定装置１１の公開鍵で復号化した復号結果とを比較し、一致するか否かを判断する（Ｓ１３６）。接続先の自動設定装置１１におけるトンネル設定部６２は、接続元の自動設定装置１１に判断結果を収容した判断結果通知信号を作成して送信し（Ｓ１３７）、判断の結果、一致しない場合には、接続元の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、

判断の結果、一致する場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、後述の処理を継続する。

【0124】

このように本実施形態では、暗号鍵ペアをパスワードに見立ててチャレンジ・レスポンス認証技術を利用している。

【0125】

以上の処理Ｓ１０１乃至処理Ｓ１３７を実行することによって接続元の自動設定装置１１と接続先の自動設定装置１１は、第三者機関である認証サーバ２３を用いて相互認証を行う。

【0126】

相互認証に成功すると、接続元の自動設定装置１１におけるトンネル設定部６２及び接続先の自動設定装置１１におけるトンネル設定部６２は、６０４トンネルの設定に必要な情報を互いに交換する。即ち、接続元の自動設定装置１１におけるトンネル設定部６２は、自身の自動設定装置１１におけるトンネル外部ＩＰアドレス、トンネル内部ＩＰアドレスとそのプレフィックス長、ＩＰｓｅｃ設定情報、及び、トンネルの構築を指示する旨の情報を収容した通信信号（トンネル構築指示信号）を作成して接続先の自動設定装置１１に送信し（Ｓ１３８）、一方、接続先の自動設定装置１１におけるトンネル設定部６２は、自身の自動設定装置１１におけるトンネル外部ＩＰアドレス、トンネル内部ＩＰアドレスとそのプレフィックス長、ＩＰｓｅｃ設定情報、及び、トンネルの構築を指示する旨の情報を収容した通信信号（トンネル構築指示信号）を作成して接続元の自動設定装置１１に送信する（Ｓ１３９）。ここで、トンネル内部ＩＰアドレスとそのプレフィックス長は、ＩＰｓｅｃのセキュリティポリシを設定するために必要となる情報である。

【0127】

接続元の自動設定装置１１におけるトンネル設定部６２は、記憶している情報によって６０４トンネルを設定できるか否かを判断する（Ｓ１４０）。このトンネル設定の可否の判断は、接続元のトンネル外部アドレス、接続元のトンネル内部ＩＰアドレス、接続先のトンネル外部ＩＰアドレス、接続先のトンネル内部ＩＰアドレス及びＩＰｓｅｃ設定情報の有無であり、これら情報がある場合には６０４トンネルの設定が可能と判断され、これら情報のうち何れかかが欠けている場合には６０４トンネルの設定が不能と判断される。判断の結果、不能と判断された場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続先の自動設定装置１１に送信し（Ｓ１４９）、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、可能と判断された場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続先の自動設定装置１１に送信する（Ｓ１４１）。

【0128】

一方、接続先の自動設定装置１１におけるトンネル設定部６２は、記憶している情報によって６０４トンネルを設定できるか否かを判断する（Ｓ１４２）。判断の結果、不能と判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続元の自動設定装置１１に送信し（Ｓ１５５）、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、可能と判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続元の自動設定装置１１に送信する（Ｓ１４３）。

【0129】

他方の自動設定装置１１から６０４トンネルの設定が可能であると判断した旨の判断結果を収容する判断結果通知信号を受信すると、接続元及び接続先の自動設定装置１１におけるトンネル設定部６２は、コネクションを解消する処理をそれぞれ行う（Ｓ１４４）。コネクションが解消されると、接続元の自動設定装置１１におけるトンネル設定部６２及び接続先の自動設定装置１１におけるトンネル設定部６２は、６０４トンネルを構築する

トンネル構築処理をそれぞれ行う（Ｓ１４５、Ｓ１４６）。

【0130】

このトンネル構築処理についてより詳細に説明すると、図１９において、自動設定装置１１の制御部５２におけるトンネル設定部６２は、所定の手順に従って自動的に設定しようとしている６ｏ４トンネルのトンネル名を生成する（Ｓ１５１）。

【0131】

トンネル名を生成する所定の手順は、例えば、順に数値を割り振る手順や順にアルファベットを割り振る手順のように、重複してトンネル名が生成されなければどのような手順でもよいが、本実施形態では、トンネルの種類を示すＩＰｖ６ｏｖｅｒＩＰｖ４トンネルを略称した「６ｏ４」にアルファベットを順に付する手順である。

【0132】

次に自動設定装置１１の制御部５２におけるトンネル設定部６２は、トンネル構築指示信号に収容されているＩＰｓｅｃ設定情報を参照することによってＩＰｓｅｃを設定するか否かを判断する（Ｓ１５２）。判断の結果、ＩＰｓｅｃを設定しない場合（非設定）には、自動設定装置１１のトンネル設定部６２は、後述の処理Ｓ１５５を実行する。

【0133】

一方、判断の結果、ＩＰｓｅｃを設定する場合（設定）には、自動設定装置１１のトンネル設定部６２は、構築するトンネルについてＩＰパケットの処理方法を規定するセキュリティポリシ（Security Policy）を設定する（Ｓ１５３）。即ち、自動設定装置１１のトンネル設定部６２は、ＩＰパケットの処理方法とＩＰパケットを特定するための情報（セレクタ）とを対応付けて登録するセキュリティポリシデータベース（Security Policy Database、以下、「ＳＰＤ」と略記する。）を作成し、作成したＳＰＤを記憶部５３に記憶する。セレクタは、セキュリティポリシ番号、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号及びトランスポート層プロトコルであり、ＩＰパケットの処理方法を指定するポリシは、ＩＰパケットの処理方法(アクション)、セキュリティプロトコル、カプセル化モード、入出力の方向送、信元側セキュリティゲートウェイのＩＰアドレス及び宛先側セキュリティゲートウェイの宛先ＩＰアドレスである。ＩＰパケットの処理方法は、ＩＰパケットの破棄、ＩＰｓｅｃ不適用の通過及びＩＰｓｅｃ適用の通過である。これらは、構築するトンネルについて設定される。即ち、接続元の自動設定装置１１において、接続先の自動設定装置１１との間に、セキュリティポリシのうち入出力の方向がｏｕｔになるようなセキュリティポリシを設定する場合には、セキュリティポリシ番号には、順に番号が割り振られ、送信元ＩＰアドレスには、接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、宛先ＩＰアドレスには、処理Ｓ１３９で取得した接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、送信元ポート番号、宛先ポート番号、トランスポート層プロトコル、アクション、セキュリティプロトコル及びカプセル化モード（例えば本実施形態ではトンネルモードに固定されている。）には、自動設定装置１１の記憶部５３に予め記憶されたＩＰｓｅｃ関連情報に基づいて設定され、送信元側セキュリティゲートウェイのＩＰアドレスには、接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定され、宛先側セキュリティゲートウェイの宛先ＩＰアドレスには、処理Ｓ１０４で情報サーバ２１から取得した接続先トンネル外部ＩＰアドレス返信信号に収容されている接続先の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定される。ＩＰパケットの処理方法には、ＩＰｓｅｃ適用の通過が設定される。接続元の自動設定装置１１において、接続先の自動設定装置１１との間に、セキュリティポリシのうち入出力の方向がｉｎになるようなセキュリティポリシを設定する場合には、セキュリティポリシ番号には、順に番号が割り振られ、送信元ＩＰアドレスには、処理Ｓ１３９で取得した接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、宛先ＩＰアドレスには、接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、送信元ポート番号、宛先ポート番号、トランスポート層プロトコル、アクション、セキュリティプロトコル及びカプセル化モード（

例えば本実施形態ではトンネルモードに固定されている。）には、自動設定装置１１の記憶部５３に予め記憶されたＩＰｓｅｃ関連情報に基づいて設定され、送信元側セキュリティゲートウェイのＩＰアドレスには、処理Ｓ１０４で情報サーバ２１から取得した接続先トンネル外部ＩＰアドレス返信信号に収容されている接続先の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定され、宛先側セキュリティゲートウェイの宛先ＩＰアドレスには、接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定され、ＩＰパケットの処理方法には、ＩＰｓｅｃ適用の通過が設定される。一方、接続先の自動設定装置１１において、接続先の自動設定装置１１との間に、セキュリティポリシのうち入出力の方向がｏｕｔになるようなセキュリティポリシを設定する場合には、セキュリティポリシ番号には、順に番号が割り振られ、送信元ＩＰアドレスには、接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、宛先ＩＰアドレスには、処理Ｓ１３８で接続元の自動設定装置１１から送信された接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、送信元ポート番号、宛先ポート番号、トランスポート層プロトコル、アクション、セキュリティプロトコル及びカプセル化モード（例えば本実施形態ではトンネルモードに固定されている。）には、自動設定装置１１の記憶部５３に予め記憶されたＩＰｓｅｃ関連情報に基づいて設定され、送信元側セキュリティゲートウェイのＩＰアドレスには、接続先の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定され、宛先側セキュリティゲートウェイの宛先ＩＰアドレスには、トンネル構築処理において接続元の自動設定装置１１と接続先の自動設定装置１１の間に確立されているコネクション情報から取得された接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定される。ＩＰパケットの処理方法には、ＩＰｓｅｃ適用の通過が設定される。接続先の自動設定装置１１において、接続先の自動設定装置１１との間に、セキュリティポリシのうち入出力の方向がｉｎになるようなセキュリティポリシを設定する場合には、セキュリティポリシ番号には、順に番号が割り振られ、送信元ＩＰアドレスには、処理Ｓ１３８で取得した接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、宛先ＩＰアドレスには、接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスとそのプレフィックス長が設定され、送信元ポート番号、宛先ポート番号、トランスポート層プロトコル、アクション、セキュリティプロトコル及びカプセル化モード（例えば本実施形態ではトンネルモードに固定されている。）には、自動設定装置１１の記憶部５３に予め記憶されたＩＰｓｅｃ関連情報に基づいて設定され、送信元側セキュリティゲートウェイのＩＰアドレスには、トンネル構築処理において接続元の自動設定装置１１と接続先の自動設定装置１１の間に確立されているコネクション情報から取得された接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定され、宛先側セキュリティゲートウェイの宛先ＩＰアドレスには、接続先の自動設定装置１１におけるトンネル外部ＩＰアドレスが設定される。

【0134】

次に、自動設定装置１１のトンネル設定部６２は、セキュリティアソシエーション（Security Association、以下、「ＳＡ」と略記する。）を接続元から接続先及び接続先から接続元のそれぞれについて確立する（Ｓ１５４）。即ち、接続元から接続先へのＳＡ及び接続先から接続元へのＳＡのそれぞれについて、自動設定装置１１のトンネル設定部６２は、ＩＫＥを用いて暗号化アルゴリズムの提示、決定及び暗号鍵の交換等を行うネゴシエーションを実行してＳＡを決定し、決定したＳＡをセキュリティアソシエーションデータベース（Security Association Database、以下、「ＳＡＤ」と略記する。）に登録する。ＳＡＤは、記憶部５３に記憶される。なお、ＩＫＥを用いて提示される暗号化アルゴリズムは、ＤＥＳ－ＣＢＣ、３ＤＥＳ－ＣＢＣ、ＣＡＳＴ－１２８、ＲＣ－５、ＩＤＥＡ及びＢｌｏｗｆｉｓｈ等の共通鍵暗号方式である。

【0135】

次に、自動設定装置１１のトンネル設定部６２は、処理Ｓ１５１で生成したトンネル名、処理Ｓ１５３でＤＨＣＰサーバ２６によって割り振られたＩＰアドレス（接続元のトン

ネル外部ＩＰアドレス）、接続元トンネル内部ＩＰアドレス、入力部５４から入力され記憶部５３に記憶されている接続先自動設定装置識別子、処理１０３で情報サーバ２１から取得した接続先トンネル外部ＩＰアドレス、処理Ｓ１５１で生成した接続先トンネル内部ＩＰアドレス、入力部５４から入力され記憶部５３に記憶されているＩＰｓｅｃ設定情報、及び、設定済みを示す情報である「設定済み」を設定トンネル管理情報テーブル１０１の対応する各フィールドにそれぞれ登録する（Ｓ１５５）。

【0136】

そして、自動設定装置１１のトンネル設定部６２は、構築したトンネルが正常に使用可能か否かを判断する（Ｓ１５６）。判断の結果、自動設定装置１１は、正常に使用可能である場合（Ｙｅｓ）には６０４トンネルの運用を開始し（Ｓ１５７）、正常に使用可能ではない場合（Ｎｏ）には、処理Ｓ６１からトンネル自動設定処理を再びやり直す（Ｓ１５８）。例えば、自動設定装置１１のトンネル設定部６２は、構築した６０４トンネルにピング（Ping）を送信し、その返信が受信されるか否かによって判断する。ピングの返信が受信された場合には、構築した６０４トンネルが正常に使用可能に構築されたと判断され、ピングの返信が受信されない場合には、構築した６０４トンネルが正常に使用可能に構築されなかったと判断される。

【0137】

このような処理Ｓ１５１乃至処理Ｓ１５８を接続元の自動設定装置１１におけるトンネル設定部６２及び接続先の自動設定装置１１におけるトンネル設定部６２がそれぞれ実行することによって６０４トンネルが構築され、６０４トンネルを利用した通信が可能となる。

【0138】

そして、自動設定装置１１は、複数の６０４トンネルを設定する場合には、処理Ｓ６１乃至処理Ｓ６８の初期処理を実行した後に、処理Ｓ１０１乃至処理Ｓ１４６（処理Ｓ１５１乃至処理Ｓ１５５のトンネル構築処理を含む）のトンネル構築処理を各６０４トンネルごとに実行する。例えば、図１に示すように、自動設定装置１１－Ａが自動設定装置１１－Ｂ及び自動設定装置１１－Ｃとの間にそれぞれ６０４トンネルを設定する場合には、自動設定装置１１－Ａは、まず、処理Ｓ６１乃至処理Ｓ６８の初期処理を実行し、次に、自動設定装置１１－Ｂとの間で処理Ｓ１０１乃至処理Ｓ１４６のトンネル構築処理を実行して、６０４トンネル５－ＡＢを設定し、そして、自動設定装置１１－Ｃとの間で処理Ｓ１０１乃至処理Ｓ１４６のトンネル構築処理を実行して、６０４トンネル５－ＡＣを設定する。なお、自動設定装置１１－Ａは、６０４トンネル５－ＡＣを設定した後に、６０４トンネル５－ＡＢを設定してもよく、６０４トンネルを設定する順は、任意である。

【0139】

以上説明したように自動設定装置１１は、第三者機関を利用した相互認証を行った上で６０４トンネルを自動的に設定することができる。このため、なりすまし等の不正な意図しない自動設定装置１１との間に６０４トンネルを設定することが防止される。また、ＩＰｓｅｃが利用可能であるので、セキュリティの高い通信を行うことができる。

【0140】

そして、このＩＰｓｅｃの利用は、入力部５４から入力され設定トンネル管理情報テーブル１０１に６０４トンネルごとに登録されることにより、６０４トンネルごとに選択可能であるので、通信の内容に応じて必要な場合にＩＰｓｅｃを利用することができるから、通信を行う場合に、自動設定装置１１の情報処理量を軽減することができ、自動設定装置１１の負荷を軽減することができる。

【0141】

また、６０４トンネルの使用を終了する場合には、認証サーバ２３を用いたトンネルを自動的に切断するトンネル切断処理が実行される。

【0142】

次に、トンネル切断処理について説明する。図２２乃至図２６は、トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その１～その５）である。

【0143】
図２２乃至図２６において、切断元の自動設定装置１１の制御部５２におけるトンネル削除部６５は、まず、設定トンネル管理情報テーブル１０１における、切断しようとしている６０４トンネルに対応するレコードのトンネル設定状態情報フィールド１１９に６０４トンネルの切断中を示す情報である「切断中」を登録する（Ｓ３０３）。
【0144】
次に、切断元の自動設定装置１１のトンネル削除部６５は、自動設定装置１１の公開鍵証明書の有効性をチェックすべく、自動設定装置１１の公開鍵証明書を更新する更新処理を行う（Ｓ３０４）。この更新処理は、図２０及び図２１を用いて説明した上述の更新処理と同様であるので、その説明を省略する。
【0145】
次に、切断元の自動設定装置１１におけるトンネル削除部６５は、６０４トンネルの切断を開始する旨の情報を収容した通信信号（切断開始通知信号）を作成して切断先の自動設定装置１１へ送信する（Ｓ３０５）。
【0146】
切断開始通知信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は、自動設定装置１１の公開鍵証明書の有効性をチェックすべく、自動設定装置１１の公開鍵証明書を更新する更新処理を行う（Ｓ３０６）。この更新処理は、図２０及び図２１を用いて説明した上述の更新処理と同様であるので、その説明を省略する。そして、切断先の自動設定装置１１におけるトンネル削除部６５は、トンネルの切断開始を了承する旨の情報を収容した通信信号（切断了承通知信号）を作成して切断元の自動設定装置１１へ返信する（Ｓ３０７）。
【0147】
切断了承通知信号を受信すると、切断元の自動設定装置１１におけるトンネル削除部６５は、自動設定装置識別子通知信号を作成して切断先の自動設定装置１１に送信する（Ｓ３０８）。
【0148】
切断元の自動設定装置１１からこの自動設定装置識別子通知信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は、自身（切断先の自動設定装置１１）の自動設定装置識別子を収容する通信信号（自動設定装置識別子通知信号）を作成して切断元の自動設定装置１１に送信する（Ｓ３０９）。
【0149】
次に、切断元と切断先の自動設定装置１１は、それぞれ他方の自動設定装置１１の公開鍵証明書を入手し、入手した他方の動設定装置１１の公開鍵証明書が真正かチェックするが、この公開鍵証明書の入手方法は、２通りある。
【0150】
まず初めに、切断元と切断先の自動設定装置１１において認証サーバから他方の自動設定装置１１の公開鍵証明書を入手する方法について説明する。
【0151】
切断先の自動設定装置１１におけるトンネル削除部６５は、切断元の自動設定装置１１における公開鍵証明書の交付を受けるべく、交付要求信号を作成して認証サーバ２３に送信する（Ｓ３１０）。
【0152】
この交付要求信号を受信すると認証サーバ２３は、受信した交付要求信号の自動設定装置識別子に基づいてリポジトリ１０５を参照し、この切断元の自動設定装置１１における自動設定装置識別子に対応する自動設定装置１１の公開鍵証明書を検索する（Ｓ３１１）。認証サーバ２３は、検索結果に基づいて、交付信号を作成して切断先の自動設定装置１１に返信する（Ｓ３１２）。
【0153】
この交付信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は

、認証サーバ２３の公開鍵証明書を用いて切断元の自動設定装置１１の公開鍵証明書が真正であるか否か検証する（Ｓ３１３）。

【0154】

さらに、切断先の自動設定装置１１からこの自動設定装置識別子通知信号を受信する（Ｓ３０９）と、切断元の自動設定装置１１におけるトンネル削除部６５は、切断先の自動設定装置１１における公開鍵証明書の交付を受けるべく、交付要求信号を作成して認証サーバ２３に送信する（Ｓ３１４）。

【0155】

この交付要求信号を受信すると認証サーバ２３は、受信した交付要求信号の自動設定装置識別子に基づいてリポジトリ１０５を参照し、この切断先の自動設定装置１１における自動設定装置識別子に対応する自動設定装置１１の公開鍵証明書を検索する（Ｓ３１５）。認証サーバ２３は、検索結果に基づいて交付信号を作成して切断元の自動設定装置１１に返信する（Ｓ３１６）。

【0156】

この交付信号を受信すると、切断元の自動設定装置１１におけるトンネル削除部６５は、認証サーバ２３の公開鍵証明書を用いて切断先の自動設定装置１１の公開鍵証明書が真正であるか否か検証する（Ｓ３１７）。

【0157】

次に、切断元と切断先の自動設定装置１１において互いに自動設定装置１１の公開鍵証明書を交換することで他方の公開鍵証明書を入手する方法について説明する。

【0158】

切断元の自動設定装置１１におけるトンネル削除部６５は、自身（切断元の自動設定装置１１）の公開鍵証明書通知信号を作成して切断先の自動設定装置１１に送信する（Ｓ３１８）。

【0159】

この公開鍵証明書通知信号を切断元の自動設定装置１１から受信した切断先の自動設定装置１１におけるトンネル削除部６５は、この受信した公開鍵証明書通知信号に収容されている切断元の自動設定装置１１の公開鍵証明書を認証サーバ２３の公開鍵証明書を用いて真正であるか否かを検証する（Ｓ３１９）。そして、切断先の自動設定装置１１におけるトンネル削除部６５は、処理Ｓ３１９で検証した結果を判断することによって、切断元の自動設定装置１１の公開鍵証明書が真正な自動設定装置１１の公開鍵証明書であるか否かを判断する（Ｓ３２０）。

【0160】

切断先の自動設定装置１１におけるトンネル削除部６５は、切断元の自動設定装置１１に判断結果通知信号を作成して送信し（Ｓ３２１）、判断の結果、真正な公開鍵証明書ではない場合には、切断元の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、真正な公開鍵証明書である場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、自身（切断先の自動設定装置１１）の公開鍵証明書通知信号を切断元の自動設定装置１１に送信する（Ｓ３２２）。

【0161】

この公開鍵証明書通知信号を切断先の自動設定装置１１から受信した切断元の自動設定装置１１におけるトンネル削除部６５は、この受信した公開鍵証明書通知信号に収容されている切断先の自動設定装置１１の公開鍵証明書を認証サーバ２３の公開鍵証明書を用いて真正であるか否かを検証する（Ｓ３２３）。そして、切断元の自動設定装置１１におけるトンネル削除部６５は、処理Ｓ３２３で検証した結果を判断することによって、切断先の自動設定装置１１の公開鍵証明書が真正な自動設定装置１１の公開鍵証明書であるか否かを判断する（Ｓ３２４）。

【0162】

切断元の自動設定装置１１におけるトンネル削除部６５は、切断先の自動設定装置１１に判断結果通知信号を作成して送信し（Ｓ３２５）、判断の結果、真正な公開鍵証明書で

はない場合には、切断先の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、真正な公開鍵証明書である場合には、切断元の自動設定装置１１におけるトンネル削除部６５は、ランダムにチャレンジ文字列を生成する（Ｓ３２６）。そして、切断元の自動設定装置１１におけるトンネル削除部６５は、チャレンジ文字列通知信号を作成して切断先の自動設定装置１１に送信する（Ｓ３２７）。

【0163】

切断先の自動設定装置１１におけるトンネル削除部６５は、チャレンジ文字列通知信号を受信すると、この信号に収容されているチャレンジ文字列を自動設定装置１１との間で予め取り決められた所定の演算方法によって演算し、演算結果を自身（切断先の自動設定装置１１）の自動設定装置１１の秘密鍵（切断先の自動設定装置１１の秘密鍵）で暗号化することによってレスポンス文字列を生成する（Ｓ３２８）。次に、切断先の自動設定装置１１におけるトンネル削除部６５は、レスポンス文字列通知信号を作成して切断元の自動設定装置１１に送信する（Ｓ３２９）。

【0164】

切断元の自動設定装置１１におけるトンネル削除部６５は、レスポンス文字列通知信号を受信すると、処理Ｓ３２６で生成したチャレンジ文字列を上述の所定の演算方法によって演算した演算結果と、この信号に収容されているレスポンス文字列を切断先の自動設定装置１１の公開鍵証明書に収容されている切断先の自動設定装置１１の公開鍵で復号化した復号結果とを比較し、一致するか否かを判断する（Ｓ３３０）。切断元の自動設定装置１１におけるトンネル削除部６５は、切断先の自動設定装置１１に判断結果通知信号を作成して送信し（Ｓ３３１）、判断の結果、一致しない場合には、切断先の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、一致する場合には、切断元の自動設定装置１１におけるトンネル削除部６５は、後述の処理を継続する。

【0165】

判断結果通知信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は、ランダムにチャレンジ文字列を生成し（Ｓ３３２）、チャレンジ文字列通知信号を作成して切断元の自動設定装置１１に送信する（Ｓ３３３）。

【0166】

切断元の自動設定装置１１におけるトンネル削除部６５は、このチャレンジ文字列通知信号を受信すると、この信号に収容されているチャレンジ文字列を上述の所定の演算方法によって演算し、演算結果を自身の自動設定装置１１の秘密鍵（切断先の自動設定装置１１の秘密鍵）で暗号化することによってレスポンス文字列を生成する（Ｓ３３４）。次に、切断元の自動設定装置１１におけるトンネル削除部６５は、レスポンス文字列通知信号を作成して切断先の自動設定装置１１に送信する（Ｓ３３５）。

【0167】

切断先の自動設定装置１１におけるトンネル削除部６５は、レスポンス文字列通知信号を受信すると、処理Ｓ３３２で生成したチャレンジ文字列を上述の所定の演算方法によって演算した演算結果と、この信号に収容されているレスポンス文字列を切断元の自動設定装置１１の公開鍵証明書に収容されている切断元の自動設定装置１１の公開鍵で復号化した復号結果とを比較し、一致するか否かを判断する（Ｓ３３６）。切断先の自動設定装置１１におけるトンネル削除部６５は、切断元の自動設定装置１１に判断結果通知信号を作成して送信し（Ｓ３３７）、判断の結果、一致しない場合には、切断元の自動設定装置１１が真正な自動設定装置１１ではないと判断し、本処理を終了する。一方、判断の結果、一致する場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、後述の処理を継続する。

【0168】

以上の処理Ｓ３０４乃至処理Ｓ３３７を実行することによって切断元の自動設定装置１１と切断先の自動設定装置１１は、第三者機関である認証サーバ２３を用いて相互認証を行う。

【0169】
相互認証に成功すると、切断元の自動設定装置１１におけるトンネル削除部６５及び切断先の自動設定装置１１におけるトンネル削除部６５は、６０４トンネルの切断に必要な情報を互いに交換する。即ち、切断元の自動設定装置１１におけるトンネル削除部６５は、切断するトンネルを識別するための情報、及び、６０４トンネルの切断を指示する旨の情報を収容した通信信号（トンネル切断指示信号）を作成して切断先の自動設定装置１１に送信し（Ｓ３３８）、一方、切断先の自動設定装置１１におけるトンネル削除部６５もトンネル切断指示信号を作成して切断元の自動設定装置１１に送信する（Ｓ３３９）。ここで、切断するトンネルを識別するための情報は、例えば、接続元のトンネル外部アドレス、トンネル内部アドレス及び自動設定装置識別子と、接続先のトンネル外部アドレス、トンネル内部アドレス及び自動設定装置識別子と、トンネル名とである。
【0170】
トンネル切断指示信号を切断先の自動設定装置１１から受信すると、切断元の自動設定装置１１におけるトンネル削除部６５は、記憶している情報によってトンネルを切断できるか否かを判断する（Ｓ３４０）。このトンネル設定の可否の判断は、提供トンネルテーブル上における該当するトンネル情報の有無であり、これら情報がある場合には６０４トンネルの切断が可能と判断され、これら情報のうち何れかかが欠けている場合には６０４トンネルの切断が不能と判断される。判断の結果、不能と判断された場合には、切断元の自動設定装置１１におけるトンネル削除部６５は、６０４トンネルを自動的に切断する本処理を終了する。一方、判断の結果、可能と判断された場合には、切断元の自動設定装置１１におけるトンネル削除部６５は、判断結果通知信号を作成して切断先の自動設定装置１１に送信する（Ｓ３４１）。
【0171】
一方、切断先の自動設定装置１１におけるトンネル削除部６５は、切断元の自動設定装置１１からこの判断結果通知信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は、記憶している情報によって６０４トンネルを切断できるか否かを判断する（Ｓ３４２）。判断の結果、不能と判断された場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、ト６０４ンネルを自動的に切断する本処理を終了する。一方、判断の結果、可能と判断された場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、判断結果通知信号を作成して切断元の自動設定装置１１に送信する（Ｓ３４３）。
【0172】
他方の自動設定装置１１から６０４トンネルの切断が可能であると判断した旨の判断結果を収容する判断結果通知信号を受信すると、切断元及び切断先の自動設定装置１１におけるトンネル削除部６５は、コネクションを解消する処理をそれぞれ行う（Ｓ３４４）。コネクションが解消されると、切断元の自動設定装置１１におけるトンネル削除部６５及び切断先の自動設定装置１１におけるトンネル削除部６５は、６０４トンネルの切断をそれぞれ実行する（Ｓ３４５、Ｓ３４６）。６０４トンネルの切断は、設定トンネル管理情報テーブル１０１から切断した６０４トンネルに対応するレコードを削除すると共に、ＳＰＤ及びＳＡＤから切断した６０４トンネルに対応するセキュリティポリシ及びセキュリティアソシエーションをそれぞれ削除することによって行われる。
【0173】
このように相互認証を行ってから６０４トンネルを切断するので、不正切断を回避することができ、トンネルの接続先の自動設定装置１１も切断する６０４トンネルに対応する情報を削除することができ、制御部５２や記憶部５３等のリソースを節約することができる。
【0174】
なお、上述の実施形態では、自動設定装置１１は、出荷時にＩＰｖ６アドレスの生成情報が予め埋め込まれ、自身の自動設定装置識別子としていたが、出荷時には一意となるような任意の文字列、例えば、製品のシリアル番号などを埋め込み、ＩＰｖ６アドレス生成

情報は、初期処理において、この一意となるような任意の文字列を用いることによって情報サーバ２１から取得するように構成してもよい。

【0175】

図２７は、情報サーバからＩＰｖ６生成情報を取得する場合における情報サーバにおけるトンネル内部ＩＰアドレス生成情報テーブルの構成を示す図である。図２８は、情報サーバからＩＰｖ６生成情報を取得する場合に係る自動設定装置の初期処理の動作を示すシーケンス図の一部である。図２９は、情報サーバからＩＰｖ６生成情報を取得する場合に係る自動設定装置の初期処理の一部において情報サーバの動作を示すフローチャートである。

【0176】

図２７において、トンネル内部ＩＰアドレス生成情報テーブルは、自動設定装置１１からの要求に応じて割り振ったトンネル内部ＩＰアドレス生成情報を自動設定装置１１の自動設定装置識別子に対応付けて登録する。トンネル内部ＩＰアドレス生成情報テーブル１０６は、例えば、図２７に示すように各レコードを管理する管理番号を登録する管理番号フィールド１６１、自動設定装置１１の自動設定装置識別子を登録する自動設定装置識別子フィールド１６２、及び、当該自動設定装置１１に割り振ったトンネル内部ＩＰアドレス生成情報を登録するトンネル内部ＩＰアドレス生成情報フィールド１６３を備えて構成され、トンネル内部ＩＰアドレス生成情報を割り振られた自動設定装置１１ごとにレコードが作成される。

【0177】

前述の実施形態における図１３を用いて説明した処理Ｓ６４と処理Ｓ６５との間において、図２８に示す処理を行う。即ち、図２８において、自動設定装置１１のトンネル設定部６２は、自動設定装置識別子及びトンネル内部ＩＰアドレス生成情報を要求する旨の情報を収容する通信信号（トンネル内部ＩＰアドレス生成情報要求信号）を作成して情報サーバ２１に送信する（Ｓ１７１）。情報サーバ２１は、トンネル内部ＩＰアドレス生成情報要求信号を受信すると、この信号に収容されている自動設定装置識別子に対してトンネル内部ＩＰアドレス生成情報を割り振る（Ｓ１７２）。

【0178】

次に、処理Ｓ１７２について、さらに詳細に説明する。図２８において、情報サーバ２１は、トンネル内部ＩＰアドレス生成情報要求信号を受信すると、この信号に収容されている自動設定装置識別子に基づいてトンネル内部ＩＰアドレス生成情報テーブル１０６からこの自動設定装置識別子に対応するトンネル外部ＩＰアドレスを検索し、この自動設定装置識別子に対応するトンネル内部ＩＰアドレス生成情報登録済みか否かを判断する（Ｓ８１）。この登録済みであるか否かの判断は、トンネル内部ＩＰアドレス生成情報要求信号に収容されている自動設定装置識別子とトンネル内部ＩＰアドレス生成情報が対応付けられて登録されているレコードがトンネル内部ＩＰアドレス生成情報テーブル１０６に存在するか否か検索する事によって行われ、レコードが存在する場合は登録済みと判断され、レコードが存在しない場合には登録済みでないと判断される。判断の結果、登録済みでないと判断された場合には、情報サーバ２１は、予め用意されているＩＰｖ６アドレスのネットワーク・プレフィックスの中から未割り振りのＩＰｖ６アドレスのネットワーク・プレフィックスを選択し、トンネル内部ＩＰアドレス生成情報テーブル１０６に新たな管理番号を付して新たなレコードを作成し、作成したレコードにおける自動設定装置識別子フィールド１６２及びトンネル内部ＩＰアドレス生成情報フィールド１６３に、トンネル内部ＩＰアドレス生成情報要求信号の自動設定装置識別子及び選択したＩＰｖ６アドレスのネットワーク・プレフィックスをそれぞれ登録する（Ｓ８２）。一方、判断の結果、登録済みと判断された場合には、情報サーバ２１は、トンネル内部ＩＰアドレス生成情報テーブル１０６に存在する、トンネル内部ＩＰアドレス生成情報要求信号に収容されている自動設定装置識別子とトンネル内部ＩＰアドレス生成情報が対応付けられて登録されているレコードからトンネル内部ＩＰアドレス生成情報を取得する（Ｓ８３）。

【0179】

そして、情報サーバ２１は、割り振ったＩＰｖ６アドレスのネットワーク・プレフィックスをトンネル内部ＩＰアドレス生成情報として収容した通信信号（トンネル内部ＩＰアドレス生成情報返信信号）を作成してトンネル自動設定装置１１に返信する（Ｓ１７３）。続いて、自動設定装置１１のトンネル設定部６２は、情報サーバ２１から設定済みトンネル内部ＩＰアドレス登録返信信号を受信すると、処理Ｓ６５以下の処理を続行する。

【0180】

このように動作することで、自動設定装置１１に割り振られトンネル内部ＩＰアドレスとして使用されるＩＰｖ６アドレスを情報サーバ２１が一括管理し、自動設定装置１１の要求に応じてＩＰｖ６アドレスを割り振っているので、テーブル１０６から登録されたＩＰｖ６アドレスで、長期に亘って使用されていないＩＰｖ６アドレスについて適時削除することで、自動設定装置１１が破棄されたり、使用されなくなったりした場合に、ＩＰｖ６アドレスを回収することができ、ＩＰｖ６アドレスを効率的に使い回すことが出来る。

【0181】

そして、上述の実施形態では、トンネル構築処理の際に、接続先の自動設定装置１１において接続元の自動設定装置１１からのコネクションが正当であるか否かをチェックしていないが、チェックするように構成してもよい。また、上述の実施形態では、トンネル削除処理の際に、切断先の自動設定装置１１において切断元の自動設定装置１１からのコネクション正当であるか否かをチェックしていないが、チェックするように構成してもよい。

【0182】

図３０は、トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル構築処理の動作を示すシーケンス図の一部である。図３１は、トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル削除処理の動作を示すシーケンス図の一部である。

【0183】

前述の実施形態における図１４を用いて説明した処理Ｓ１０８と図１５の処理Ｓ１０９との間において、図３０に示す処理を行う。即ち、図３０において、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１０８において接続元の自動設定装置１１から受信した自動設定装置識別子通知信号に収容されている接続元の自動設定装置１１における自動設定装置識別子、及び、接続元の自動設定装置１１におけるトンネル外部ＩＰアドレスを要求する旨の情報を収容した通信信号（接続元トンネル外部ＩＰアドレス要求信号）を作成して情報サーバ２１に送信する（Ｓ１６１）。情報サーバ２１は、接続元トンネル外部ＩＰアドレス要求信号を受信すると、この信号に収容されている自動設定装置識別子に基づいて提供トンネル設定情報テーブルから１０２からこの自動設定装置識別子に対応するトンネル外部ＩＰアドレスを検索する（Ｓ１６２）。そして、情報サーバ２１は、検索したトンネル外部ＩＰアドレスを収容した通信信号（接続元トンネル外部ＩＰアドレス返信信号）を作成して接続先の自動設定装置１１に返信する（Ｓ１６３）。情報サーバ２１から接続元トンネル外部ＩＰアドレス返信信号を受信すると、接続先の自動設定装置１１におけるトンネル設定部６２は、接続元の自動設定装置１１からのコネクションが真正であるか否か判断する（Ｓ１６４）。この真正であるか否かの判断は、コネクションを確立している接続元の自動設定装置１１のＩＰアドレスと情報サーバ２１から取得した接続元トンネル外部ＩＰアドレス返信信号に収容されている接続元トンネル外部ＩＰアドレスとを比較することによって行われ、両ＩＰアドレスが一致する場合には真正と判断され、両ＩＰアドレスが不一致である場合には真正でないと判断される。判断の結果、真正でないと判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、真正であると判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１０９以下の処理を続行する。

【0184】

そして、前述の実施形態における図２２を用いて説明した処理Ｓ３０８と図２３の処理

Ｓ３０９との間において、図３１に示す処理を行う。即ち、図３１において、切断先の自動設定装置１１におけるトンネル削除部６５は、処理Ｓ３０８において切断元の自動設定装置１１から受信した自動設定装置識別子通知信号に収容されている切断元の自動設定装置１１における自動設定装置識別子、及び、切断元の自動設定装置１１におけるトンネル外部ＩＰアドレスを要求する旨の情報を収容した通信信号（切断元トンネル外部ＩＰアドレス要求信号）を作成して情報サーバ２１に送信する（Ｓ３６１）。情報サーバ２１は、切断元トンネル外部ＩＰアドレス要求信号を受信すると、この信号に収容されている自動設定装置識別子に基づいて提供トンネル設定情報テーブルから１０２からこの自動設定装置識別子に対応するトンネル外部ＩＰアドレスを検索する（Ｓ３６２）。そして、情報サーバ２１は、検索したトンネル外部ＩＰアドレスを収容した通信信号（切断元トンネル外部ＩＰアドレス返信信号）を作成して切断先の自動設定装置１１に返信する（Ｓ３６３）。情報サーバ２１から切断元トンネル外部ＩＰアドレス返信信号を受信すると、切断先の自動設定装置１１におけるトンネル削除部６５は、切断元の自動設定装置１１からのコネクションが真正であるか否か判断する（Ｓ３６４）。この真正であるか否かの判断は、コネクションを確立している切断元の自動設定装置１１のＩＰアドレスと情報サーバ２１から取得した切断元トンネル外部ＩＰアドレス返信信号に収容されている切断元トンネル外部ＩＰアドレスとを比較することによって行われ、両ＩＰアドレスが一致する場合には真正と判断され、両ＩＰアドレスが不一致である場合には真正でないと判断される。判断の結果、真正でないと判断された場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、真正であると判断された場合には、切断先の自動設定装置１１におけるトンネル削除部６５は、処理Ｓ３０９以下の処理を続行する。

【0185】

このように動作することで、トンネル構築処理において、接続先の自動設定装置１１は、接続元の自動設定装置１１が真正なトンネル外部ＩＰアドレスを持つ自動設定装置１１であるかチェックすることで、セキュリティを高めることができ、トンネル構築処理の開始直後に実行することで接続元の自動設定装置が不正な場合、それ以降のトンネル構築処理を実行させないことで自動設定装置１１の負荷を下げることができる。また、トンネル削除処理において、切断先の自動設定装置１１は、切断元の自動設定装置１１が真正なトンネル外部ＩＰアドレスを持つ自動設定装置１１であるかチェックすることで、セキュリティを高めることができ、トンネル削除処理の開始直後に実行することで切断元の自動設定装置が不正な場合、それ以降のトンネル削除処理を実行させないことで自動設定装置１１の負荷を下げることができる。

【0186】

また、上述の実施形態では、トンネル構築処理の際に、接続先の自動設定装置１１において接続元の自動設定装置１１から送信されたトンネル内部ＩＰアドレスが正当であるか否かをチェックしていないが、チェックするように構成してもよい。また、上述の実施形態では、トンネル構築処理の際に、接続元の自動設定装置１１において接続先の自動設定装置１１から送信されたトンネル内部ＩＰアドレスが正当であるか否かをチェックしていないが、チェックするように構成してもよい。

【0187】

図３２は、トンネル内部ＩＰアドレスのチェックを行う場合に係る情報サーバにおける設定済みトンネル内部ＩＰアドレステーブルの構成を示す図である。図３３は、トンネル内部ＩＰアドレスのチェックを行う場合に係る自動設定装置の初期処理の動作を示すシーケンス図の一部である。図３４及び図３５は、トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル構築処理の動作を示すシーケンス図の一部である。

【0188】

図３２において、設定済みトンネル内部ＩＰアドレステーブルは、自動設定装置１１の要求に応じて自動設定装置１１のＬＡＮ側インタフェース部に設定したトンネル内部ＩＰアドレスをを自動設定装置識別子に対応付けて登録する。設定済みトンネル内部ＩＰアド

レステーブル１０７は、例えば、図３２に示すように各レコードを管理する管理番号を登録する管理番号フィールド１７１、自動設定装置１１の自動設定装置識別子を登録する自動設定装置識別子フィールド１７２、及び、当該自動設定装置１１のＬＡＮ側インタフェース部に設定されたトンネル内部ＩＰアドレスを登録する設定済みトンネル内部ＩＰアドレスフィールド１７３を備えて構成され、トンネル内部ＩＰアドレスをＬＡＮ側インターフェースに設定済みの自動設定装置１１ごとにレコードが作成される。

【0189】

前述の実施形態における図１３を用いて説明した処理Ｓ６６と処理Ｓ６７との間において、図３３に示す処理を行う。即ち、図３３において、自動設定装置１１のトンネル設定部６２は、自動設定装置識別子、設定済みトンネル内部ＩＰアドレス(ＬＡＮ側インターフェースに設定されたトンネル内部アドレス)及び設定済みトンネル内部ＩＰアドレスの登録を要求する旨の情報を収容する通信信号（設定済みトンネル内部ＩＰアドレス登録要求信号）を作成して情報サーバ２１に送信する（Ｓ９１）。情報サーバ２１は、設定済みトンネル内部ＩＰアドレス登録要求信号を受信すると、設定済みトンネル内部ＩＰアドレステーブル１０７に新たな管理番号を付して新たなレコードを作成し、作成したレコードにおける自動設定装置識別子フィールド１７２及び設定済みトンネル内部ＩＰアドレスフィールド１７３に、設定済みトンネル内部ＩＰアドレス登録要求信号に収容されている自動設定装置識別子及び設定済みトンネル内部ＩＰアドレス登録要求信号に収容されているトンネル内部ＩＰアドレスをそれぞれ登録する（Ｓ９２）。そして、情報サーバ２１は、設定済みトンネル内部ＩＰアドレスの登録が完了した旨の情報を収容した通信信号（設定済みトンネル内部ＩＰアドレス登録返信信号）を作成してトンネル自動設定装置１１に返信する（Ｓ９３）。続いて、自動設定装置１１のトンネル設定部６２は、情報サーバ２１から設定済みトンネル内部IPアドレス登録返信信号を受信すると、処理Ｓ６７以下の処理を続行する。

【0190】

そして、前述の実施形態における図１７を用いて説明した処理Ｓ１３９と図１８の処理Ｓ１４０との間において、図３４に示す処理を行う。即ち、図３４において、接続元の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１３９において接続先の自動設定装置１１からトンネル構築指示信号を受信すると、接続先の自動設定装置１１における自動設定識別子と、接続先の自動設定装置１１におけるトンネル内部ＩＰアドレスを要求する旨の情報を収容した通信信号（設定済み接続先トンネル内部ＩＰアドレス要求信号）を作成して情報サーバ２１に送信する（Ｓ１７１）。

【0191】

この設定済み接続先トンネル内部ＩＰアドレス要求信号を受信すると情報サーバ２１は、この受信した設定済み接続先トンネル内部ＩＰアドレス要求信号に収容されている接続先の自動設定装置１１の自動設定装置識別子に基づいて設定済みトンネル内部ＩＰアドレステーブル１０７を参照し、この接続先の自動設定装置１１の自動設定装置識別子に対応する設定済みトンネル内部ＩＰアドレスを検索する（Ｓ１７２）。情報サーバ２１は、検索した設定済み接続先トンネル内部ＩＰアドレスを収容する通信信号（設定済み接続先トンネル内部ＩＰアドレス返信信号）を作成して接続元の自動設定装置１１に返信する（Ｓ１７３）。設定済み接続先トンネル内部ＩＰアドレス返信信号を受信すると、接続元の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１３９で接続先の自動設定装置１１から送信されたトンネル内部ＩＰアドレスとこの情報サーバ２１から取得した設定済み接続先トンネル内部ＩＰアドレス返信信号に収容されている設定済み接続先トンネル内部ＩＰアドレスを比較することによって、接続先の自動設定装置１１から送信されたトンネル内部ＩＰアドレスが真正であるか否かを判断する（Ｓ１７４）。この判断は、接続先の自動設定装置１１から送信されたトンネル内部ＩＰアドレスと設定済み接続先トンネル内部ＩＰアドレスとが一致する場合に真正であると判断され、接続先の自動設定装置１１から送信されたトンネル内部ＩＰアドレスと設定済み接続先トンネル内部ＩＰアドレスとが不一致である場合には真正でないと判断される。判断の結果、真正でないと判断された場

合には、接続元の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続先の自動設定装置１１に送信し(Ｓ１４９)、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、真正であると判断された場合には、接続元の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１４０以下の処理を続行する。

【0192】

前述の実施形態における図１８を用いて説明した処理Ｓ１４１と処理Ｓ１４２との間において、図３５に示す処理を行う。即ち、図３５において、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１３８において接続元の自動設定装置１１からトンネル構築指示信号を受信すると、接続元の自動設定装置１１における自動設定装置識別子と、接続元の自動設定装置１１におけるトンネル内部ＩＰアドレスを要求する旨の情報を収容した通信信号（設定済み接続元トンネル内部ＩＰアドレス要求信号）を作成して情報サーバ２１に送信する（Ｓ１８１）。

【0193】

この設定済み接続元トンネル内部ＩＰアドレス要求信号を自身すると情報サーバ２１は、この受信した設定済み接続元トンネル内部ＩＰアドレス要求信号に収容されている接続元の自動設定装置１１の自動設定装置識別子に基づいて設定済みトンネル内部ＩＰアドレステーブル１０７を参照し、この接続元の自動設定装置１１の自動設定装置識別子に対応する設定済みトンネル内部ＩＰアドレスを検索する（Ｓ１８２）。情報サーバ２１は、検索した設定済み接続元トンネル内部ＩＰアドレスを収容する通信信号（設定済み接続元トンネル内部ＩＰアドレス返信信号）を作成して接続先の自動設定装置１１に返信する（Ｓ１８３）。設定済み接続元トンネル内部ＩＰアドレス返信信号を受信すると、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１３９で接続元の自動設定装置１１から送信されたトンネル内部ＩＰアドレスとこの情報サーバ２１から取得した設定済み接続元トンネル内部ＩＰアドレス返信信号に収容されている設定済み接続元トンネル内部ＩＰアドレスを比較することによって、接続元の自動設定装置１１から送信されたトンネル内部ＩＰアドレスが真正であるか否かを判断する（Ｓ１８４）。この判断は、接続元の自動設定装置１１から送信されたトンネル内部ＩＰアドレスと設定済み接続元トンネル内部ＩＰアドレスとが一致する場合に真正であると判断され、接続元の自動設定装置１１から送信されたトンネル内部ＩＰアドレスと設定済み接続元トンネル内部ＩＰアドレスとが不一致である場合には真正でないと判断される。判断の結果、真正でないと判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、判断結果を収容する通信信号（判断結果通知信号）を作成して接続元の自動設定装置１１に送信し(Ｓ１４９)、６０４トンネルを自動的に設定する本処理を終了する。一方、判断の結果、真正であると判断された場合には、接続先の自動設定装置１１におけるトンネル設定部６２は、処理Ｓ１４２以下の処理を続行する。

【0194】

このように動作することで、トンネル構築処理において、接続元の自動設定装置１１は、接続先の自動設定装置１１が真正なトンネル内部ＩＰアドレスを持つ自動設定装置１１であるかチェックすることで、セキュリティを高めることができる。また、トンネル構築処理において、接続先の自動設定装置１１は、接続元の自動設定装置１１が真正なトンネル内部ＩＰアドレスを持つ自動設定装置１１であるかチェックすることで、セキュリティを高めることができる。

【0195】

さらに、上述の実施形態では、自動設定装置１１は、１個の物理的なＷＡＮ側インターフェース部５５に対し複数の論理的なインターフェースを生成することによって複数の他の自動設定装置１１へ複数の６０４トンネルをそれぞれ同時に設定したが、複数個の物理的なＷＡＮ側インターフェース部を備えることによって複数の他の自動設定装置１１へ複数の６０４トンネルをそれぞれ同時に設定するように構成してもよい。

【0196】

図３６は、複数のＷＡＮ側インターフェース部を備えるトンネル自動設定装置を含むネットワークの構成を示すブロック図である。図３７は、複数のＷＡＮ側インターフェース部を備えるトンネル自動設定装置に係る設定トンネル管理情報テーブルの構成を示す図である。図３８は、トンネル自動設定装置がＷＡＮ側インターフェー部を複数備える場合における情報サーバの提供トンネル設定情報テーブルの構成を示す図である。

【0197】

図３６において、自動設定装置１１’は、ＬＡＮ側インターフェース部５１と、制御部５２’と、記憶部５３’と、入力部５４と、複数のＷＡＮ側インターフェース部５５’（５５’－０、５５’－１、・・・、５５’－ｎ）とを備えて構成される。これらＬＡＮ側インターフェース部５１、制御部５２’、記憶部５３’、入力部５４及びＷＡＮ側インターフェース部５５’は、ＷＡＮ側インターフェース部５５’が複数であって各ＷＡＮ側インターフェース部５５’－０、５５’－１、・・・、５５’－ｎを識別するための識別子であるＷＡＮ側インタフェースデバイス名が各ＷＡＮ側インターフェース部５５’－０、５５’－１、・・・、５５’－ｎにそれぞれ付与され、図３７に示すように設定トンネル管理情報記憶部７３’に記憶される設定トンネル管理情報テーブル１０１’がＷＡＮ側インターフェースデバイス名を登録するＷＡＮ側インターフェースデバイス名フィールド１１２を図３に示す設定トンネル管理情報テーブル１０１にさらに備えられて構成され、制御部５２’のトンネル設定部６２’が６０４トンネルを自動的に設定する場合にこのＷＡＮ側インターフェースデバイス名を用いることを除き、上述したＬＡＮ側インターフェース部５１、制御部５２、記憶部５３、入力部５４及びＷＡＮ側インターフェース部５５とそれぞれ同様であるので、その説明を省略する。

【0198】

そして、情報サーバ２１は、各ＷＡＮ側インターフェース部５５’－０、５５’－１、・・・、５５’－ｎにそれぞれ付与されるトンネル外部ＩＰアドレスを個別に管理するために、提供トンネル設定情報をＷＡＮ側インターフェースデバイス名と自動設定装置識別子との組に対応付けて提供トンネル設定情報記憶部に記憶される。例えば、図３８に示すように、提供トンネル設定情報記憶部に記憶される提供トンネル設定情報テーブル１０２’は、ＷＡＮ側インターフェースデバイス名を登録するＷＡＮ側インターフェースデバイス名フィールド１２２を図４に示す提供トンネル設定情報テーブル１０２にさらに備えられて構成され、ＷＡＮ側インターフェースデバイス名と自動設定装置識別子との組ごとにレコードが作成される。

【0199】

そして、処理Ｓ６４、処理Ｓ６５、処理Ｓ１０８、処理Ｓ１０９、処理Ｓ１１０、処理Ｓ１１１の処理において、自動設定装置識別子に代えて自動設定装置識別子とＷＡＮ側インタフェースデバイス名との組を用いる。ここで、接続先の自動設定装置１１が複数のＷＡＮ側インターフェース部５５を備えている場合には、処理Ｓ１０２乃至処理Ｓ１０４を行うことによって、接続元の自動設定装置１１’におけるトンネル設定部６２’は、情報サーバ２１から複数のトンネル外部ＩＰアドレスを取得することになるが、接続元の自動設定装置１１におけるトンネル設定部６２’は、複数のトンネル外部ＩＰアドレスから任意に１個のトンネル外部ＩＰアドレスを用いればよい。

【0200】

なお、トンネル切断処理の場合には、トンネル切断指示信号を受信することによって切断すべき６０４トンネルが特定されるので、６０４トンネルが複数設定されている場合でも上述した処理Ｓ３０３乃至処理Ｓ３４３を実行することによって６０４トンネルを切断することができる。

【0201】

そして、上述の実施形態では、自動設定装置１１、１１’は、ルータ装置に組み込まれた場合について説明したが、これに限定されるものではなく、例えば、通信パケットのルーティングを行うルーティング機能に加えてプロトコル変換を行う機能をさらに備えたゲートウェイ装置に組み込んでもよい。

【0202】
また、上述の実施形態では、自動設定装置１１、１１’は、情報サーバ２１、登録サーバ２２、認証サーバ２３及びＮＴＰサーバ２４の所在情報をＩＰアドレスで記憶部５３に記憶するように構成したが、ホスト名とＩＰアドレスの対応関係を記述したデータベースを管理して、クライアントからの要求に応じてホスト名からそのＩＰアドレスを検索し、検索結果をクライアントに返信するＤＮＳ（Domain Name System）サーバ２５を図１に破線で示すようにネットワーク１にさらに備えさせ、自動設定装置１１、１１’は、情報サーバ２１、登録サーバ２２、認証サーバ２３及びＮＴＰサーバ２４のうち少なくとも１つの所在情報をホスト名で記憶部５３に記憶するように構成してもよい。このように構成することによって、情報サーバ２１や登録サーバ２２や認証サーバ２３やＮＴＰサーバ２４のＩＰアドレスが変更された場合でも自動設定装置１１、１１’は、情報サーバ２１等に接続することができる。特に、情報サーバ２１等の所在情報は、製造段階等に記憶部５３に記憶されるので、自動設定装置１１、１１’が出荷された後に情報サーバ２１等のＩＰアドレスが変更された場合でも自動設定装置１１、１１’は、情報サーバ２１等に接続することができる。

【0203】
さらに、上述の実施形態において、接続元と接続先とが同一であってＩＰｓｅｃを適用する６ｏ４トンネルとＩＰｓｅｃを適用しない６ｏ４トンネルとの２個の６ｏ４トンネルを設定し、通信の内容に応じて２個の６ｏ４トンネルの内から何れか一方を選択するように構成することによって、通信の内容に応じて暗号化の必要な場合にＩＰｓｅｃを利用するようにできるから、通信を行う場合に、制御部５２の情報処理量を軽減することができ、制御部５２の負担を軽減することができる。

【0204】
そして、上述の実施形態では、制御部５２、５２’は、設定されている６ｏ４トンネルに障害が生じているか否かを判断し、障害が生じている場合にも６ｏ４トンネルを削除するように構成してもよい。障害の有無は、例えば、ピング（Ping）を６ｏ４トンネルの設定先の自動設定装置１１、１１’に送信し、当該ピングに対する受信応答をタイムアウトする前に受信した場合には障害が無いと判断し、タイムアウトした場合には障害が有ると判断する。このように構成することによって、障害により使用することができなくなった６ｏ４トンネルの放置を回避することができ、制御部５２、５２’や記憶部５３、５３’等のリソースの無駄をなくすことができる。そして、６ｏ４トンネルを削除した場合に、トンネル削除部６６は、トンネル設定部６２を用いて、削除した６ｏ４トンネルにおける他方の自動設定装置１１、１１’を新たに接続先として６ｏ４トンネルを自動的に再設定するように構成してもよい。このように構成することによって、障害を自動的に除去することができるので、６ｏ４トンネル自体の耐障害性を向上させることができ、使用可能な状態で６ｏ４トンネルを維持することができる。

【0205】
また、上述の実施形態では、自動設定装置１１は、ＩＰｖ４のＩＳＰネットワーク３及びＩＰｖ４のネットワーク４上に、他の自動設定装置１１との間にＩＰｖ６ｏｖｅｒＩＰｖ４トンネルを形成する実施形態である。ＩＰｖ４のネットワークが順次ＩＰｖ６を採用することによってＩＰｖ６のネットワークに移行して上述の実施形態におけるＩＳＰネットワーク３及びネットワーク４がＩＰｖ６になった場合でも、同様の動作によって、一の自動設定装置１１は、ＩＳＰネットワーク３及びネットワーク４上に、他の自動設定装置１１との間にＩＰｖ６ｏｖｅｒＩＰｖ６トンネルを形成することができる。このようにネットワーク１の全てのノードがＩＰｖ６で動作するようになった場合でも、本発明にかかる自動設定装置１１を用いることで、製造企業等は、トンネル自動設定装置１１を管理することができるだけでなく、各ＩＰｖ６のネットワーク２間にトンネルを設定することによって、セキュア（安全な）通信経路を確保することができる。

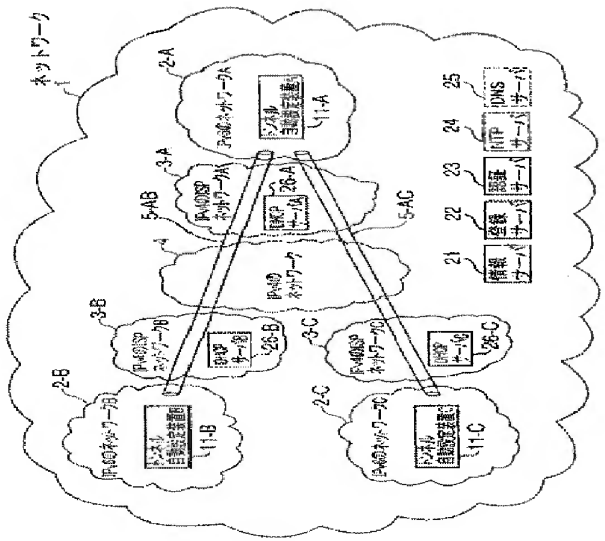
【図面の簡単な説明】
【0206】

【図1】実施形態におけるネットワークの全体構成を示す図である。
【図2】トンネル自動設定装置を含むネットワークの構成を示すブロック図である。
【図3】トンネル自動設定装置における設定トンネル管理情報テーブルの構成を示す図である。
【図4】情報サーバにおける提供トンネル設定情報テーブルの構成を示す図である。
【図5】登録サーバにおけるログイン認証情報登録テーブルの構成を示す図である。
【図6】登録サーバにおける自動設定装置本人情報登録テーブルの構成を示す図である。
【図7】認証サーバにおけるリポジトリの構成を示す図である。
【図8】公開鍵証明書取得処理の動作を示すシーケンス図である。
【図9】自動設定装置の公開鍵証明書の発行処理における動作を示すフローチャートである。
【図10】自動設定装置の公開鍵証明書の記憶処理における動作を示すフローチャートである。
【図11】認証サーバの公開鍵証明書に対する更新処理における動作を示すシーケンス図である。
【図12】認証サーバの公開鍵証明書に対する更新処理における動作を示すフローチャートである。
【図13】トンネル自動設定処理の初期処理の動作を示すシーケンス図である。
【図14】トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その１）である。
【図15】トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その２）である。
【図16】トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その３）である。
【図17】トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その４）である。
【図18】トンネル自動設定処理におけるトンネル構築処理の動作を示すシーケンス図（その５）である。
【図19】トンネル自動設定処理におけるトンネル構築処理の動作を示すフローチャートである。
【図20】自動設定装置の公開鍵証明書に対する更新処理における動作を示すシーケンス図である。
【図21】自動設定装置の公開鍵証明書における使用可能性判断処理の動作を示すフローチャートである。
【図22】トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その１）である。
【図23】トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その２）である。
【図24】トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その３）である。
【図25】トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その４）である。
【図26】トンネル自動設定処理におけるトンネル削除処理の動作を示すシーケンス図（その５）である。
【図27】情報サーバからＩＰｖ６生成情報を取得する場合における情報サーバにおけるトンネル内部ＩＰアドレス生成情報テーブルの構成を示す図である。
【図28】情報サーバからＩＰｖ６生成情報を取得する場合に係る自動設定装置の初期処理の動作を示すシーケンス図の一部である。
【図29】情報サーバからＩＰｖ６生成情報を取得する場合に係る自動設定装置の初期処理の一部において情報サーバの動作を示すフローチャートである。

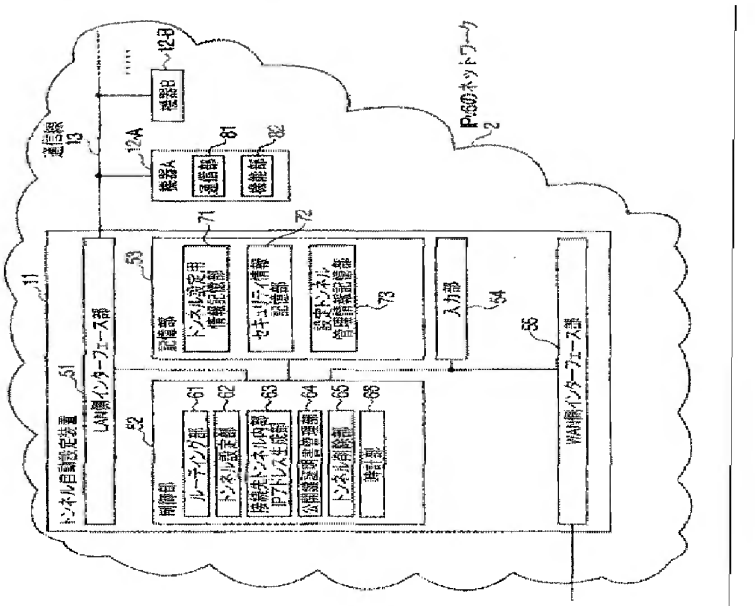
【図30】トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル構築処理の動作を示すシーケンス図の一部である。
【図31】トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル削除処理の動作を示すシーケンス図の一部である。
【図32】トンネル内部ＩＰアドレスのチェックを行う場合に係る情報サーバにおける設定済みトンネル内部ＩＰアドレステーブルの構成を示す図である。
【図33】トンネル内部ＩＰアドレスのチェックを行う場合に係る自動設定装置の初期処理の動作を示すシーケンス図の一部である。
【図34】トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル構築処理の動作を示すシーケンス図の一部である。
【図35】トンネル外部ＩＰアドレスのチェックを行う場合に係る自動設定装置のトンネル削除処理の動作を示すシーケンス図の一部である。
【図36】複数のＷＡＮ側インターフェース部を備えるトンネル自動設定装置を含むネットワークの構成を示すブロック図である。
【図37】複数のＷＡＮ側インターフェース部を備えるトンネル自動設定装置に係る設定トンネル管理情報テーブルの構成を示す図である。
【図38】トンネル自動設定装置がＷＡＮ側インターフェー部を複数備える場合における情報サーバの提供トンネル設定情報テーブルの構成を示す図である。
【符号の説明】
【0207】
１　ネットワーク
２　ＩＰｖ６のネットワーク
３　ＩＰｖ４のＩＳＰネットワーク
４　ＩＰｖ４のネットワーク
５　ＩＰｖ６ｏｖｅｒＩＰｖ４トンネル
１１、１１’　トンネル自動設定装置
２１　情報サーバ
２２　登録サーバ
２３　認証サーバ
２４　ＮＴＰサーバ
２５　ＤＮＳサーバ
２６　ＤＨＣＰサーバ
５１　ローカル・エリア・ネットワーク側インターフェース部
５２、５２’　制御部
５３、５３’　記憶部
５４　入力部
５５、５５’　ワイド・エリア・ネットワーク側インターフェース部
６２、６２’　トンネル設定部
６３　接続先トンネル内部ＩＰアドレス生成部
６４　公開鍵証明書管理部
６５　トンネル削除部
６６　時計部
７１　トンネル設定用情報記憶部
７２　セキュリティ情報記憶部
７３、７３’　設定トンネル管理情報記憶部
１０１、１０１’　設定トンネル管理情報テーブル
１０２、１０２’　提供トンネル設定情報テーブル
１０３　ログイン認証情報登録テーブル
１０４　自動設定装置本人情報登録テーブル
１０５　リポジトリ

１０６　トンネル内部ＩＰアドレス生成情報テーブル
１０７　設定済みトンネル内部ＩＰアドレステーブル

【図1】

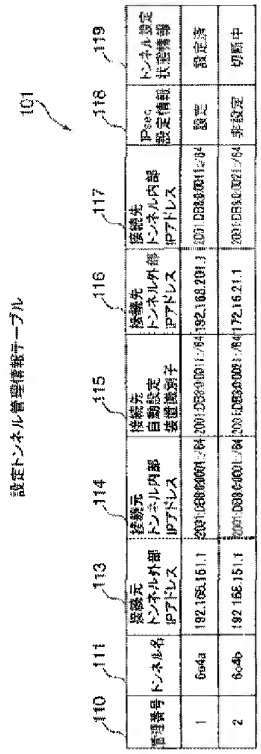


【図2】

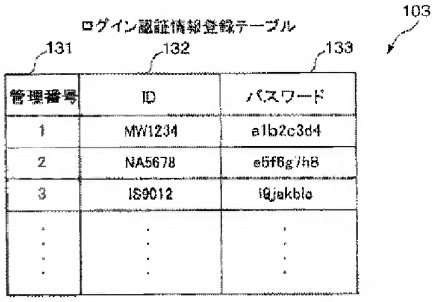


EX1009, Page 797

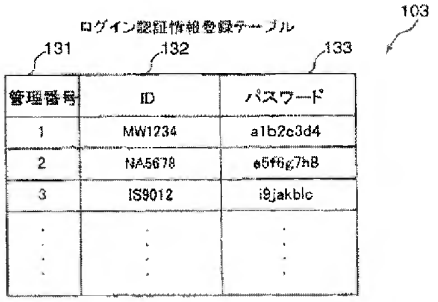
【図3】


設定トンネル管理情報テーブル
101
110
111
113
114
115
116
117
118
119
管理番号
トンネル名
接続元トンネル外部IPアドレス
接続元トンネル内部IPアドレス
接続先自動設定装置識別子
接続先トンネル外部IPアドレス
接続先トンネル内部IPアドレス
IPsec設定情報
トンネル設定共通情報
1
6in4a
192.168.151.1
2001:DB8:0:0001::/64
192.168.201.1
2001:DB8:0011::/64
設定
設定済
2
6in4b
192.168.151.1
2001:DB8:0:0001::/64
172.16.21.1
2001:DB8:0021::/64
未設定
切断中

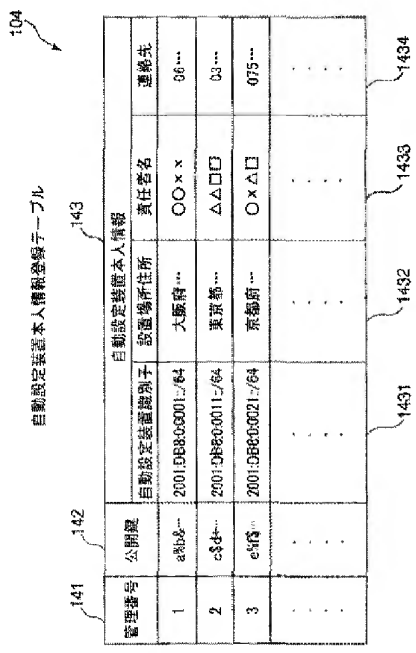
【図4】


ログイン認証情報登録テーブル
103
131
132
133
管理番号
ID
パスワード
1
MW1234
a1b2c3d4
2
NA5678
e5f6g7h8
3
IS9012
i8jakbic

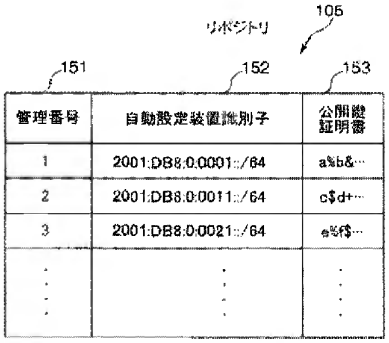
【図5】


ログイン認証情報登録テーブル
103
131
132
133
管理番号
ID
パスワード
1
MW1234
a1b2c3d4
2
NA5678
e5f6g7h8
3
IS9012
i8jakbic

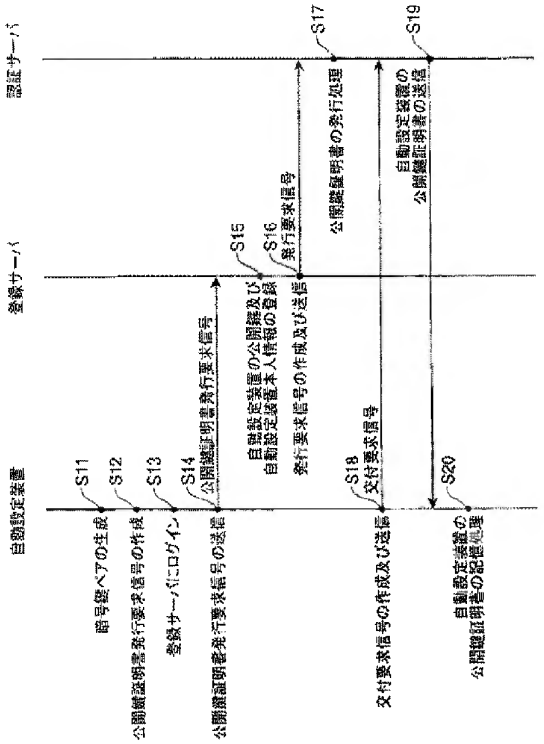
【図6】


自動設定装置本人情報登録テーブル
104
141
142
143
1431
1432
1433
1434
管理番号
公開鍵
自動設定装置識別子
設置場所住所
責任者名
連絡先
1
a%b&…
2001:DB8:0:0001::/64
大阪府…
○○××
06-…
2
c$d+…
2001:DB8:0:0011::/64
東京都…
△△□□
03-…
3
e%f$…
2001:DB8:0:0021::/64
京都府…
○×△□
075-…

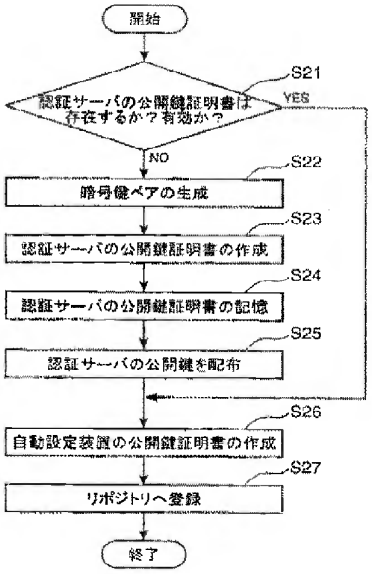
【図7】


リポジトリ
105
151
152
153
管理番号
自動設定装置識別子
公開鍵証明書
1
2001:DB8:0:0001::/64
a%b&…
2
2001:DB8:0:0011::/64
c$d+…
3
2001:DB8:0:0021::/64
e%f$…

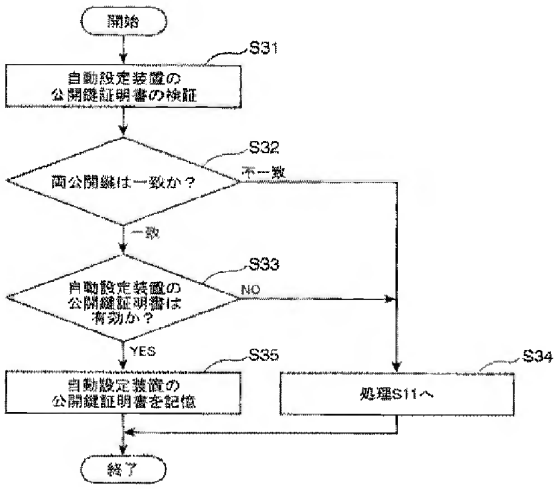
【図8】


認証サーバ
登録サーバ
自動設定装置
S11
暗号鍵ペアの生成
S12
公開鍵証明書発行要求信号の作成
S13
登録サーバにログイン
S14
公開鍵証明書発行要求信号の送信
S15
S16
発行要求信号
公開鍵証明書の発行処理
S17
S18
交付要求信号
S19
自動設定装置の
公開鍵証明書の送信
S20
自動設定装置の
公開鍵証明書の記憶処理

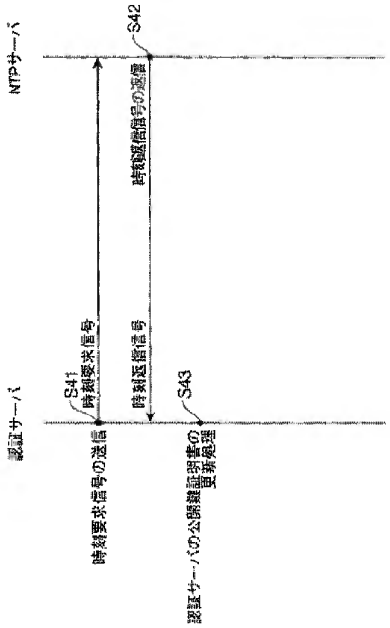
【図9】


開始
S21
認証サーバの公開鍵証明書は
存在するか？有効か？
YES
NO
S22
暗号鍵ペアの生成
S23
認証サーバの公開鍵証明書の作成
S24
認証サーバの公開鍵証明書の記憶
S25
認証サーバの公開鍵を配布
S26
自動設定装置の公開鍵証明書の作成
S27
リポジトリへ登録
終了

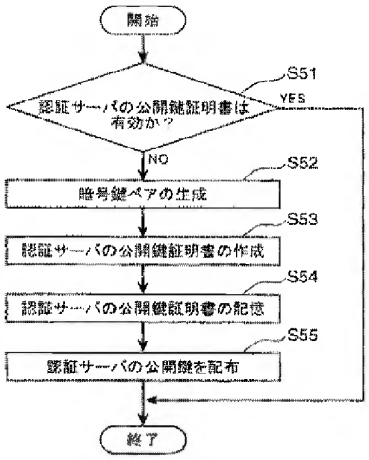
【図10】


開始
S31
自動設定装置の
公開鍵証明書の検証
S32
両公開鍵は一致か？
不一致
一致
S33
自動設定装置の
公開鍵証明書は
有効か？
NO
YES
S34
処理S11へ
S35
自動設定装置の
公開鍵証明書を記憶
終了

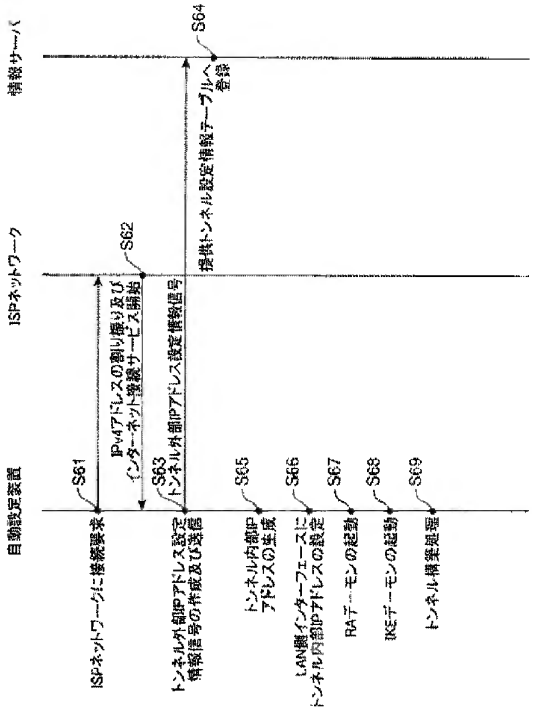
【図11】


NTPサーバ
認証サーバ
S41
時刻要求信号
時刻要求信号の送信
S42
時刻返信信号
時刻返信信号の送信
S43
認証サーバの公開鍵証明書の
登録処理

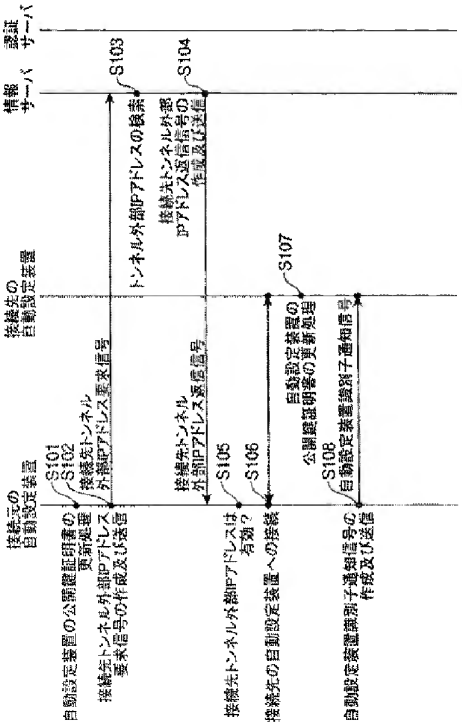
【図12】



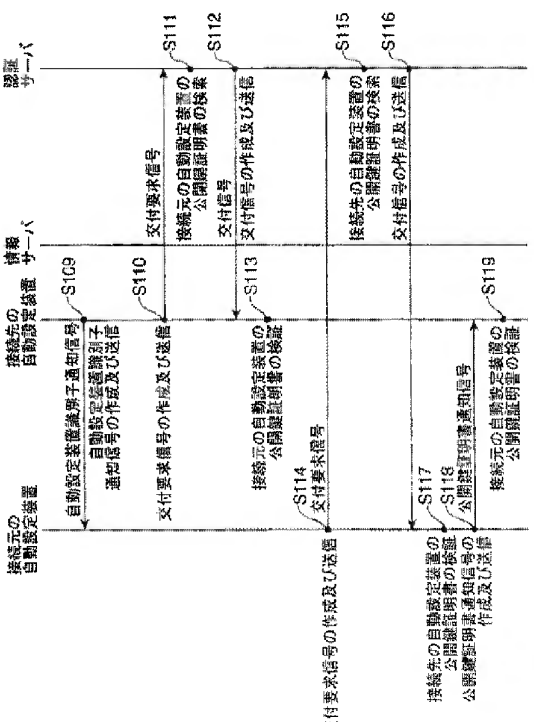
【図13】



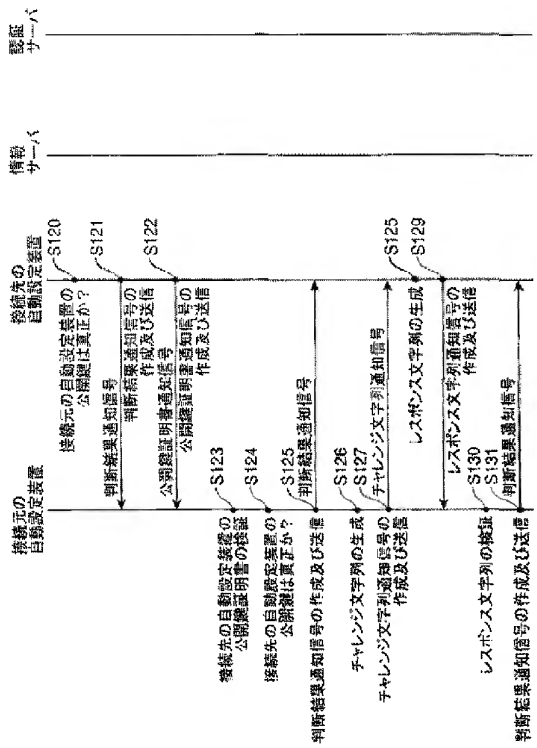
【図14】



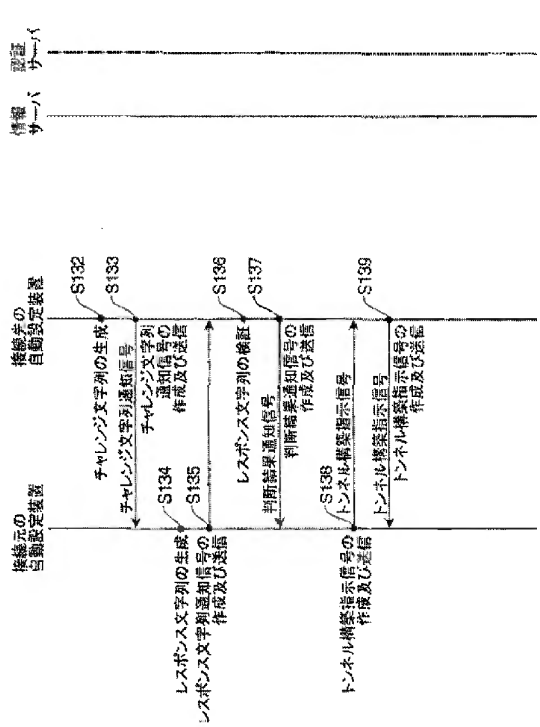
【図15】



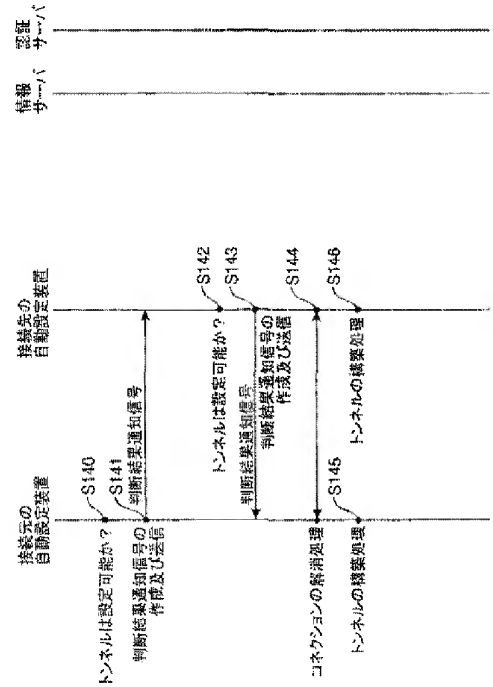
【図16】



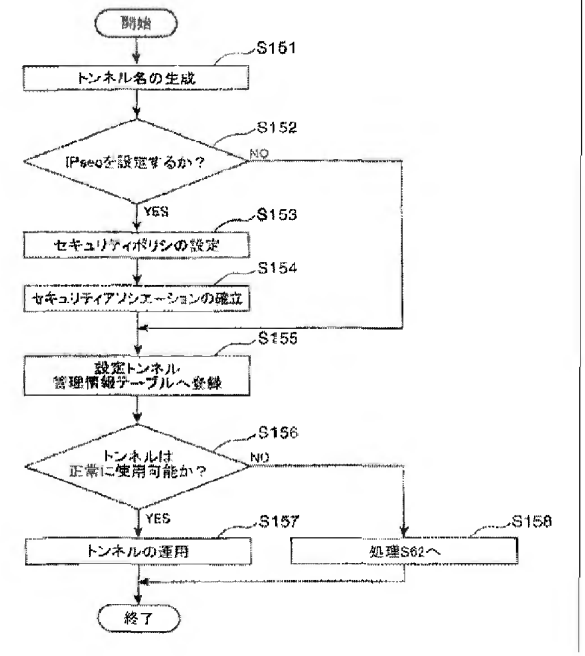
【図17】



【図18】



【図19】



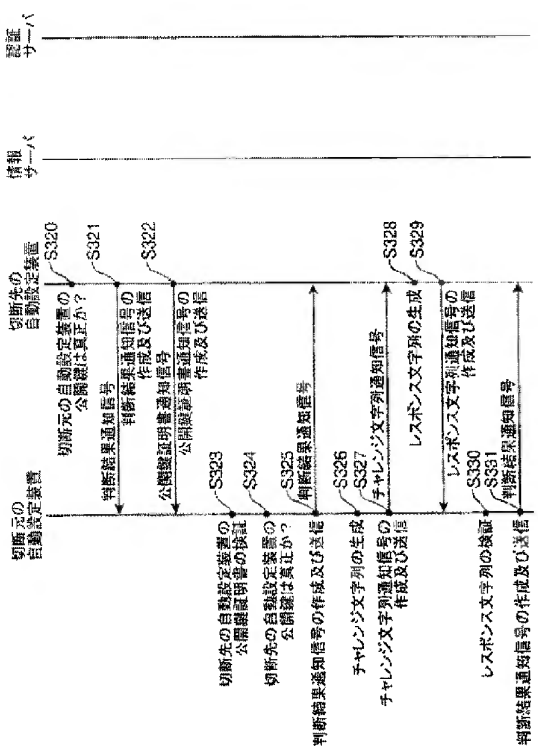
【図20】

【図21】

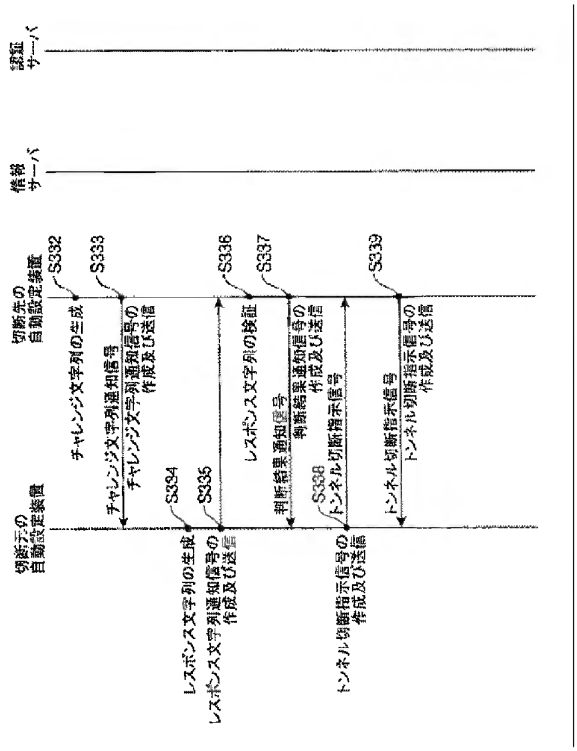
【図22】

【図23】

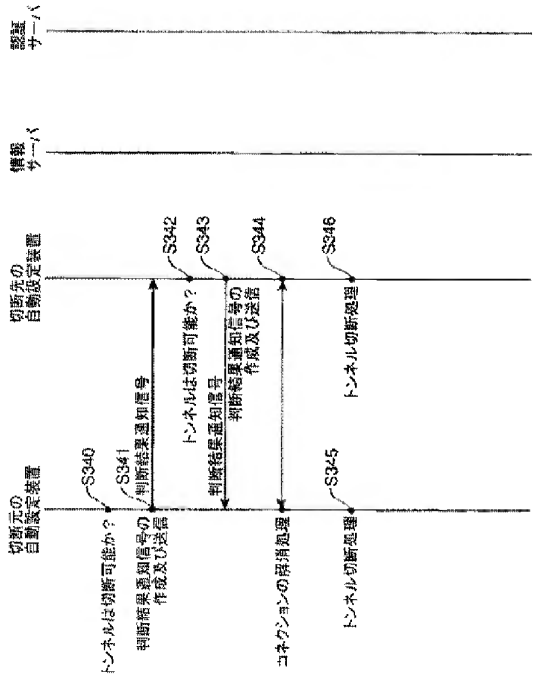
【図24】



【図25】



【図26】

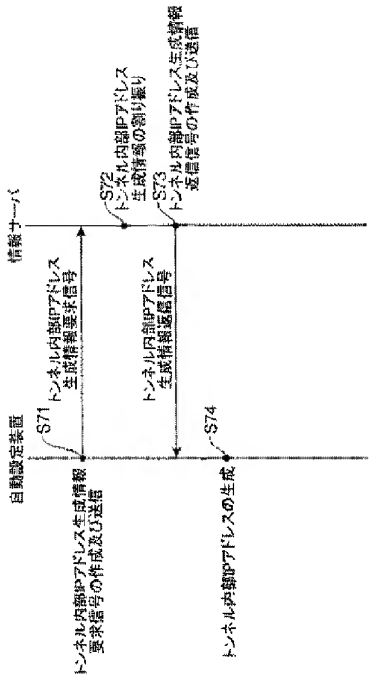


【図27】

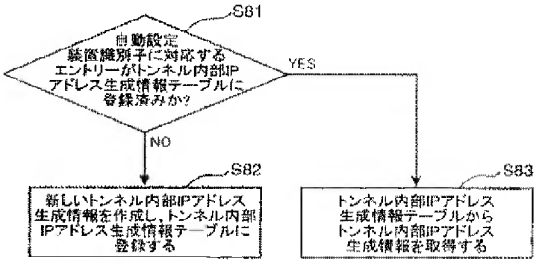
トンネル内部IPアドレス生成情報テーブル　106

161 管理番号	162 自動設定装置識別子	163 トンネル内部IPアドレス生成情報
1	00000001	2001:DB8:0:0001::/64
2	00000002	2001:DB8:0:0011::/64
3	00000003	2001:DB8:0:0021::/64
・・・・	・・・・・	・・・・・

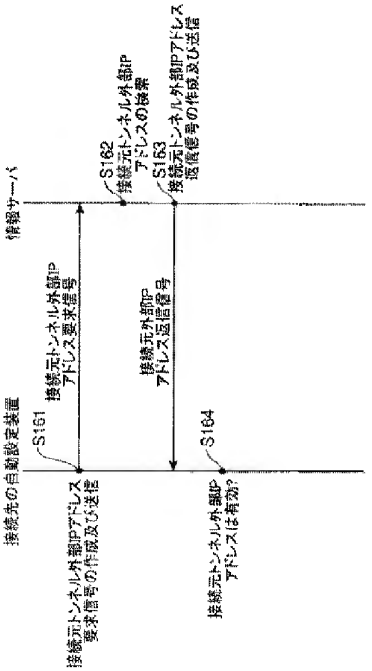
【図28】



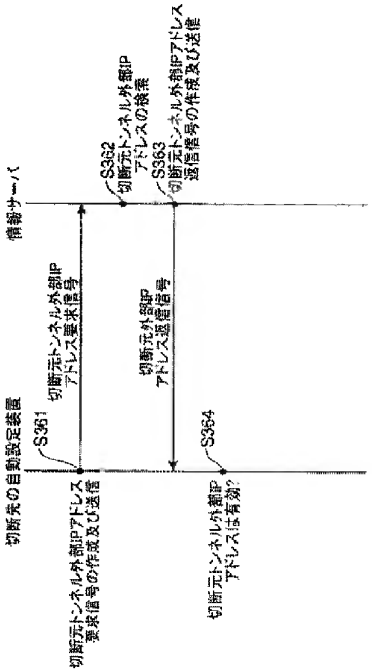
【図29】



【図30】



【図31】

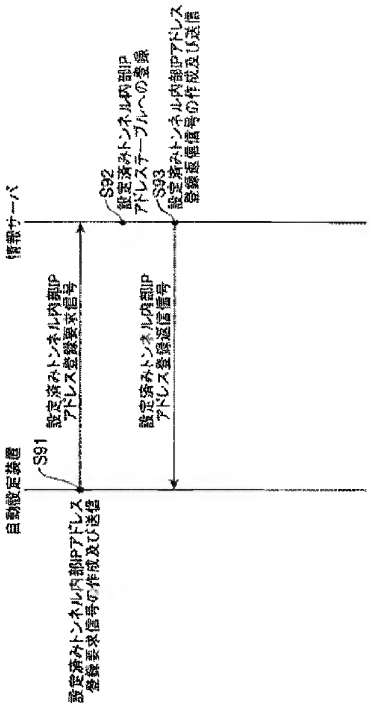


【図32】

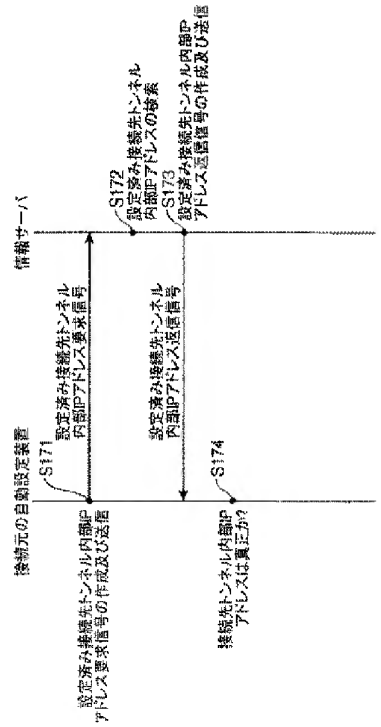
設定済みトンネル内部IPアドレステーブル　107

171 管理番号	172 自動設定装置識別子	173 設定済みトンネル内部IPアドレス
1	2001:DB8:0:0001::/64	2001:DB8:0:0001::/64
2	2001:DB8:0:0011::/64	2001:DB8:0:0011::/64
3	2001:DB8:0:0021::/64	2001:DB8:0:0021::/64
・・・	・・・	・・・

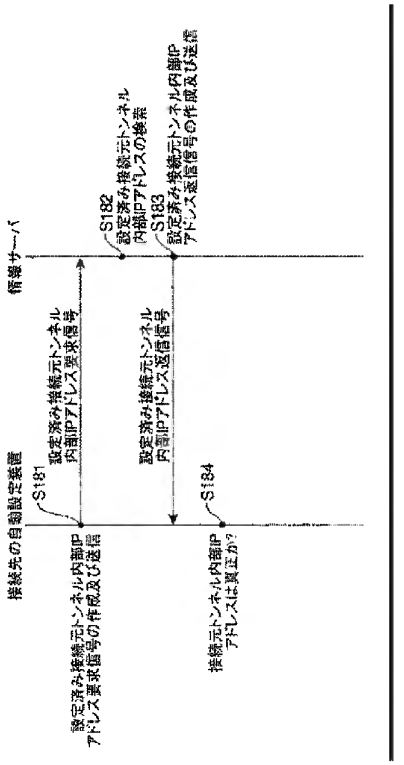
【図33】



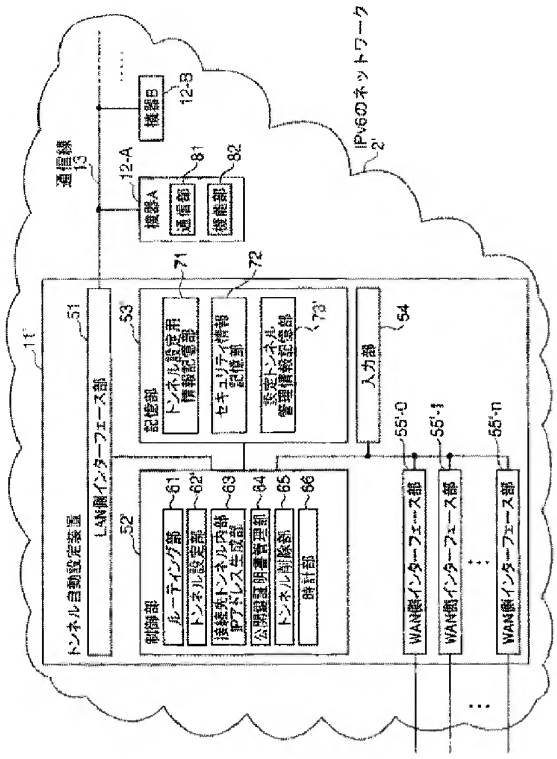
【図34】



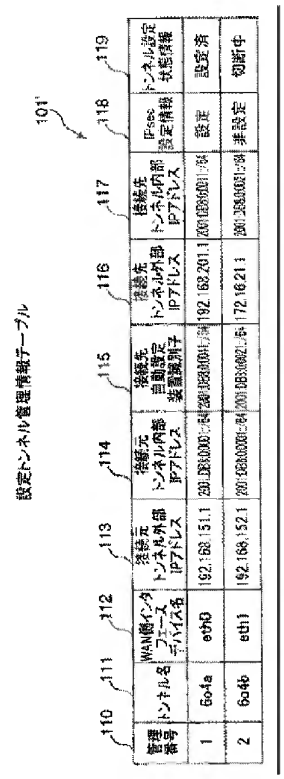
【図35】



【図36】



【図37】



【図38】

提供トンネル設定情報テーブル　102'

121 管理番号	122 WAN側インタフェースデバイス名	123 自動設定装置識別子	124 トンネル外部IPアドレス
1	eth0	2001:DB8:0:0001::/64	192.168.151.1
2	eth1	2001:DB8:0:0001::/64	192.168.152.1
3	eth0	2001:DB8:0:0011::/64	192.168.201.1
4	eth0	2001:DB8:0:0021::/64	172.16.21.1
...	...	...	...

(72)発明者　高添　智樹
大阪府門真市大字門真１０４８番地　松下電工株式会社内
(72)発明者　松田　和宏
東京都新宿区西新宿１－２６－２　株式会社インターネット総合研究所内
(72)発明者　黒木　秀和
東京都新宿区西新宿１－２６－２　株式会社インターネット総合研究所内
(72)発明者　水嶌　友昭
東京都新宿区西新宿１－２６－２　株式会社インターネット総合研究所内
(72)発明者　荻野　司
東京都新宿区西新宿１－２６－２　株式会社インターネット総合研究所内
Ｆターム(参考)　5J104 EA05　KA01　KA05　PA07
5K067 AA30　BB21　DD17　DD30　DD57　EE16　HH24　HH36　KK15

AMENDMENTS TO THE SPECIFICATION

Please amend paragraph [0449] of the specification as follows:

[0449] Similarly, any suitable encryption keys may be secured within one or more shares of data according to any suitable algorithm such as the Shamir secret sharing algorithm. For example, encryption keys used to encrypt a data set prior to parsing and splitting, encryption keys used to encrypt a data portions after parsing and splitting, or both may be secured using, for example, the Shamir secret sharing algorithm or any other suitable algorithm.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Statutory or Terminal Disclaimer	1814	1	160	160
		Total in USD ($)		**340**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated April 11, 2013, please amend the above-identified U.S. patent application as follows:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Remarks/Arguments begin on page 9 of this paper.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 104093-0002-105

In re Application of: Orsini et al.

Application No.: 13/371,363

Filed: February 10, 2012

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

The owner*, Security First Corp., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 8,271,802

as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney or agent of record. Reg. No. 70,069

/Christopher J. Han/ — Signature
July 11, 2013 — Date

Christopher J. Han — Typed or printed name

(617) 951-7000 — Telephone Number

☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

36779335_1

REMARKS

Applicants amend independent claim 1 to clarify the claimed invention; and the specification to improve clarity. The amendments are fully supported by the specification and do not add new matter. Applicants respectfully traverse the rejections and request reconsideration and withdrawal of the same in light of the following remarks:

Summary of Examiner Interview

The undersigned wishes to thank Examiner Chao for the courtesies extended during the telephonic interviews conducted on Tuesday, May 21, 2013 and Wednesday, June 26, 2013. During the interviews, the undersigned, his colleague Regina Sam (Reg. No. 67,362), and the Examiner discussed the rejections under § 101, § 112, and § 103.

The Terminal Disclaimer Overcomes the Double Patenting Rejection

The Examiner rejected claims 1-27 under obviousness-type non-statutory double patenting over U.S. Patent No. 8,271,802. Without concurring in the rejection, but solely to advance prosecution, Applicants submit herewith a Terminal Disclaimer, thereby obviating the rejection. Accordingly, Applicants respectfully request that the double-patenting rejection be withdrawn.

Independent Claim 1 Recites Patentable Subject Matter Under § 101

The Examiner rejected claims 1-9 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. See Office Action pg. 4.

In order to expedite prosecution, and without conceding the issue of patentability, Applicants have amended independent claim 1 to specify that the step of encrypting is performed by processing circuitry. The Examiner agreed during the interview on May 21, 2013 that this amendment would overcome the § 101 rejection. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection under 35 U.S.C. § 101 for claims 1-9.

The Amended Specification Satisfies the Written Description Requirement of § 112

The Examiner rejected claims 6, 15, and 24 as allegedly containing subject matter which was not sufficiently described in the specification. In particular, the Examiner objected to the addition of "secret sharing" to the above-identified claims, contending that Applicant's specification did not adequately describe secret sharing algorithm. Without concurring in the rejection, but in order to advance prosecution, Applicants have amended paragraph 449 of the specification to explicitly recite "Shamir secret sharing." Support for this amendment can be found in at least U.S. Provisional Application No. 60/718,185 (see, *e.g.*, pages 178, 256, 264, 270, 275, and 277), to which the present application claims priority, and which was incorporated by reference in the specification. The Examiner agreed during the interview on May 21, 2013 that this amendment would overcome the § 112 rejection and would not raise a new matter issue. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection under 35 U.S.C. § 112 for claims 6, 15, and 24.

Independent Claims 1, 10, and 19 Patently Distinguish over the Cited References

Independent claims 1, 10, and 19 are rejected under 35 U.S.C. § 103 as being allegedly obvious from Krawczyk, Secret Sharing Made Short ("SSMS") in view of Krawcyzk, Distributed Fingerprints and Secure Information Dispersal ("DFSID"), and Li U.S. Patent Application Publication No. 2006/0080454 ("Li"), or in the alternative, Hand, Spread Spectrum Storage with Mnemosyne ("Hand"). Applicants respectfully traverse the rejection.

Independent claim 1 recites, *inter alia*, generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed. Independent claims 10 and 19 recite a non-transitory computer readable medium and a computer system, respectively, directed towards similar subject matter as independent claim 1.

During the interview on June 26, 2013, the Examiner indicated that none of DFSID, Li, and Hand show this claimed feature. Rather, the Examiner contended that SSMS teaches the claimed generating data splitting information step, by reference to "information dispersal" in § 3. Applicants respectfully disagree. The cited section states

> *Information dispersal* was introduced by Rabin [15]. It is a scheme intended for the distribution of a piece of information among n active processors, in such a way that the recovery of the information is possible in the presence of m active processors (i.e. out of m fragments), where m and n are parameters satisfying $1 \leq m \leq n$ . . . **The basic idea is to add to the information, say a file F, some amount of redundancy and then to partition it into n fragments, each transmitted to one of the parties.** Reconstruction of F is possible out of m (legitimate) fragments.

(SSMS, § 3, emphasis added).

The cited section discusses adding redundancy information to original data so that the data can be recovered from less than all of the initial pieces. Nowhere in the above-cited section, however, does SSMS describe data splitting information which determines into which of a plurality of shares of data a unit of data of an encrypted data set will be placed. Specifically, the redundancy information does not indicate how a particular unit of original data ends up in a particular fragment; rather the redundancy information is added to the original data and is itself distributed along with the original data. Moreover, while SSMS discusses "partitioning" a file F into n fragments, SSMS does not describe *how* any data units from the file F *are* distributed into the n fragments – i.e., there is no discussion of how any of the n fragments is composed, much less a discussion of generating data splitting information which determines into which of the n fragments a unit of data from the file F is placed. The mere fact of "partitioning" does not suggest generating data splitting information usable to determine into which of a plurality of shares of data a unit of data will be placed.

For at least the forgoing reasons, Applicants respectfully submit that SSMS, DFSID, Li, and Hand, either alone or in combination, fail to describe, teach, or suggest all of the elements of independent claims 1, 10, and 19 (or any of claims 2-9, 11-18, and 20-27 that depend therefrom). Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejections of claims 1-27 under 35 U.S.C. § 103.

Conclusion

For at least the reasons set forth above, Applicants respectfully submit that claims 1-27 are allowable and that this application is in condition for allowance. Reconsideration and prompt allowance of this application are respectfully requested.

Applicants believe no fee is due with this response other than as indicated on the Fee Transmittal submitted concurrently herewith. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: July 11, 2013

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application.

Listing of Claims

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. (Original) The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. (Original) The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. (Previously Presented) The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

7. (Original) The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. (Original) The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. (Original) The method of claim 1, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

10. (Previously Presented) A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. (Original) The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. (Previously Presented) The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

16. (Original) The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. (Original) The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. (Original) The non-transitory computer readable medium of claim 10, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

19. (Previously Presented) A computer system for securing a data set, the system comprising:

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. (Original) The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. (Original) The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. (Previously Presented) The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir secret sharing algorithm.

25. (Original) The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. (Original) The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. (Original) The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/371,363	ORSINI ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 11 JUL 2013	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
JAB

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	16348675
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/joanne ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	18-JUL-2013
Filing Date:	10-FEB-2012
Time Stamp:	11:52:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	10053
Deposit Account	061075
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	79173 f60e29b168c1abf875a4426edf52b4a5bfcd2afe	no	3
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	127451 17e5bdf2685d9e648a79cfe00146e35adf362cb7	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	Xu_et_al_Locality_Driven_Key_Management_Architecture.pdf	1551641 f5cba8620c561d141f815ac9b34bdb725fd888bb4	no	11
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30571 776060d9f895d1fd616fb89fb8db527d8888e286	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1788836		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/joanne ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed more than three months after the U.S. filing date, OR more than three months after the date of entry of the national stage of a PCT application, AND after the mailing date of the first Office Action on the merits, whichever occurs first, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith a copy of non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, Applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases that have not been previously submitted are submitted herewith, and a corresponding entry for the Examiner's initials has been added on the form PTO/SB/08b filed concurrently herewith. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	**Publication No.**	**Attorney Docket No.**	**Filing Date**	**Status**
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/371,364	US 2012-0159197	104093-0002-106	2/10/2012	Pending

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 06-1075 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: July 18, 2013

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2007/0071234	03-29-2007	Lagrange et al.	
		US-2007/0124584	05-31-2007	Gupta	
		US-2007/0162744	07-12-2007	Hoshino et al.	
		US-2009/0304004	12-10-2009	Huynh Van et al.	
		US-2010/0054474	03-04-2010	Schneider	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Xu, "Locality Driven Key Management Architecture for Mobile Ad-hoc Networks," 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems," pgs. 436-446.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed more than three months after the U.S. filing date, OR more than three months after the date of entry of the national stage of a PCT application, AND after the mailing date of the first Office Action on the merits, whichever occurs first, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, Applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases that have not been previously submitted are submitted herewith, and a corresponding entry for the Examiner's initials has been added on the form PTO/SB/08b filed concurrently herewith. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, Applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	**Publication No.**	**Attorney Docket No.**	**Filing Date**	**Status**
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/371,364	US 2012-0159197	104093-0002-106	2/10/2012	Pending

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 06-1075 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: August 21, 2013

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2007/0162744	07-12-2007	Hoshino et al.	
		US-8,060,832	11-15-2011	Kruempelmann et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	16650176
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Joanne Ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	21-AUG-2013
Filing Date:	10-FEB-2012
Time Stamp:	17:23:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	4692
Deposit Account	061075
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	79085 478900cba99692bcb919ac66bff8518a5b800ae9	no	3
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	125788 b0e88e773412e1662ee5a767654d2c74250d4cde	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (SB06)	fee-info.pdf	30499 6f4d31663f91a995915fc68cd7fe2f8ece6f3aab	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	235372		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Rabin et al., Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance, 1989, Retrieved from the Internet <URL: dl.acm.org/citation.cfm?id=62050>, pp 1-14 as printed.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/17/2013	mc

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-2007/0071234	03-29-2007	Lagrange et al.	
/M.C./		US-2007/0124584	05-31-2007	Gupta	
/M.C./		US-2007/0162744	07-12-2007	Hoshino et al.	
/M.C./		US-2009/0304004	12-10-2009	Huynh Van et al.	
/M.C./		US-2010/0054474	03-04-2010	Schneider	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	09/06/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

37008896_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.C./		Xu, "Locality Driven Key Management Architecture for Mobile Ad-hoc Networks," 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems," pgs. 436-446.	

Examiner Signature	/Michael Chao/	Date Considered	09/06/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

37008896_1

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/02/2012	07/16/2012	03/12/2013	09/06/2013					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					
	21	✓	✓	✓	✓					
	22	✓	✓	✓	✓					
	23	✓	✓	✓	✓					
	24	✓	✓	✓	✓					
	25	✓	✓	✓	✓					
	26	✓	✓	✓	✓					
	27	✓	✓	✓	✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(fountain OR erasure OR tornado OR raptor OR rateless) adj (coding or codes) encrypted key (hash OR fingerprint OR checksum) and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:43
L2	0	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 encrypted key (hash OR fingerprint OR checksum) and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:43
L3	1	(orsini and rick or hare and mark or davenport and rojer or winick and steven).in. and @pd>"20130411"	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2013/07/17 09:43
L4	1	(security adj first).asn. and @pd>"20130411"	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2013/07/17 09:43
L5	27	726/27.ccls. and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:46
L6	9	713/153.ccls. and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:46

7/ 17/ 2013 9:48:16 AM
C:\ Users\ mchao\ Documents\ EAST\ Workspaces\ 13371363.wsp

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-2007/0162744	07-12-2007	Hoshino et al.	
/M.C./		US-8,060,832	11-15-2011	Kruempelmann et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	09/06/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

37710693_1

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,307,443	11-06-2012	Wang et al.	
		US-8,261,265	09-04-2012	Chen et al.	
		US-8,250,643	08-21-2012	Enomoto et al.	
		US-8,195,976	06-05-2012	Rao et al.	
		US-8,060,088	11-15-2011	Ihattula	
		US-7,926,090	04-12-2011	Blevins et al.	
		US-7,921,288	04-05-2011	Hildebrand	
		US-7,865,741	01-04-2011	Wood et al.	
		US-7,801,781	09-21-2010	Olin et al.	
		US-7,756,792	07-13-2010	Hughes	
		US-7,752,482	07-06-2010	Gredone et al.	
		US-7,721,150	05-18-2010	Belyakov et al.	
		US-7,623,809	11-24-2009	Nakano et al.	
		US-7,535,905	05-19-2009	Narayanan et al.	
		US-7,478,427	01-13-2009	Mukherjee et al.	
		US-7,428,754	09-23-2008	Neumann et al.	
		US-7,363,361	04-22-2008	Tewari et al.	
		US-7,346,925	03-18-2008	Marcjan	
		US-7,140,044	11-21-2006	Redlich et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		JP-2006-174152-A	06-29-2006	Matsushita Electric Works Ltd.		√

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,107,385	09-12-2006	Rajan et al.	
		US-7,085,854	08-01-2006	Corente	
		US-7,003,668	02-21-2006	Berson et al.	
		US-6,915,436	07-05-2005	Booth, III et al.	
		US-6,785,768	08-31-2004	Peters et al.	
		US-6,505,216	01-07-2003	Schutzman et al.	
		US-6,415,373	07-02-2002	Peters et al.	
		US-5,666,514	09-09-1997	Cheriton	
		US-5,623,549	04-22-1997	Ritter	
		US-5,603,003	02-11-1997	Akizawa et al.	
		US-2013/0042105	02-14-2013	Orsini et al.	
		US-2012/0266231	10-18-2012	Spiers et al.	
		US-2012/0255035	10-04-2012	Orsini et al.	
		US-2012/0255034	10-04-2012	Orsini et al.	
		US-2011/0145413	06-16-2011	Dawson et al.	
		US-2011/0093113	04-21-2011	Sager et al.	
		US-2010/0332617	12-30-2010	Goodwin et al.	
		US-2010/0318812	12-16-2010	Auradkar et al.	
		US-2010/0283734	11-11-2010	Hallbauer et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2010/0223613	09-02-2010	Schneider	
		US-2010/0125730	05-20-2010	Dodgson et al.	
		US-2010/0005028	01-07-2010	Hartley et al.	
		US-2009/0305900	12-10-2009	Belouchi et al.	
		US-2009/0300284	12-03-2009	Murotani et al.	
		US-2009/0292919	11-26-2009	England	
		US-2009/0209232	08-20-2009	Cha et al.	
		US-2009/0113203	04-30-2009	Tsuge et al.	
		US-2009/0097657	04-16-2009	Scheidt et al.	
		US-2009/0092252	04-09-2009	Noll et al.	
		US-2008/0240441	10-02-2008	Kawakami	
		US-2008/0232592	09-25-2008	Lee et al.	
		US-2008/0155252	06-26-2008	Nambiar	
		US-2008/0126614	05-29-2008	Ooi et al.	
		US-2008/0072035	03-20-2008	Johnson et al.	
		US-2008/0046752	02-21-2008	Berger et al.	
		US-2008/0016334	01-17-2008	Kurapati et al.	
		US-2007/0097885	05-03-2007	Traversat et al.	
		US-2006/0165060	07-27-2006	Dua	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages. Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2006/0078127	04-13-2006	Cacayorin	
		US-2006/0046728	03-02-2006	Jung et al.	
		US-2005/0198306	09-08-2005	Palojarvi et al.	
		US-2005/0160290	07-21-2005	Moon et al.	
		US-2005/0132060	06-16-2005	Mo et al.	
		US-2005/0071631	03-31-2005	Langer	
		US-2004/0122960	06-24-2004	Hall et al.	
		US-2003/0084290	05-01-2003	Murty et al.	
		US-2003/0061481	03-27-2003	Levine et al.	
		US-2003/0023958	01-30-2003	Patel et al.	
		US-2003/0005094	01-02-2003	YUAN et al.	
		US-2002/0184444	12-05-2002	Shandony	
		US-2002/0178361	11-28-2002	Genty et al.	
		US-2002/0141590	10-03-2002	Montgomery	
		US-2002/0023210	02-21-2002	Tuomenoksa et al.	
		US-2002/0016926	02-07-2002	Nguyen et al.	
		US-2007/157025	07-05-2007	Sastry et al.	
		US-2010/0077252	03-25-2010	Siewert et al.	
		US-2010/0306578	12-02-2010	THORNTON et al.	
		US-8,397,288	03-12-3013	Melvin, Jr. et al.	
		US-8,341,115	12-25-2012	Natanzon et al.	
		US-8,261,084	09-04-2012	Nonaka et al.	
		US-7,743,261	06-22-2010	Nonaka et al.	
		US-7,596,741	09-29-2009	LaVigne et al.	
		US-7,549,061	06-16-2009	Nonaka et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Dierks, "The Transport Layer Security Protocol," RFC 4346m Version 1.1, April 2006, 86 pages	
		Johnson, "MLS-Net and Secure Parser: A New Method for Securing and Segregating Network Data" [Online] 8-July 2007"XP002582437 5th International Symposium on Risk Management and Informatic: WMS12007, Orlando Florida, USA	
		Kent, "Security Architecture for the Internet Protocol," RFC 2401, November 1998, 67 pages.	
		Kroç, Erol, "Access Control in Peer-to-Peer Storage Systems," 1 Oct 2006, XP55036196, Retrieved from the Internet: URL:ftp://ftp.tik.ee.ethz.ch/pub/studfents/2006-So/MA-2006-10.pdf [retrieved on 2012-08-23] page. 61-62	
		Pattam, "Enhancing Security in 802.11 and 802.1X Networks with Intrusion Detection," Jan. 20, 2006, Univ. of New Orleans Theses and Dissertations, Paper 1034, 111 pages	
		Sengar et al., "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network," Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, 8 pages (2005)	
		Copies of Office Actions and Replies for U.S. Application No. 12/148,365 (104093-0001-102)	
		Copies of Office Actions and replies for U.S. Application No. 13/024,791 (104093-0001-103)	
		Copies of Office Actions and replies for U.S. Application No. 13/024,804 (104093-000-104)	
		Copies of Office Actions and Replies for U.S. Application No. 13/371,364 (104093-0002-106)	

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 09/17/2013

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
09/17/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No. 13/371,363	Applicant(s) ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 July 2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-27* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Continuation of Attachment(s) 2). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :7/11/2013, 7/18/2013, 8/21/2013.

DETAILED ACTION

This action is in response to argument filed 7/11/2013. Application 13/371,363 claims priority to 10/25/2004. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 7/11/2013 was filed after the mailing date of the Non-Final OA on 4/11/2013. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

The following references in the IDS do not appear relevant and have not been "considered."

Belouchi et al., US 2009/0305900, Genemap of the Human Genes Associated with Longevity.

The information disclosure statement filed 8/21/2013, 7/18/2013 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because it does not provide (b) a column that provides a space next to each document listed to permit the examiner's initials. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing

the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

The portions of these IDSs that list related applications cannot be considered because they are not in a form that allows the Examiner to mark them as considered. In addition, they are not documents but rather constitute entire prosecution histories. Although the Examiner is aware of the co-pending and allowed cases, he cannot "consider" an entire prosecution history.

Response to Arguments

Applicant's arguments filed 7/11/2013 have been fully considered but they are not persuasive.

It is a principle of patent prosecution that the Applicant may act as his own lexicographer and define the invention in any terms he deems fit. This benefit is counterbalanced by the requirement that claims are given their broadest reasonable construction in light of the specification (see MPEP 2111). This counterbalance is required because without broadly construing the claim terms in view of the detailed description an Applicant could create his own terms and then merely claim the prior art does not feature said terms; such would frustrate the purpose of 35 USC 102 and 103.

Thus, while the Applicant may use any terminology he desires, the terminology is afforded only the meaning required by the claim viewed in light of the specification. The result of these axioms is that when Applicant points out distinctions between the prior art and the claimed invention it is useful to provide supporting citations to the

specification so that Applicant's arguments can gain the benefit of the context of the Application. This is especially true when the Applicant and the Examiner disagree as to the meaning of a claim term; which is the present issue.

For example, if Applicant responds by an argument directed toward a particular limitation and provides a citation to an embodiment of the specification to which he avers the claim requires; the Examiner might respond by pointing out other possible interpretations, or alternatively by pointing out portions of the detailed description which are not presently claimed. This would clarify both the Applicant's and the Examiner's position for the benefit of both parties as well as any parties which must review the prosecution history.

Presently, Applicant and Examiner disagree as to the appropriate interpretation of "data splitting information". The Examiners position is that the term is defined by the context in which it is recited by the claim. Applicant's position is that the "data splitting information" requires *"information which determines into which of the n fragments a unit of data from the file F is placed."* (Applicant's Arguments p. 11 ¶ 2). In the prior art systems cited below, the Krawczyk references, referred to as SSMS and DFSID, the file F is split into n fragments ("2. Using IDA partition the encryption file E into n fragments, $E_1, E_2, \ldots, E_n$." SSMS p. 6). Applicant further states that *"The mere fact of 'partitioning' does not suggest generating data splitting information usable to determine into which of a plurality of shares of data a unit of data will be placed"* (Applicant's Arguments p. 11 ¶ 2).

However, to the Examiner, it is self-evident that any system that uses IDA to partition data either uses IDA as “data splitting information”, or IDA must inherently include “data splitting information” to partition the file. The key issue at this point, is what Applicant intends “data splitting information" to be, which of course, would require citations to the detailed description. In this respect the arguments are lacking.

What follows is an overly verbose discussion of the claimed invention and the mapping of the prior art thereto. While not critical to the Examiner's response (see above) it may be useful to gain insight into the Examiner’s analysis of the claim.

Applicant’s sole argument is that the cited prior art Krawczyk (Secret Sharing made Short) SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) DFSID, in view of {Li or, in the alternative, Hand} does not disclose “splitting information”. This argument is not persuasive for reasons detailed below.

Background

In a prior action dated 7/26/2012 the Examiner had rejected claims 6, 15, and 24 as failing to fulfill the written description requirement because a "Shamir algorithm" was not described in the specification. Adi Shamir is a cryptographer who has authored

numerous algorithms, the most common of which is the RSA algorithm. In response to this rejection Applicant's pointed to, and have now amended the specification to include (see remarks p. 10) "Shamir secret sharing algorithm" as detailed in the provisional Application 60/718,185.

Upon the performance of an updated search for “Shamir secret sharing”, the Krawczyk references were found and applied in a rejection; where the DFSID reference explicitly contemplated its use with SSMS (DFSID § 5 and NFOA 4/11/2013 p. 9 ll. 9-11).

These two Krawczyk references have been (NFOA 4/11/2013) and are currently cited as disclosing all the claimed limitations with the exception of “splitting information” and the rearranging the shares of claims 4, 13 and 22. While the Krawczyk reference discloses the invention in nearly identical language, no “splitting information” was found. Thus, the Examiner believed that Krawczyk did not disclose such and it became necessary to determine how the splitting information was used.

Claim 1 recites:

“generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares a data unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information

. . .

Causing the plurality of shares to be stored in respective separate storage locations;

. . . ."

SSMS discloses the following analogous steps (absent the splitting information).

"2. Using IDA partition the encrypted file E into n fragments, El, Ez,. . . ,En.

3. . . .

4. Send to each participant Pi, i = 1'2,. . . ,n the share Si = (E;, Ki). The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." (SSMS p. 6).

As disclosed by the prior art (SSMS, DSFID) n shares are created which are indistinct such that any threshold m number is sufficient to reconstruct the file (SSMS p. 6)(also Applicant's claim 1). (The details of this will be discussed later in the Prior Art Splitting section.) If shares are indistinct, then what use is the "data splitting information [is] usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed"? In addition, any system which "separate[ed] the encrypted data set" would inherently disclose "splitting information," which would make the splitting information limitation superfluous unless it required something more, an implied limitation, or a reason to place data in a particular share.

The answer must be that the shares are not indistinct, and the only distinction in the claim is which "storage location" the share is sent to. Note that claim 4, requires rearrangement of the data in the share, which would have no utility unless it changed

where the data was located at (since any m number of shares can reconstruct the file, switching the data of the shares among storage locations would perform no action). At the time, a brief inspection of the specification did not yield a definition, or any other recitation of the term "splitting information". Thus, the Examiner interpreted the "splitting information" to define how to distribute the data of the encrypted file to physical locations. In other words, the Examiner interpreted the context of the shares in the claim to define how the "data splitting information" is used. In accordance with this interpretation, and the understanding that the Krawczyk references were agnostic with regard to where the particular data was sent the Li or Hand references were combined which featured particular algorithms for managing analogously coded data distribution.

("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109])

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

However, Applicant responds in the present remarks (p. 10-11) and during the most recent interview 6/26/2013 (noted in remarks p. 10) that this interpretation was incorrect and that the data splitting information determines which logical "share" the data goes into (how the data is separated) rather than what storage location the share is destined (What Li and Hand were cited for). Thus, the Examiner is again stuck with the

conundrum of determining an appropriate interpretation of "data splitting information" and to contrast that with the prior art method of partitioning ("2. Using IDA partition the encryption file E into n fragments, E_1, E_2, . . . , E_n." SSMS p. 6).

Applicant's Disclosure

As a preliminary note, the term "splitting information" was not found in the specification. Upon review of the figures, Figure 21-23 feature a block without a numeric indicator titled "Split data according to session key". The following description of which was found on ¶¶ 303-306: (see also ¶¶ 311-314, 320-322, 332-335)

> [0303] 1. Generating a session master key and encrypt the data using RSI stream cipher.
> [0304] 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.
> [0305] 3. In this embodiment of the method, the session master key will be stored along with the secured data shares in a data depository. Separating the session master key according to the pattern of the Parser Master Key and append the key data to the encrypted parsed data.
> [0306] 4. The resulting four shares of data will contain encrypted portions of the original data and portions of the session master key. Generate a stream cipher key for each of the four data shares.

Note that while these sections of the specification disclose that the "splitting information" is a "session master key," they do not disclose how it is actually used to define which data goes into the shares. This is irrelevant at this point because the prior art discloses a key that inherently determines which "data" is placed in the share.

Prior Art Splitting

SSMS was cited as disclosing the separating portion of the limitation: ("2. Using IDA partition the encryption file E into n fragments, E_1, E_2, . . . , E_n." SSMS p. 6)("3. Using PSS generate n shares for the key K" SSMS p. 6). SSMS defines IDA ("We assume a generic information dispersal algorithm that we denote by IDA" p. 6) as

"Information Dispersal was introduced by Rabin [15]" (§ 3). See also DFSID ¶ 2. The referenced Information Dispersal Algorithm is defined in Rabin et al. (Efficient Dispersal of Information for Security, Load Balancing, and Fault tolerance).

SSMS provides a brief disclosure of the workings of an IDA algorithm ("Remark:" beginning on SSMS p. 5) which "determine[s] into which of a plurality of shares a data unit of data of the encrypted data set will be placed".

> "For completeness, we outline the following simple information dispersal scheme based on Reed Solomon erasure codes. The information to be shared is partitioned into m equal parts where each part is viewed as an element over a finite field (e.g. GF@), for a large enough prime p) . These m elements are then viewed as coefficients of a polynomial of degree m - 1, and the n fragments for distribution are obtained by evaluating this polynomial in n different points. Clearly the whole information can be reconstructed (by interpolation) from any m fragments. We stress that for large files, it is not necessary to work on a huge field but just to view the information as the concatenation of different polynomials. Notice the difference between such a scheme and Shamir's secret sharing in which the information is represented by the free coefficient and not by the whole polynomial (this is essential in Shamir's scheme to provide perfect secrecy but not for information dispersal where secrecy is not a concern)."

However to fully illustrate the workings of the prior art, the Rabin reference will now be discussed. While Rabin discloses the method in multitude of detail, the portion with which we are concerned is how the prior art IDA scheme splits the data. (Rabin p. 4)

The characters b_i may be considered as integers taken from a certain range $[0 \cdots B]$. For example, if the b_i are eight-bit bytes, then $0 \leq b_i \leq 255$. Take a prime $B < p$. For bytes, $p = 257$ will suffice; but we may wish to choose a prime larger than the smallest $B < p$. Note that with $p = 257$ there is an excess of one bit per byte, we shall see later how to implement IDA in fields $GF(2^s)$, $s = 8$ for bytes, without any excess. Now, F is a string of residues mod p, that is, a string of elements in the finite field Z_p. All the following computations are in Z_p, that is, mod p.

Choose an appropriate integer m so that $n = m + k$ satisfies $n/m \leq 1 + \epsilon$ for a specified $\epsilon > 0$. Choose n vectors $a_i = (a_{i1}, \ldots, a_{im}) \in Z_p^m$, $1 \leq i \leq n$, such that every subset of m different vectors are linearly independent. Alternatively, it will suffice to assume that with high probability, a randomly chosen subset of m vectors in $\{a_1, \ldots, a_n\}$ is linearly independent. We shall see later on how to satisfy each of these conditions.

The file F is segmented into sequences of length m. Thus

$$F = (b_1, \ldots, b_m), (b_{m+1}, \ldots, b_{2m}), \ldots.$$

Denote $S_1 = (b_1, \ldots, b_m)$, etc. For $i = 1, \ldots, n$,

$$F_i = c_{i1}, c_{i2}, \ldots, c_{iN/m},$$

where

$$c_{ik} = a_i \cdot S_k = a_{i1} \cdot b_{(k-1)m+1} + \cdots + a_{im} \cdot b_{km}. \tag{1}$$

It follows that $|F_i| = |F|/m$.

If m pieces of F_i say, $F_1, \ldots, F_m$ are given, we reconstruct F as follows. Let $A = (a_{ij})_{1 \leq i,j \leq m}$ be the $m \times m$ matrix whose ith row is a_i. It is readily seen that

$$A \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} c_{11} \\ \vdots \\ c_{m1} \end{bmatrix},$$

and hence

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = A^{-1} \cdot \begin{bmatrix} c_{11} \\ \vdots \\ c_{m1} \end{bmatrix}.$$

Denote the ith row of A^{-1} by $(\alpha_{i1}, \ldots, \alpha_{im})$, then in general, for $1 \leq k \leq N/m$,

$$b_j = \alpha_{i1}c_{1k} + \cdots + \alpha_{im}c_{mk}, \qquad 1 \leq j \leq N, \tag{2}$$

1

2 The prior art Rabin discloses "separating the encrypted data set into the plurality

3 of shares based on" linearly independent vectors a_i. This is how the prior art separates

the claimed "encrypted data". Rabin goes on to disclose that this is done using matrix multiplication through the inverse of the matrix A formed of vectors a_i.

Recall now that SSMS first encrypts the data S with key K before using IDA (Rabin or the Remark section on SSMS p. 5) to partition (separate) the data. Separating the data through a matrix multiplication (Rabin) or by evaluating the polynomial at different points (SSMS p. 5) is not like cutting a file into pieces and placing contiguous bits in various shares, rather, the matrix multiplication and polynomial evaluation creates each share based upon every byte in the input file. Thus, when the file is first encrypted, it is implicit that the encrypted/unencrypted files would generate distinct shares. Thus, the embodiment of Applicant's invention which separates data based on a Key, is inherently disclosed by the combination of SSMS in view of DFSID.

Claim Interpretation of "splitting information"

As seen above, through exploration of Applicant's specification (Applicant's Disclosure) and review of the structures of the prior art (Prior Art Splitting), the cited references SSMS in view of DFSID disclose the process of Applicant's specification ¶¶ 303-306. However, these paragraphs are unclaimed, thus the claim must be afforded a broadest reasonable interpretation. This means that, until clarified, the Examiner must maintain his prior claim interpretation; that the "splitting information" defines how to distribute the data of the encrypted file to physical locations.

Paradoxically this is a narrower interpretation than Applicant appears to be asserting (see remarks pp. 10-11), but when the claimed invention has features which are not detailed in the specification with similar language certain assumptions and interpretations must be made. In this instance, the Examiner was forced to assume that the claim required that the “splitting information” determined the physical storage locations. Even if Applicant's asserted interpretation of the claim were adopted, and the splitting information decided only into which logical share data would be placed, rather than Examiners interpretation of what physical location to store the share, such is an inherent feature of any system which "separate[s] the encrypted data set" and would therefore be disclosed solely by the Krawczyk references SSMS in view of DFSID, as detailed above in the Prior Art Splitting section.

Note that whether or not all the references (SSMS in view of DFSID in view of Li or Hand) are required to support the § 103 rejection, finality need not be withdrawn. See Fed. Reg. Vol. 76, No. 225 pp. 72278-79: “Factual Situations That Do Not Constitute a New Ground of Rejection . . . 3. Relying on fewer than all references in support of a § 103 rejection, but relying on the same teachings.”

Available at <URL: http://www.gpo.gov/fdsys/pkg/FR-2011-11-22/html/2011-29446.htm>.

Note that while the Examiner has highlighted an alternate interpretation of the claim, that the “splitting information" is a key which somehow determines how the shares are composed, and that this is shown by the combination of SSMS in view of

SFSID, the Examiner was still unable to determine how the splitting information "is usable to determine into which of a plurality of shares . . . ." In other words, the Examiner is unable to determine what differences may exist between the claimed "splitting information/session master key" and they Key of SSMS.

In future arguments it may be useful to point out which portions of the specification detail the use of the "splitting information," and any other potential disclosures that may be relevant to the claimed "splitting information," despite having dissimilar wording.

Applicant's argument, with respect to the prior art, is not persuasive, either because Applicant is arguing unclaimed features (Applicant's Disclosure ¶¶ 303-306) or because such is inherently disclosed by the prior art (Prior Art Splitting). While Applicant has asserted that there "is no discussion of how any of the n fragments is composed" (remarks p. 11 ¶ 2), SSMS discloses algorithms and information to separate a file both explicitly (Remarks on p. 5) and inherently by reference to the prior published Rabin IDA scheme (discussed above). As Applicant has provided no further definition of "splitting information" in the claim, and the Examiner was unable to determine how Applicant's specification might differ from the prior art, Applicant's argument is unpersuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-12, 14-21, and 23-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID, in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, SSMS teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("1. Choose a random encryption key K. Encrypt the secret S using the encryption function ENC under the key K, let E = $ENC_K(S)$" SSMS p. 6).

[creating hash information based on a hash operation using the data set;]

generating [data splitting] information, wherein the [data splitting] information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; (SSMS discloses information used to split the data into shares, see below, but does not disclose particularizing which share contains which

data. Although the claim does not draw a distinction between the two, it has been assumed that "data splitting information" requires the latter.)

("We assume a generic information dispersal algorithm that we denote by IDA, and which works for parameters n (number of file fragments) and m (number of required fragments to reconstruct the file)." SSMS p. 6)

("we outline the following simple information dispersal scheme based on Reed Solomon erasure codes. The information to be shared is partitioned into m equal parts where each part is viewed as an element over a finite field (e.g. GF@), for a large enough prime p) . These m elements are then viewed as coefficients of a polynomial of degree m - 1, and the n fragments for distribution are obtained by evaluating this polynomial in n different points." SSMS pp. 5-6. This details how the information used to determine into which of a plurality of shares data will be placed.)

separating the encrypted data set into the plurality of shares [based on the data splitting information;] ("2. Using IDA partition the encryption file E into n fragments, E_1, E_2, . . . , E_n." SSMS p. 6)("3. Using PSS generate n shares for the key K" SSMS p. 6)

including in the plurality of shares (a) data indicative of the encryption key and [(b) the hash information]; and ("4. Send to each participant P_i, I = 1, 2, . . . , n the share $S_i = (E_i, K_i)$. The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 7)

causing the plurality of shares to be stored in respective separate storage locations; (to each participant. SSMS p. 7. "The distribution process gets ~ 1 sin put the secret S (and the values of n and m) and generates n shares Sl, Sz, . . , , Sn, which are privately delivered to the system participants." SSMS p. 3) (where the system is a set of distributed servers "These constructions have many applications, especially in distributed scenarios where secrecy and integrity of information are to be protected. For example, consider a group of five servers sharing a data base of confidential information such that no pair of servers is allowed to learn about the information without

the collaboration of a third one. (That is, the system tolerates up to two corrupted servers without compromising the information)." SSMS p. 2)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The reconstruction process reconstructs the correct secret when input with any subset of m shares." SSMS p. 3)

SSMS does not disclose:

creating hash information based on a hash operation using the data set;

(b) the hash information;

Further, while SSMS explicitly and implicitly discloses "separating the encrypted data set into the plurality of shares [based on the data splitting information;]" which inherently contains some information on how to "separat[e] the encrypted data". SSMS does not disclose that the system is purposed to particularly select shares to store data in. Since the shares are indistinct,

("wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares." Applicants claim 1 "The reconstruction process reconstructs the correct secret when input with any subset of m shares." SSMS p. 3)

such that any share is useable in place of any other share, determining which data to place in a share is a superfluous limitation. There is, however, one interpretation that would allow 'splitting information which particularizes which share to store data in' to have meaning. Since the only distinction between the shares is that they are stored in distinct physical storage locations, the splitting information could define how to distribute the data into distinct physical locations. This would make "splitting information" meaningful, whereas otherwise, it would be an inherent feature of any system that

"separat[es] the encrypted data". SSMS does not disclose a particular method of data distribution:

data splitting information [is usable to determine into which of a plurality of shares data will be placed; which, in turn, determines into which respective storage location the data will be placed]

DFSID discloses an analogous algorithm purposed for use with SSMS (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]").

DFSID further creating hash information based on a hash operation using the data set;

(b) the hash information:

"1. Use IDA to distribute the file among the n processors. Denote by F_i the piece distributed to processor p_i.

2. Fingerprint each piece F_i, i = 1, . . , n, by the DFP method (as described in Section 3). That is, for each i, compute $H(F_i)$ and then distribute this value among all processors using the coding function C. (Each processor p_j gets a share s_{ij} corresponding to $H(F_i)$)." (DFSID § 4.1, see also § 4.1 generally)

A fingerprint is a hash, see DFSID § 3.

A person of ordinary skill in the art at the time of invention would have modified SSMS by including the fingerprint of DFSID. It would have been obvious to one of ordinary skill in the art at the time of invention to modify SSMS with DFSID since it was

suggested explicitly by DFSID (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]") and to solve the information integrity problem (DFSID Abstract).

SSMS in view of DFSID does not disclose a particular method of data distribution:

data splitting information [is usable to determine into which of a plurality of shares data will be placed; which, in turn, determines into which respective storage location the data will be placed]

In other words, SSMS in view of DFSID does not disclose a particular share distribution scheme.

(1) Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data (“each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server).” Li [0109]; alternatively “in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys.” Li [0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. (“the availability vector will include the media

erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined SSMS in view of DFSID with Li by using the concepts of Li to implement the distribution of shares (SSMS p. 2). It would have been obvious to one of ordinary skill in the art at the time of invention to combine SSMS in view of DFSID with Li in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

(2) In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined SSMS in view of DFSID with Hand by using the concepts of Hand to implement the distribution of shares (SSMS p. 2). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement necessary but unspecified functionality of SSMS in view of DFSID using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. (determinism is a necessary feature of any system that will retrieve obfuscated data)

With respect to claims 3, 12, 21, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2)

With respect to claims 5, 14, 23, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2)

With respect to claims 6, 15, 24, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm. ("In order to achieve a space efficient secret sharing scheme we combine an information dispersal scheme with a secure encryption scheme and a perfect (e.g. Shamir's) secret sharing scheme." SSMS § 3)

With respect to claims 7, 16, 25, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of including data indicative of the encryption key comprises:
encrypting the encryption key with a second key; and
including in the plurality of shares data indicative of the encrypted encryption key. ("The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 6. See also p. 7. Encryption requires a key of some kind.)

With respect to claims 8, 17, 26, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2).

With respect to claims 9, 18, 27, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over SSMS in view of DFSID in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, SSMS in view of DFSID in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified SSMS in view of DFSID in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of

ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

In the alternative, Claims 1-3, 5, 7-12, 14, 16-21, 23, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, Horne teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("In the protocol that we describe, S encrypts C with a key K and sends the encryption EK(C)to R." Horne 2.2 ¶ 3)

creating hash information based on a hash operation using the data set; ("In order to take part in the protocol ES requires the correct hash of the encrypted content, H(EK(C)), and the key K that decrypts the content. . . . we assume that S sent the pair K,H(EK(C))———————————— to ES in a preprocessing stage, together with a description of C." Horne 2.2 ¶ 3; see also Horne § 4.2)

generating data splitting information, ("A Straightforward Method Based on Error

Correcting Codes" Horne § 4.1) [wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;]

separating the encrypted data set into the plurality of shares based on the data splitting information; ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and ("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7; "The reconstruction operation of R should therefore be to decrypt each block, examine its signature, and if it is correct use the block in the reconstruction of the original content." Horne § 4.1. Signatures are encrypted hashes. "After receiving this message R picks a small random set of the encrypted encoded blocks (where is a parameter to

be defined below). It sends to ES this set of encrypted blocks, together with their indexes and the encrypted message that is directed from S to ES." Horne § 4.1 ¶ 3; "In order to verify the encrypted content that it receives from S, R should forward this signature and randomly chosen encrypted blocks to ES." Horne § 4.2 ¶ 8)

causing the plurality of shares to be stored in respective separate storage locations; (Horne § 5 ¶ 4)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

Although Horne discloses that a distributed storage system may be used (Horne § 5 ¶ 4) it does not disclose how the data is distributed among the stores, as claimed:

wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller

than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]; alternatively "in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. ("the availability vector will include the media erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined Horne with Li by using the concepts of Li to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Li in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting

information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

Also Hand uses the hash of data as its identifier ("GUID for an archival fragment is a secure hash over the data it holds." Hand § 4.1)

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined Horne with Hand by using the concepts of Hand to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique.

("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]) ("The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K." Hand § 27.2 ¶ 6-7).

With respect to claims 3, 12, 21, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs)

With respect to claims 5, 14, 23, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing

the plurality of shares to have a substantially random distribution of the encrypted data set. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs).

With respect to claims 7, 16, 25, Horne in view of Li or Hand discloses: wherein the step of including data indicative of the encryption key comprises:

Encrypting the encryption key with a second key; and. ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2)

Including in the plurality of shares data indicative of the encrypted encryption key.("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7).

With respect to claims 8, 17, 26, Horne in view of Li or Hand discloses: further comprising the method step of storing the second key outside of the plurality of shares

("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2; ES is distinct from source S and receiver R), wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

With respect to claims 9, 18, 27, Horne in view of Li or Hand discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, Horne in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival

copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified Horne in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 6, 15, 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne)] in view of SSMS.

With respect to claims 6, 15, and 24 Horne in view of Li or Hand discloses: wherein the data indicative of the encryption key comprises data created using a [Shamir secret sharing algorithm]. ("The encryption can be done using public key cryptography" Horne § 2.1.2 ¶ 5) ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2). While Horne does disclose the use of a public key encryption, it does not disclose a Shamir Algorithm. SSMS discloses a Shamir secret sharing algorithms use with coded data ("In order to achieve a space efficient secret sharing scheme we combine an information dispersal scheme with a

secure encryption scheme and a perfect (e.g. Shamir's) secret sharing scheme." SSMS § 3). A person of ordinary skill in the art at the time of invention would have modified Horne in view of {Li or, in the alternative, Hand} with SSMS by utilizing the key splitting mechanism of SSMS with the combination. It would have been obvious to one of ordinary skill in the art at the time of invention to use the key splitting of SSMS in order to create space efficient secured secret shares (SSMS § 1).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Chao/
Examiner, Art Unit 2492

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed after the mailing date of a Final Office Action or Notice of Allowance, whichever occurred first, but on or before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Supplemental Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(2), that no item of information contained in this Supplemental Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Supplemental Information Disclosure Statement

was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Supplemental Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 06-1075 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: November 15, 2013

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/joanne ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,347,084	01-01-2013	Tavernier et al.	
		US-8,208,897	06-26-2012	Kaneko et al.	
		US-8,189,769	05-29-2012	Ramasamy et al.	
		US-7,934,100	04-26-2011	Fujimaki	
		US-7,657,760	02-02-2010	Teramoto et al.	
		US-7,234,063	06-19-2007	Baugher et al.	
		US-7,171,685	01-30-2007	Batra et al.	
		US-6,701,303	03-02-2004	Dunn et al.	
		US-2008/0270603	10-30-2008	Berger et al.	
		US-2007/0033644	02-08-2007	Thomas et al.	
		US-2004/0268148	12-30-2004	Karjala et al.	
		US-2002/0075844	06-20-2002	Hagen	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Mondal, "Mobile IP," Chapter 7, Fluwer Academic/Plenum Publishers, New York, pp. 173-202 (2003)	
		Nacht, "The Spectrum of Modern Firewalls," Computers & Security, 16 (1997), pp. 54-56.	
		Shaw et al (eds.), "Handbook on Electronic Commerce, Conway, Chapter 31, Springer-Verlag, Berlin Heidelbert, pp. 649-690 (2000)	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	17413675
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Joanne Ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	15-NOV-2013
Filing Date:	10-FEB-2012
Time Stamp:	15:22:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	1976
Deposit Account	061075
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Non Patent Literature	Mondal_Mobile_IP_Chapter_7.pdf	1246989 6281365b10dc49011994103debf91f42c3a2c22d	no	30
Warnings:					
Information:					
2	Non Patent Literature	Nacht_The_Spectrum_of_Modern_Firewalls.pdf	232773 1a396aac7344c7565c77a3c82cf026af5d3eadd6	no	3
Warnings:					
Information:					
3	Non Patent Literature	Shaw_Handbook_on_Electronic_Commerce_Ch31.pdf	1608953 547c5996cb506bb0fe4b40eb09f5af6468c8c60e	no	42
Warnings:					
Information:					
4	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	70560 e3c0d73318f1da65069f015d5629f0641a9b6415	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	128010 cdcdb498ae9a5c88aa9dc5683813154aae96bb0a	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Fee Worksheet (SB06)	fee-info.pdf	30572 1f61eec7ccea367833f2f0b2ef61dbe256f738ae	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3317857		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

RESPONSE TO FINAL ACTION UNDER 37 C.F.R. 1.116

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated September 17, 2013, Applicants respectfully request reconsideration and allowance in view of the following remarks.

Remarks/Arguments begin on page 2 of this paper.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. [ ] Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
      i. [ ] Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
      ii. [ ] Other _____

   b. [x] Enclosed
      i. [x] Amendment/Reply
      ii. [x] Affidavit(s)/Declaration(s)
      iii. [x] Information Disclosure Statement (IDS)
      iv. [ ] Other _____

2. Miscellaneous

   a. [ ] Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. [ ] Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. [x] The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any Overpayments, to Deposit Account No. 06-1075 .
      i. [x] RCE fee required under 37 CFR 1.17(e)
      ii. [x] Extension of time fee (37 CFR 1.136 and 1.17)
      iii. [ ] Other _____

   b. [ ] Check in the amount of $ _____ enclosed

   c. [ ] Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Christopher J. Han/	Date	February 13, 2014
Name (Print/Type)	Christopher J. Han	Registration No.	70,069

41244027_1

PTO/SB/22 (03-13)
Approved for use through 03/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-105
Application Number 13/371,363	Filed February 10, 2012
For SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	
Art Unit 2492	Examiner M. W. Chao

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☒ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600.00
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration number 70,069 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Christopher J. Han/ — Signature
February 13, 2014 — Date

Christopher J. Han — Typed or printed name
(617) 951-7000 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.

41083047_1

REMARKS

Independent claims 1, 10, and 19 are rejected under 35 U.S.C. § 103 as being allegedly obvious from Krawczyk, *Secret Sharing Made Short* ("SSMS") in view of Krawcyzk, *Distributed Fingerprints and Secure Information Dispersal* ("DFSID"), and Li, U.S. Patent Application Publication No. 2006/0080454 ("Li"), or in the alternative, Hand, *Spread Spectrum Storage with Mnemosyne* ("Hand"). In the alternative, independent claims 1, 10, and 19 are rejected under 35 U.S.C. § 103 as being allegedly obvious from Horne, *Escrow Services and Incentives in Peer-to-Peer Networks* ("Horne") and Li, or in the alternative, Hand. Applicants respectfully traverse the rejection.

Submission of Declaration

Applicants submit the enclosed Declaration of Dr. George T. Ligler under 37 C.F.R. § 1.132 (the "Ligler Decl."). Dr. Ligler is a Rhodes Scholar with degrees from Furman University and Oxford University, and he has over three decades of relevant technical experience. *See*, Ligler Decl., ¶¶ 1-5. Dr. Ligler describes in detail the operation of various embodiments of SSMS, DFSID, Horne, Li, Hand, and Rabin, *Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance* ("Rabin"), compares the references to the claimed approach, and sets forth his reasoned and incontrovertible conclusion that one of ordinary skill in the art would not be led to the claimed approach by the references, whether taken alone or in combination. *See*, Ligler Decl., ¶¶ 14-29.

Independent Claims 1, 10, and 19 Patently Distinguish over the Cited References

Independent claim 1 recites, *inter alia*, generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed. Independent claims 10 and 19 recite a non-transitory computer readable medium and a computer system, respectively, directed towards similar subject matter as independent claim 1. Support for this subject matter can be found throughout Applicant's specification, including, for example, at ¶¶ 122-125 and 290-298. In one non-limiting example,

¶ 291 describes a process that places units of data from a data set in 1 of 4 shares of data, where the placement of each unit is determined by a number in a substantially random sequence of numbers.

The cited references, either alone or in combination, fail to render obvious the claimed subject matter. The Examiner contends that a combination of SSMS and DFSID teaches the claimed data splitting information by partitioning a file F into n fragments using an information dispersal algorithm (IDA). *See* Office Action pp. 4. Applicants' respectfully disagree. SSMS and DFSID fail to teach data splitting information which is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed, as claimed.

SSMS and DFSID discuss using an IDA as taught by Rabin to "partition the encrypted file *E* into *n* fragments, $E_1, E_2, \ldots, E_n$." *See* SSMS pp. 5-6 and DFSID pp. 1-2. However, as discussed in the Ligler Decl., Rabin's IDA does not place units of data (e.g., bits, bytes, or any other logical block of data) from a data set into a plurality of shares. *See* Ligler Decl. 18-21. Instead, Rabin's IDA computes each share based upon the entire original file (*Ibid.*). There is no reason to generate data splitting information that is usable to determine into which of the shares a unit of data is placed because no unit of data from the file is placed in the shares. S*ee* Rabin, pg. 338. Indeed, the Examiner concedes this point: "the matrix multiplication and polynomial evaluation creates each share based upon every byte in the input file." *See* Office Action pg. 12. Thus, while the shares generated by Rabin's IDA may be *based on* the input file through a matrix multiplication, the generated shares do not contain any *units of data* from the input file. That is, Rabin's IDA computes shares based on the input file *in its entirety*, but does not actually *place* units of data from the input file into the shares. Therefore, Rabin, and by extension SSMS and DFSID, do not show data splitting information which is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed.

Li and Hand, either alone or in combination, also fail to teach data splitting information usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed. Li discusses a peer-to-peer media streaming method which uses erasure resilient coding so that media may be assembled from "fixed numbers of erasure coded blocks regardless of where and what specific blocks are retrieved." *See* Li, Abstract and ¶ 24. Li, however, also describes the use of matrix multiplication and a generator matrix in the development of coded

messages, as is done in Rabin. *See* Li, ¶ 107 and Ligler Decl. 26. Hand discusses encoding data using Rabin's IDA, which, as discussed above in relation to SSMS and DFSID, does not disclose or suggest the claimed data splitting information. Therefore, neither Li nor Hand remedy the deficiencies of DFSID and SSMS.

Horne also fails to teach data splitting information usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed. *See* Ligler Decl. 28. The Examiner concedes that Horne does not "disclose how data is distributed among the stores" and relies on Li and Hand to remedy this deficiency. *See* Office Action pg. 27. However, as discussed above, Li and Hand do not teach or suggest the claimed data splitting information.

Conclusion

For at least the forgoing reasons, Applicants respectfully submit that the cited references, either alone or in combination, fail to render obvious independent claims 1, 10, and 19 and all claims that depend thereon. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection under § 103 for claims 1-27

Applicants believe no fee is due with this response other than as reflected on the enclosed Fee Transmittal. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: February 13, 2014

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorney For Applicants

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	1252	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE - 2nd and Subsequent Request	1820	1	1700	1700
		Total in USD ($)		**2300**

PATENTS
Docket No: 104093-0002-105

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants : Orsini et al.

Application No. : 13/371,363 Confirmation No. : 7984

Filed : February 10, 2012

For : SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

Art Unit : 2492

Examiner : Michael W. Chow

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

DECLARATION UNDER 37 C.F.R. § 1.132 OF DR. GEORGE T. LIGLER

Madam:

I, Dr. George T. Ligler, hereby declare as follows:

1. I am self-employed as the sole proprietor of GTL Associates. I provide consulting services primarily related to systems engineering of computer systems, both hardware and software, and telecommunications. "Systems engineering" is the engineering that it takes to put together a computer system, starting from requirements through design, implementation and fielding. Since I began GTL Associates in

1988, I have worked with 41 clients in the United States, Europe and Asia, including assignments at both the national and international levels on real-time computer system standards including computer displays for aviation at the request of the Federal Aviation Administration. I have also served on a *pro bono* basis both on several panels formed by the National Research Council to advise the Government on issues related to computer system technology, design and implementation and, at the request of Secretary of Commerce Gutierrez, on a 2008 Expert Panel related to technology implementation for the 2010 Census.

2. I earned a Bachelor's degree in Mathematics (*summa cum laude*) from Furman University in 1971, and Master of Science (M.Sc.) and Doctorate (D.Phil.) degrees in Computer Science from Oxford University in 1973 and 1975, respectively. My studies at Oxford were supported by a Rhodes Scholarship. My doctoral dissertation was directed to the design of computer programming languages.

3. I have thirty-eight years of professional experience in the design and development of hardware and software for computer and telecommunications systems (as well as the design and development of those systems in their entirety) for a wide variety of applications. These computer

systems vary from embedded real-time microprocessor-based application-specific systems, such as encryption devices to secure both sensitive unclassified as well as classified information, to major national and international data communications networks. Applications have included the use of computer technology to support data communications, including secure data communications, over cable television networks, cellular networks, air/ground VHF communication networks, and conventional public switched telephone networks. I have also been responsible for the development and manufacture of color graphics display generators and color computer monitors.

4. I have authored or co-authored twenty technical publications in several fields, including articles relating to computer programming languages, computer software development methodologies, and computer/computer system architecture. Additionally, I have co-authored five reports issued by the National Research Council.

5. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and a member of the IEEE Computer Society, the Association for Computing Machinery (ACM), and the Institute of Navigation.

6. I have been retained by attorneys for assignee

of this application at my normal rate of $475.00 per hour.

7. A copy of my resume is attached to this Declaration as Exhibit A.

A. Topics Considered

8. It is my understanding that the current independent claims in the above-named patent application ("the Orsini application") stand rejected for obviousness based on Krawczyk, "Secret Sharing Made Short" ("SSMS") in view of Krawczyk, "Distributed Fingerprints and Secure Information Dispersal" ("DFSID"), and Li, U.S. Patent Application Publication Number 2006/0080454 ("Li") or in the alternative in view of Hand and Roscoe, "Spread Spectrum Storage with Mnemosyne", ("Hand")(September 17, 2013 Office Action at page 15). Alternatively, the current independent claims of the Orsini application stand rejected for obviousness based upon Horne et al., "Escrow Services and Incentives in Peer-to-Peer Networks" ("Horne") in view of Li, or in the alternative Hand.

9. I have been asked to review the references applied by the Examiner to determine whether they, alone or in combination, render the currently pending independent claims 1, 10, and 19 in the Orsini application obvious.

B. Materials Reviewed

10. In considering the above topics, I have particularly reviewed the following materials:

a) the Orsini application;

b) SSMS;

c) DFSID;

d) Li;

e) Hand;

f) Rabin, "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance", *Journal of the ACM*, Vol. 36, No.2, 1989, pp. 335-348 ("Rabin"), cited by both SSMS and DFSID;

g) Horne; and

h) Pertinent portions of the prosecution history of the Orsini application, including the Office Action dated September 17, 2013 and Applicant's Amendment in Response to Non-Final Office Action dated July 11, 2013, which contains the currently pending claims.

C. Level of Skill in the Art

11. A person of ordinary skill in the art of the Orsini application in 2004, that art in particular being systems for securing data from unauthorized access or use (Orsini application at Paragraph 0002), was a skilled

individual with three years of experience in the art and a bachelor's degree in computer science, computer engineering, or electrical engineering. Alternatively, the individual might have a graduate degree in one of these fields and one or two years of experience in the art. I base this definition of the level of skill in the art on my personal experience in the engineering of secure computer systems and data networks as well as discussions with a number of people in the field in the relevant time frame.

D. The Currently Pending Claims of the Orsini application

12. Each of the currently pending claims in the Orsini application recites,

> generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed (July 11, 2013 Amendment in Response to Non-Final Office Action, pages 3, 5, and 6).

I will call this recitation the "generating data splitting information usable for data placement feature" in the remainder of this Declaration.

13. For example, pending claim 1 is as follows

(emphasis added):

1. A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

E. Summary of Findings

14. Neither SSMS or DFSID discloses or suggests

the "generating data splitting information usable for data placement feature" of the currently pending independent claims of the Orsini application. More specifically, the currently pending claims expressly recite a particular type of "data splitting information" not present or suggested in SSMS or DFSID. Moreover, a person of ordinary skill in the art would not be motivated or led to modify SSMS, alone or in view of DFSID, to reach the "generating data splitting information usable for data placement feature" of the pending claims. Neither Li nor Hand remedy this deficiency of SSMS and DFSID.

15. Horne also does not disclose or suggest the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application. As is the case for SSMS and DFSID, neither Li nor Hand can remedy this deficiency.

F. Neither SSMS nor DFSID disclose or suggest the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application

16. As noted by the Examiner, both SSMS and DFSID are based upon using an Information Dispersal Algorithm (IDA) as introduced in Rabin (September 17, 2013 Office Action at, e.g., pages 9-12). The text from Rabin cited by the Examiner

on page 11 of the September 17, 2013 Office Action is as follows:

The characters b_i may be considered as integers taken from a certain range $[0 \cdots B]$. For example, if the b_i are eight-bit bytes, then $0 \le b_i \le 255$. Take a prime $B < p$. For bytes, $p = 257$ will suffice; but we may wish to choose a prime larger than the smallest $B < p$. Note that with $p = 257$ there is an excess of one bit per byte, we shall see later how to implement IDA in fields $GF(2^s)$, $s = 8$ for bytes, without any excess. Now, F is a string of residues mod p, that is, a string of elements in the finite field Z_p. All the following computations are in Z_p, that is, mod p.

Choose an appropriate integer m so that $n = m + k$ satisfies $n/m \le 1 + \epsilon$ for a specified $\epsilon > 0$. Choose n vectors $a_i = (a_{i1}, \ldots, a_{im}) \in Z_p^m$, $1 \le i \le n$, such that every subset of m different vectors are linearly independent. Alternatively, it will suffice to assume that with high probability, a randomly chosen subset of m vectors in $\{a_1, \ldots, a_n\}$ is linearly independent. We shall see later on how to satisfy each of these conditions.

The file F is segmented into sequences of length m. Thus

$$F = (b_1, \ldots, b_m), (b_{m+1}, \ldots, b_{2m}), \ldots.$$

Denote $S_i = (b_1, \ldots, b_m)$, etc. For $i = 1, \ldots, n$,

$$F_i = c_{i1}, c_{i2}, \ldots, c_{iN/m},$$

where

$$c_{ik} = a_i \cdot S_k = a_{i1} \cdot b_{k-1)m+1} + \cdots + a_{im} \cdot b_{km}. \qquad (1)$$

It follows that $|F_i| = |F|/m$.

If m pieces of F, say, $F_{i_1}, \ldots, F_{i_m}$ are given, we reconstruct F as follows. Let $A = (a_{ij})_{i=i_1,\ldots,i_m}$ be the $m \times m$ matrix whose jth row is a_{i_j}. It is readily seen that

$$A \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} c_{i_1} \\ \vdots \\ c_{i_m} \end{bmatrix},$$

and hence

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = A^{-1} \cdot \begin{bmatrix} c_{i_1} \\ \vdots \\ c_{i_m} \end{bmatrix}.$$

Denote the ith row of A^{-1} by $(\alpha_{i1}, \ldots, \alpha_{im})$, then in general, for $1 \le k \le N/m$,

$$b_j = \alpha_{i1} c_{ik} + \cdots + \alpha_{im} c_{mk}, \qquad 1 \le j \le N. \qquad (2)$$

---

17. In considering the relevance of SSMS and DFSID to the pending claims of the Orsini application, it is

essential to note two properties of Rabin's IDA.

18. First, in Rabin's IDA, each character in the file F that is to be dispersed is a factor within a term in the calculation of every one of the pieces F_i that are dispersed. This can be seen from examination of the equation for F_i in conjunction with equation (1) above. There are N/m elements in each F_i. Each of these elements is calculated using a different S_i, where each S_i contains a different subset of m elements of the N elements of the original file F, and all S_i are used in the calculation of each F_i.

19. Second, in Rabin's IDA, no character b_i from the file F itself actually appears in any of the pieces F_i that are to be dispersed. Again, this can be readily seen from the equation for F_i in conjunction with equation (1) above.

20. In view of these fundamental properties, Rabin's IDA does not disclose the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application. First, since each piece of data is used to calculate the value of every data share to be dispersed, the recited determination of "which of a plurality of shares of data a unit of data of the encrypted data set will be placed" (emphasis added) is

not met by Rabin—each "unit of data of the encrypted data set" is essential to the calculation of every one of the "plurality of shares".

21. Second, since no piece of the data actually appears in any of Rabin's shares, the recited determination of "which of a plurality of shares of data a unit of data of the encrypted data set will be placed" (emphasis added), is not met.

22. In short, Rabin's IDA is very different from the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application. Since neither SSMS nor DFSID suggests the wholescale departure from Rabin's technique that would be needed to have the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application (indeed, see SSMS at Section 3, second paragraph, and the Abstract of DFSID), the references taken alone or in combination neither disclose nor suggest the "generating data splitting information usable for data placement" feature of the currently pending claims.

23. I note that the September 17, 2013 Office Action discusses "splitting information" at length (see, e.g., pages 9, 12-14). I find that however the

interpretation of the term "splitting information" is resolved, the particular type of "splitting information" recited in the currently pending claims of the Orsini application is neither disclosed or suggested in SSMS and SFSID.

G. A person of ordinary skill would not be led by either SSMS or DFSID to make the extensive modifications required to SSMS and/or DFSID to reach the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application

24. As stated above, meeting the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application would require a fundamentally different type of IDA than that relied upon by SSMS and DFSID—i.e., an entirely different information dispersal algorithm. Particularly given the strong endorsement of Rabin's and related IDAs in SSMS and DFSID (see, e.g., SSMS's use of "remarkably" when describing Rabin's IDA in Section 3, page 140 and DFSID's described "building on" Rabin in its Abstract, page 207), a person of ordinary skill would not be motivated to make such a major modification to those references.

H. Neither Li nor Hand remedy the deficiencies of SSMS and DFSID

25. The September 17, 2013 Office Action cites Li and/or Hand as providing a particular share distribution scheme (page 19). Li and Hand do not, and the Examiner has not stated otherwise in the discussion of combining these references with SSMS and DFSID, disclose or suggest the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application.

26. Li is directed toward receiver-driven peer-to-peer media streaming for loosely coupled peer-to-peer networks (Li at, e.g., Paragraph 0002). Li describes, as stated by the Examiner, the use of "a high rate erasure resilient code to ensure that one or more of the peers will have the data blocks necessary to reconstruct particular data units while simplifying the demand on the client to identify which of the peers contains the necessary data" (Li at Paragraph 106; September 17, 2013 Office Action at page 19). In a manner related to that discussed for Rabin above, matrix multiplication involving original messages x_i and a generator matrix G in the development of coded messages c_i (Li at, e.g.,

paragraph 0107) indicates that Li neither teaches or suggests the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application.

27. Hand expressly uses Rabin's IDA and therefore cannot remedy the defects of SSMS and DFSID discussed above (Hand at page 2, subsection entitled "Dispersal" of Section 3).

I. Horne also does not disclose or suggest the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application

28. Horne is directed toward aspects of distribution of content, such as music, in peer-to-peer networks (Abstract). The Examiner does not appear to assert that Horne contains the "generating data splitting information usable for data placement" feature of the pending claims of the Orsini application (see, e.g., the September 13, 2013 Office Action at page 26, lines 1 to 3 and page 27, lines 13-16). Indeed, Horne, in Section 4.1 (cited by the Examiner on page 26 of the September 13, 2013 Office Action), describes a sender party S forming, from *k* blocks of content, *n* encoded content blocks and then sending all *n* of those encoded content blocks to a receiver party S as well as to an

escrow server ES--no notion of placing portions of the data content into respective shares is involved (Horne, Section 4.1).

29. The Examiner cites Li or, in the alternative, Hand to remedy this shortcoming of Horne. However, for the reasons discussed in Paragraphs 25-27 above, neither Li nor Hand disclose or suggest the "generating data splitting information usable for data placement" feature of the currently pending claims of the Orsini application. I therefore conclude that the combination of Horne in view of Li or, in the alternative, Hand does not reach this feature of the pending claims.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so make are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 and that such willful false statements may jeopardize the validity of the application and any patent issued thereon.

Date: 13 February 2014

/George T. Ligler/
George T. Ligler

EXHIBIT A

February 2014

Resume

George T. Ligler

GTL ASSOCIATES
4808 Cypress Ford Drive
Fuquay Varina, North Carolina 27526-9083
ligler1@earthlink.net
(919) 346-1807

Education

Oxford University, Oxford, England
M.Sc., Computer Science, 1973
D. Phil., Computer Science, 1975
(Rhodes Scholarship, Woodrow Wilson Fellow)

Furman University, Greenville, South Carolina
B.S., Mathematics, 1971
Summa Cum Laude

Experience

December 1988 - Present: GTL ASSOCIATES
Potomac, MD and Fuquay Varina, North Carolina
Proprietor

Established consulting firm in telecommunications, computer system and hardware/software engineering, and information management. Systems integration/engineering and product management services provided to forty-one clients in the United States, Europe and Asia. Assignments have included telecommunications network design, product and service definition and management, consulting on major program management and the systems integration process, applications systems engineering, business process improvement, competitive analysis, red teaming of major proposals, representation of clients in international fora, support of patent licensing discussions, participation in litigation as a consulting expert and/or expert witness, and new business venture planning.

Experience

August 2007 – November 2007: PROJECT MANAGEMENT ENTERPRISES, INC., Bethesda, Maryland

Senior Consultant

Subject matter expert on a part-time employee basis to support the Federal Aviation Administration's implementation of Automatic Dependent Surveillance—Broadcast (ADS-B) as a component of the Next Generation Air Transportation System.

December 1984 - December 1988: COMPUTER SCIENCE CORPORATION, Falls Church, Virginia

Vice President, Systems Group, November 1987 - December 1988

Assignments on major program acquisition efforts within Systems Group, CSC's $750M/year Government business. Areas of involvement included pre-award project team preparation, proposal review and assistance, subcontractor selection and management, competitive analysis, and business acquisition process review.

Vice President & Executive Director, Consolidated Data Network, Systems Division, October 1986 - November 1987

Program Office responsibility for a $282 million, 8-year effort to provide, operate, and maintain packet-switched data network for the U.S. Treasury Department, with AT&T and BBN as major subcontractors. Put in place a network design and implementation infrastructure that achieved peak cutover rates of over 20 network locations per working day, enabling customer to transition to new expanded enforcement data system without major delay. Reduced CSC cost per site cutover by over 20%. Established material planning methodology (MRPII) to improve inventory management. Laid the groundwork for resolution of several important contractual issues. Recruited and developed successor program manager.

Experience

Vice President, Communications and Controls Products, Systems Division, December 1984 - October 1986

Responsible for a $12M/year business area engaged in the supply of Energy Management and Control Systems (EMCS) and communications subsystems for urban rapid transit systems. Expanded EMCS business from Tri-Service applications to commercial arena and made that business profitable. Responsible for the development of selected communication security products as value-added options for CSC's systems integration thrust.

March 1982 - December 1984. AYDIN CORPORATION, Fort Washington, Pennsylvania

President, Aydin Controls Division, March 1982 -December 1984.

Vice President, Aydin Corporation, February 1983 - December 1984.

General management responsibility for a 375-person, fully-integrated Division with annual sales of $27M of computer graphics equipment. Product lines in color raster scan display generators, high resolution monitors, and turnkey CAD/CAM systems. Market areas included process control, utilities, defense, and petrochemical resource exploration. Division growth 1981-1984 of approximately 45%, outperforming most graphics terminal competitors. Significant operational improvements boosted margins for investment in sales, marketing, and product development.

April 1980 - March 1982. BURROUGHS CORPORATION, Paoli, Pennsylvania.

Deputy Manager, Great Valley Labs, April 1980 - January 1981.

Deputy General Manager and Director of Engineering, Special Systems Division, Federal and Special Systems Group, January 1981 to March 1982

Experience

Chief technical executive for Special Systems Division precursor. Later responsible for 400 research and engineering personnel engaged in the development of primarily command/control/ communications and secure systems. Research component of organization executing projects in diverse areas of computer science and engineering, including distributed processing, local area networks, software tools/engineering, VLSIC design, and machine intelligence. Remaining activities matrixed into Division programs for customers including NATO, NSA, Navy, Army, and FAA. Assist with general management of a $50M marketing, engineering, and manufacturing operation.

September 1976 - April 1980. TEXAS INSTRUMENTS, Dallas, Texas.

Project Manager, Research Manager.

Developed software products (e.g., compilers, programming tools) which became sources of TI revenue. Built an applied research and development activity of 15-20 persons with diverse program elements in computer systems and software engineering. Chaired a 25-member corporate-wide technical working group on advanced computer architectures; member of corporate computer science thrust team.

September 1975 - September 1976. UNIVERSITY OF TEXAS AT SAN ANTONIO, San Antonio, Texas.

Assistant Professor of Computer Science

Taught graduate/undergraduate courses in programming languages and analysis of algorithms. Research and publication in software engineering and programming language design. Chairman, Division Faculty Recruiting Committee.

Professional Activities and Awards

Author or co-author of twenty technical papers in the areas of software engineering, telecommunications, computer and computer systems architecture, navigation and information systems for aviation, and computer graphics. Co-author of five reports issued by the National Research Council.

Member, Association of American Rhodes Scholars, ACM, ION. Senior Member, IEEE.

Numerous invited lectures, panels, and program committee memberships.

Adjunct faculty member (two dissertation committees), Union Institute, 1989-1993.

Inducted into Furman University's Alumni Hall of Fame, 1979.

Member of National Research Council's Committee on Review of the Information Systems Modernization of the Internal Revenue Service, 1990-1995.

Member of Technical Review Committee for Georgia Institute of Technology's Futurenet, which formed the backbone for telecommunications within the 1996 Olympic Village, 1994-1996.

Member, Program Management Committee, RTCA (Aviation Standards Federal Advisory Committee), August 2000 to present. Co-Chair of RTCA's Special Committee on Satellite Navigation, June 2005 to present. Chair of RTCA's Integration and Coordination Committee, April 2009 to present. Chair of RTCA's Special Committee on Unmanned Aircraft Systems, May 2013 to present.

Chair, Co-Chair or Facilitator of RTCA Standards Working Groups that developed six aviation standards, 1992-2009. Rapporteur for development of International Civil Aviation Organization Standards and Recommended Practices for the Universal Access Transceiver (2002-2005).

Member of National Research Council's Panel on Research on Future Census Methods, December 2000 to March 2004.

Recipient of RTCA's 2006 Achievement Award.

Member (invited by Federal Aviation Administration), Automatic Dependent Surveillance-Broadcast (ADS-B) Aviation Rulemaking Committee, July 2007-July 2009.

Member (invited by Secretary of Commerce), Census Expert Panel, March 2008- September 2008.

Member of National Research Council's Panel to Review the 2010 Census, September 2009 to present.

Member (invited by the Federal Aviation Administration), Automatic Dependent Surveillance Broadcast (ADS-B) In Aviation Rulemaking Committee, June 30, 2010 to November 30, 2012.

Member (invited by RTCA), NextGen Advisory Committee Subcommittee, December 2010 to present.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement, pursuant to 37 C.F.R. § 1.114(c), accompanies the Request for Continued Examination (37 C.F.R. § 1.114) submitted herewith.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this

Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: February 13, 2014

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,473,860	10-29-2002	Chan	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	18197274
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Joanne Ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	13-FEB-2014
Filing Date:	10-FEB-2012
Time Stamp:	15:44:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2300
RAM confirmation Number	1458
Deposit Account	061075
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Extension of Time	104093-0002-105_Extension.pdf	88808 1cd7a8d40b05cf6db1cd7b0887cb95463635c8ca	no	1
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	104093-0002-105_RCE_Transmittal.pdf	95531 81d0e95bb57b5e0b900772869c36554a8e78a27c	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3	Miscellaneous Incoming Letter	104093-0002-105_Ligler_Declaration.pdf	327481 590a0f748f5bcd5dd7c35acb7cde00c8f32b11e0	no	22
Warnings:					
Information:					
4		104093-0002-105_Final_Response.pdf	103992 38e5e94f65344fa7779303802a26a4b44ee4eef8	yes	4

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Applicant Arguments/Remarks Made in an Amendment	2	4

Warnings:					
Information:					
5	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	69392 5ccb7befbdf777765dd471747dd582f0cbd25998	no	2
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	126140 ca7d13e17f9a757490fef031cdaa2b263b99837e	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Fee Worksheet (SB06)	fee-info.pdf	32362 9114a09bfdc277517d5b701af59a14ea8ee79fad	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	843706

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed before the mailing date of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114 (37 C.F.R. § 1.97(b)(4)).

41993544_1

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith a copy of a non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, Applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases that have not been previously submitted are submitted herewith. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, Applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	Publication No.	Attorney Docket No.	Filing Date	Status
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/371,364	US 2012-01159197	104093-0002-106	2/10/2012	Pending

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: April 7, 2014

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	18687120
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/joanne ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	07-APR-2014
Filing Date:	10-FEB-2012
Time Stamp:	16:17:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	104093-0002-105_IDS.pdf	78171 9f7acee815dd9ea4cb94a6e4ce3b080937fa f570	no	3

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	127105 acef9cf911cb245c61e99090274e3d4d3975813c	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	Copy_of_OAs_and_Replies_for_12148365.pdf	2816426 4687ad10fc686d8bb73be64c5a96e2478c3d1232	no	55
Warnings:					
Information:					
4	Non Patent Literature	Copy_of_Reply_Brief_for_13024791.pdf	383744 d4daff41a7df8c8b4f11f6c8beaf5d8395be70b9	no	9
Warnings:					
Information:					
5	Non Patent Literature	Copy_of_Reply_for_13024804.pdf	984443 47c49c6a0d535c161135cbef2a0ac51f05a4f06b	no	25
Warnings:					
Information:					
6	Non Patent Literature	Copy_of_Reply_for_13371364.pdf	1428898 4d77775fb5643bbf08ae3817509fad96827ca9c2	no	34
Warnings:					
Information:					
7	Non Patent Literature	Rosen_BGP-MPLS_VPNs.pdf	1074834 3223f8eb61ff7fe7b94c56f834846dbdb7e930b2	no	25
Warnings:					
Information:					
		Total Files Size (in bytes):	6893621		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,058,188	05-02-2000	Chandersekaran et al.	
		US-6,182,214	01-30-2001	Hardjono	
		US-7,035,405	04-25-2006	Schwenk	
		US-2002/0178355	11-28-2002	D'Sa et al.	
		US-2006/0075222	04-06-2006	Moloney et al.	
		US-2007/0064704	03-22-2007	Balay et al.	
		US-2008/0037557	02-14-2008	Fujita et al.	
		US-2011/0085667	04-14-2011	BERRIOS et al.	
		US-2011/0135094	06-09-2011	Muto et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rosen, "BGP/MPLS VPNs," Network Working Group, RFC 2547, March 1999, 25 pages	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 67/108	4/25/2014	mc
G06F 11/1092	4/25/2014	mc

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/17/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	4/25/2014	mc
google searched "array coding" and "erasure OR error coding raid"	4/25/2014	mc

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-8,347,084	01-01-2013	Tavernier et al.	
/M.C./		US-8,208,897	06-26-2012	Kaneko et al.	
/M.C./		US-8,189,769	05-29-2012	Ramasamy et al.	
/M.C./		US-7,934,100	04-26-2011	Fujimaki	
/M.C./		US-7,657,760	02-02-2010	Teramoto et al.	
/M.C./		US-7,234,063	06-19-2007	Baugher et al.	
/M.C./		US-7,171,685	01-30-2007	Batra et al.	
/M.C./		US-6,701,303	03-02-2004	Dunn et al.	
/M.C./		US-2008/0270603	10-30-2008	Berger et al.	
/M.C./		US-2007/0033644	02-08-2007	Thomas et al.	
/M.C./		US-2004/0268148	12-30-2004	Karjala et al.	
/M.C./		US-2002/0075844	06-20-2002	Hagen	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	04/25/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

39383392_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.C./		Mondal, "Mobile IP," Chapter 7, Fluwer Academic/Plenum Publishers, New York, pp. 173-202 (2003)	
/M.C./		Nacht, "The Spectrum of Modern Firewalls," Computers & Security, 16 (1997), pp. 54-56.	
/M.C./		Shaw et al (eds.), "Handbook on Electronic Commerce, Conway, Chapter 31, Springer-Verlag, Berlin Heidelbert, pp. 649-690 (2000)	

Examiner Signature	/Michael Chao/	Date Considered	04/25/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

39383392_1

Examiner-Initiated Interview Summary	Application No. 13/371,363	Applicant(s) ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*. (3)_____.

(2) *Christopher J. Han (Reg. No. 70,069)*. (4)_____.

Date of Interview: *22 April 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☒102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Plank, Xu, see OA mailed herewith*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and Examiner discussed Examiner suggested amendments to the claims with respect to the "data splitting information" limitation. No agreement was reached.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 05/01/2014

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
05/01/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No. 13/371,363	Applicant(s) ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7/11/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-27* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *4/07/2014; 2/13/2014; 11/15/2013*.

3) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *herewith* .

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This action is in response to argument filed 7/11/2013. Application 13/371,363 claims priority to 10/25/2004. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 7/11/2013 was filed after the mailing date of the Non-Final OA on 4/11/2013. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

The documents submitted on 9/20/2012 and 4/07/2014, which appear to be transmittal letters, with the subheading of "Notice of Related Patent Applications" fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because it does not provide (b) a column that provides a space next to each document listed to permit the examiner's initials. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing

the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

The portions of these transmissions in the form titled "Information Disclosure Statement by Applicant" have been considered. To clarify, while the IDS documents themselves have been considered, the documents submitted simultaneously with the IDS that lists “related applications” have not been “considered” Although the Examiner is aware of the co-pending and allowed cases, he cannot “consider” an entire prosecution history. Whether or not Applicant intended these “related applications” to function as an IDS per se the Examiner must still note for the record that they are not “considered” since there is no singular document for consideration.

Response to Arguments

Applicant's arguments filed 2/13/2014 have been fully considered but they are not persuasive.

Although much has been said in the prosecution history regarding the claimed “splitting information”, OA dated 9/19/2013, Applicant’s remarks on 7/11/2013, as well as the presently presented 132 affidavit (on 2/13/2014) and remarks 2/13/2014; it appears that the only outstanding issue is the appropriate interpretation of the claim language:

“**generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed**”

In order to address the above, it must first be determined what a "share of data" is; the only definition of which is found in the last clause of the claim:

"wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares."

In the art, this is termed "erasure coding" which is defined in Xu (Highly Available Distributed Storage Systems) as

("Erasure-correcting codes are a mathematical means of representing data so that lost information can be recovered. With an (n,k) erasure-correcting code, **we represent k symbols of the *original* data with n symbols of *encoded* data (n – k is called the amount of *redundancy* or *parity*).**" Xu § 2.1)

"erasure coding" is defined in Krawczyk as"

("Information Dispersal was introduced by Rabin [15]. It is a scheme intended for the distribution of a piece of information among n active processors, in such a way that the recovery of the information is possible in the presence of m active processors (i.e. out of m fragments), where m and n are parameters satisfying 1 <= m <= n. The scheme assumes that active processors behave honestly, i.e. returned fragments are unmodified. The basic idea is to add to the information, say a file F, some amount of redundancy and then to partition it into n fragments, each transmitted to one of the parties. **Reconstruction of F is possible out of m (legitimate) fragments.** Remarkably, each distributed fragment is of length which is clearly space optimal. Information dispersal schemes can be implemented in a variety of ways, all corresponding to the notion of erasure codes in the theory of error correcting codes (see [15, 13, 91)." Krawczyk, SSMS, § 3)

Note the **bolded** fragments which similarly disclose the property of erasure coding, that the original data can be reconstructed with a subset of the distributed data. It can further be seen that both disclosures similarly state that "erasure coding" breaks an input data into a plurality of parts.

Applicant's claimed "splitting information" is stated to be used to determine which part comprises a piece of data. It is not stated how this information is used, nor how it is generated, only that it is used to separate the data, in some way. The Examiner

believes it should be self-evident at this point that both Krawczyk (SSMS) and Xu must similarly disclose some "information" that is used to determine how to separate the data since they are both commonly directed to the separation of data. The references also explicitly state how they generate information used in splitting the input data.

> **Xu**: ("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimentional array of size l x n. In a distributed storage system, the bits in the same column are stored in the same disk. If any bit in a disk is corrupted, then the disk is considered to be a failure disk and needs repair, i.e., the corresponding column of the code is considered to be an erasure." Xu § 2.1. See also Xu §§ 3-5 for further methods)
>
> **Krawczyk**: ("2. Using IDA partition the encryption file E into n fragments, E_1, E_2, . . . , E_n." SSMS p. 6).
>
> **Krawczyk**: ("For completeness, we outline the following simple information dispersal scheme based on Reed Solomon erasure codes. The information to be shared is partitioned into m equal parts where each part is viewed as an element over a finite field (e.g. GF(p)), for a large enough prime p). These m elements are then viewed as coefficients of a polynomial of degree m - 1, and the n fragments for distribution are obtained by evaluating this polynomial in n different points. Clearly the whole information can be reconstructed (by interpolation) from any m fragments. We stress that for large files, it is not necessary to work on a huge field but just to view the information as the concatenation of different polynomials. Notice the difference between such a scheme and Shamir's secret sharing in which the information is represented by the free coefficient and not by the whole polynomial (this is essential in Shamir's scheme to provide perfect secrecy but not for information dispersal where secrecy is not a concern)." SSMS § 3).

Note that each of the underlined portion comprises "information", information which is used to separate the data into n fragments or shares; information that is usable to determine into which share data should be placed; information that might be termed "splitting information".

Applicant argues (Rem. p. 3 on 2/13/2014), that the cited SSMS and DFSID "does not place units of data (e.g., bits, bytes, or any other logical block of data) from the data set into a plurality of shares". This interpretation is contrary to proper claim interpretation; a proper interpretation of a claim comprising the transitional phrase "comprising" does not exclude additional unrecited acts, such as transforming the data

by encryption, compression, or evaluation of polynomial coefficients (SSMS). Both SSMS and Xu, and any method of erasure coding commonly use "codes [that] are a mathematical means of representing data so that lost information can be recovered." As to how Applicant's erasure code may differ from the species of SSMS and Xu, such is unclaimed.

Note that Applicant's specification specifically provides that the shares: "although FIG. 33 is illustrated in terms of byte by byte operations, the operation may take place at the bit level or at any other suitable level." (¶ 436 as published 2012/0166815). Thus the splitting information might appropriately be interpreted as a method of determining where the shares are placed, since a share might reasonably be interpreted as a "suitable level".

Applicant's, George T. Ligler, affidavit filed 2/13/2014; the affidavit generally asserts that none of the cited references disclose "generating data splitting information". This assertion, extrinsic evidence, affidavit, is not persuasive.

Regardless of how Applicant, Applicant's representative, or the Affiant characterize the prior art references the critical issue is does the prior art disclose a broadest reasonable interpretation of "generating data splitting information".

As seen above, Applicant appears to be claiming a type of erasure coding system; where SSMS and Xu disclose species of erasure coding. The claim does not state or imply how the "data splitting" information is generated nor applied. More

particularly Applicant has never argued, asserted, implied, or otherwise provided any evidence on the record that his erasure coding scheme is different than the prior art.

To reiterate, Applicant has never responded to Examiners comments that definition of "splitting information" information is necessary (OA p. 4 ll. 4-10; Interview on 7/11/2013 and more recently on the interview summary mailed herewith.) Applicant has never responded to the rejection by pointing to any portion of his own specification that might illustrate the "splitting information" nor pointed out how Applicant's "splitting information" differs from the prior art. The closest the arguments have come to defining the "splitting information" is in the presently presented arguments which state: "does not place units of data (e.g., bits, bytes, or any other logical block of data) from the data set into a plurality of shares". This neither states how the "splitting information" is generated nor how it works and is also unclaimed. Again, note that even if the above were claimed, a share might just be the entire "logical block of data" and inherently disclosed by any erasure coding scheme.

In summary, the Examiner believes a lack of illustration as to the distinction of the argued "splitting information" is a strong implication that the below stated rejection is appropriate and correct. If Applicant's intended claim scope in fact differs from the method disclosed in the Krawczyk references (SSMS, DSFID) then Applicant has no reason to be shy about particularly pointing out and distinctly claiming such difference.

Note that although Li and Hand were previously cited as disclosing the generation of data splitting information for an alternate interpretation thereof; it has become evident that that interpretation was overly narrow and the "data splitting" information is just that, information on how the data is split. This is inherent to all erasure coding schemes and the rejection has been edited to reflect this scope.

Examiner's suggested amendment to the independent claims to overcome the references:

"segmenting the encrypted data set into a plurality of blocks which are represented by a plurality of shares, wherein the particular bits from a given block are selected for a share based on data splitting information,

wherein the data splitting information specifies different amounts of bits from the respective block for a plurality of the shares; or (e.g. ¶ 441 as published)

wherein the data splitting information specifies a plurality of non-contiguous bits of at least one byte of the original encrypted data set for at least one share;" (e.g. Fig. 35)

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory

obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 10, and 19 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 7, 16, and 26 of US application 13/371,364. Although the conflicting claims are not identical, they are not patentably distinct from each other because (claims 16 and 26) they substitute hash information for

integrity information, which is stated to include in its scope hash information in ¶ 400. As to claim 1, of the present application, the claim is identical except for the "by processing circuitry"; which while not significant enough to avoid being anticipated by claim 7 of '364 presumably includes some difference in scope.

In summary, claims 1, 10, and 19 are anticipated by copending claims of '364, 7, 16, and 26.

Claims 1-27 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-6, 8-15, 17-25, and 27-30 of US application 13/371,364. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims sole distinguishing factor is that the claims of '364 lack the "hash information". As seen in the art combination below, for erasure coding systems, it was known to append hash information, see DFSID as cited below.

A person of ordinary skill in the art at the time of invention would have modified the claims of '364 by including the fingerprint of DFSID. It would have been obvious to one of ordinary skill in the art at the time of invention to modify '364 which are similar with SSMS with DFSID since it was suggested explicitly by DFSID (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]") and to solve the information integrity problem (DFSID Abstract).

Integrity information includes in its scope hash information as disclosed by Applicant in ¶¶ 394, 395.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-12, 14-21, and 23-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID.

With respect to claims 1, 10, 19, SSMS teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

Encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set; ("1. Choose a random encryption key K. Encrypt the secret S using the encryption function ENC under the key K, let E = $ENC_K(S)$" SSMS p. 6).

[creating hash information based on a hash operation using the data set;]

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; (SSMS discloses information used to split the data into shares)

("We assume a generic information dispersal algorithm that we denote by IDA, and which works for parameters n (number of file fragments) and m (number of required fragments to reconstruct the file)." SSMS p. 6)

("we outline the following simple information dispersal scheme based on Reed Solomon erasure codes. The information to be shared is partitioned into m equal parts where each part is viewed as an element over a finite field (e.g. GF@), for a large enough prime p) . These m elements are then viewed as coefficients of a polynomial of degree m - 1, and the n fragments for distribution are obtained by evaluating this polynomial in n different points." SSMS pp. 5-6. This details how the information used to determine into which of a plurality of shares data will be placed.)

separating the encrypted data set into the plurality of shares based on the data splitting information; ("2. Using IDA partition the encryption file E into n fragments, $E_1, E_2, \ldots, E_n$." SSMS p. 6)("3. Using PSS generate n shares for the key K" SSMS p. 6)

including in the plurality of shares (a) data indicative of the encryption key and [(b) the hash information]; and ("4. Send to each participant P_i, I = 1, 2, . . . , n the share $S_i = (E_i, K_i)$. The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 7)

causing the plurality of shares to be stored in respective separate storage locations; (to each participant. SSMS p. 7. "The distribution process gets ~ 1 sin put the secret S (and the values of n and m) and generates n shares Sl, Sz, . . , , Sn, which are privately delivered to the system participants." SSMS p. 3) (where the system is a set of distributed servers "These constructions have many applications, especially in distributed scenarios where secrecy and integrity of information are to be protected. For example, consider a group of five servers sharing a data base of confidential information such that no pair of servers is allowed to learn about the information without the collaboration of a third one. (That is, the system tolerates up to two corrupted servers without compromising the information)." SSMS p. 2)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. (“The reconstruction process reconstructs the correct secret when input with any subset of m shares.” SSMS p. 3)

SSMS does not disclose:

creating hash information based on a hash operation using the data set;

(b) the hash information;

DFSID discloses an analogous algorithm purposed for use with SSMS (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]").

DFSID further creating hash information based on a hash operation using the data set;

(b) the hash information:

"1. Use IDA to distribute the file among the n processors. Denote by F_i the piece distributed to processor p_i.

2. Fingerprint each piece F_i, i = 1, . . , n, by the DFP method (as described in Section 3). That is, for each i, compute $H(F_i)$ and then distribute this value among all processors using the coding function C. (Each processor p_j gets a share s_{ij} corresponding to $H(F_i)$)." (DFSID § 4.1, see also § 4.1 generally)

A fingerprint is a hash, see DFSID § 3.

A person of ordinary skill in the art at the time of invention would have modified SSMS by including the fingerprint of DFSID. It would have been obvious to one of ordinary skill in the art at the time of invention to modify SSMS with DFSID since it was

suggested explicitly by DFSID (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]") and to solve the information integrity problem (DFSID Abstract).

With respect to claims 2, 11, 20, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. (determinism is a necessary feature of any system that will retrieve obfuscated data)

With respect to claims 3, 12, 21, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. (“An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S” SSMS § 2)

With respect to claims 5, 14, 23, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set. (“An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S” SSMS § 2)

With respect to claims 6, 15, 24, SSMS in view of DFSID discloses: wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm. ("In order to achieve a space efficient secret sharing scheme we combine an information dispersal scheme with a secure encryption scheme and a perfect (e.g. Shamir's) secret sharing scheme." SSMS § 3)

With respect to claims 7, 16, 25, SSMS in view of DFSID discloses: wherein the step of including data indicative of the encryption key comprises:
encrypting the encryption key with a second key; and
including in the plurality of shares data indicative of the encrypted encryption key. ("The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 6. See also p. 7. Encryption requires a key of some kind.)

With respect to claims 8, 17, 26, SSMS in view of DFSID discloses: further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("Send to each participant . . . portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS § 3. A second encryption, a second key, to transmit the share, and therefore not contained within the share.)

With respect to claims 9, 18, 27, SSMS in view of DFSID discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Send to each participant . . ." SSMS § 3.)

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over SSMS in view of DFSID in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, SSMS in view of DFSID does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a

form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified SSMS in view of DFSID with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 1-3, 5-12, 14-21, and 23-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID, in view of Xu et al. (Highly Available Distributed Storage Systems).

As seen above the Krawczyk references disclose the recited limitations; there are however other art that would form an obvious combination therewith to change the nature of the claim elements:

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

In other words, there are other obvious methods of generating splitting information to determine how to separate data into a plurality of shares that are:

Restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("Erasure-correcting codes are a mathematical means of representing data so that lost information can be recovered. With an (n,k) erasure-correcting code, we represent k symbols of the *original* data with n symbols of *encoded* data (n – k is called the amount of *redundancy* or *parity*)." Xu § 2.1)

Xu further teaches that: ("The complexity of the computations needed to construct the encoded data (a process called *encoding*) and to recover the original data

(a process called *decoding*) is an important consideration for practical systems. Array codes are ideal in this respect. Array codes have been studied extensively." Xu § 2.1)

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; ("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimentional array of size l x n. In a distributed storage system, the bits in the same column are stored in the same disk. If any bit in a disk is corrupted, then the disk is considered to be a failure disk and needs repair, i.e., the corresponding column of the code is considered to be an erasure." Xu § 2.1)

separating the encrypted data set into the plurality of shares based on the data splitting information;

("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimentional array of size l x n. In a distributed storage system, the bits in the same column are stored in the same disk. If any bit in a disk is corrupted, then the disk is considered to be a failure disk and needs repair, i.e., the corresponding column of the code is considered to be an erasure." Xu § 2.1)

See also Xu § 2.4.1 ("In X-Code, information bits are placed in array of size (n-2) x n. Like other array codes [2][3][5][11], parity bits are constructed by adding the information bits along several parity check *lines* or *diagonals* of given slopes." Alternative methods of splitting the data)

See also Xu § 2.5 B-codes for an additional method of splitting data.

A person of ordinary skill in the art at the time of invention would have modified the Information Dispersal Algorithm of Krawczyk with Xu by utilizing any of the array coding methods disclosed in Xu as a substitute erasure coding method for that disclosed in SSMS. It would have been obvious to one of ordinary skill in the art at the time of invention to use an alternate erasure coding method in order to obtain efficient encoding and decoding, for which array codes are ideal Xu § 2.1.

Additionally, the Krawczyk reference at § 3 states that the "Information dispersal schemes can be implemented in a variety of ways, all corresponding to the notion of erasure codes in the theory of error correcting codes". The Xu reference discloses in § 3 that "We will show here a more systematic way of using proper redundancy, based on error-correcting codes (particularly the MDS array codes described above)". Thus, Both the Information Dispersal Algorithm (IDA) of Krawczyk and the array codes of Xu are species of "error-correcting codes".

The modification of Krawczyk's discussed IDS scheme with that of Xu is either a (1) simple substitution of one known element for another to obtain predictable results the (2) use of a known technique to improve [a] similar method in the same way.

As to the particular findings required mandated by MPEP 2143(I)(B-C); the fact that the Krawczyk and Xu references are species of the same genus and that Krawczyk discloses that the "information dispersal scheme can be implemented in a variety of ways [corresponding to the genus of error-correcting codes]" supports a finding of all the factors.

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over SSMS in view of DFSID, in view of Xu et al. (Highly Available Distributed Storage Systems), in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, SSMS in view of DFSID, in view of Xu does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects

become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified SSMS in view of DFSID in view of Xu with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Plank, James (A tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems) discloses a mechanism for separating varying lengths of data.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Chao/
Primary Examiner, Art Unit 2492

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-6,058,188	05-02-2000	Chandersekaran et al.	
/M.C./		US-6,182,214	01-30-2001	Hardjono	
/M.C./		US-7,035,405	04-25-2006	Schwenk	
/M.C./		US-2002/0178355	11-28-2002	D'Sa et al.	
/M.C./		US-2006/0075222	04-06-2006	Moloney et al.	
/M.C./		US-2007/0064704	03-22-2007	Balay et al.	
/M.C./		US-2008/0037557	02-14-2008	Fujita et al.	
/M.C./		US-2011/0085667	04-14-2011	BERRIOS et al.	
/M.C./		US-2011/0135094	06-09-2011	Muto et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	04/25/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

41993633_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.C./		Rosen, "BGP/MPLS VPNs," Network Working Group, RFC 2547, March 1999, 25 pages	

Examiner Signature	/Michael Chao/	Date Considered	04/28/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

41993633_1

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S69	1	(security adj first).asn. and @pd>"20130411"	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2013/07/17 09:43
S68	1	(orsini and rick or hare and mark or davenport and rojer or winick and steven).in. and @pd>"20130411"	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2013/07/17 09:43
S67	0	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 encrypted key (hash OR fingerprint OR checksum) and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:43
S66	0	(fountain OR erasure OR tornado OR raptor OR rateless) adj (coding or codes) encrypted key (hash OR fingerprint OR checksum) and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:43
S71	9	713/153.ccls. and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:46
S70	27	726/27.ccls. and @pd>"20130411" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2013/07/17 09:46
S73	73	orsini adj2 rick	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/03/27 12:22
S74	136	(orsini and rick or hare and mark or davenport and rojer or winick and steven).in.	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2014/03/27 12:46
S78	1	orsini adj2 rick and header.clm.	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/03/27 13:38
S87	153	data adj splitting and shares	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/27 17:24

S86	1072	data adj splitting	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/27 17:24
S88	575	erasure adj code	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/27 17:33
S89	71	g06f2221/0784.cpc.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/27 17:37
S90	2128	torrent	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:43
S91	450	bit adj torrent	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:44
S93	175	h04L67/108.cpc. and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:46
S92	468	h04L67/108.cpc.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:46
S94	112	h04L67/108.cpc. and (@ad<"20041025" or @rlad<"20041025") and (bit or byte)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:47
S95	101	h04L67/108.cpc. and (@ad<"20041025" or @rlad<"20041025") and (bit$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:48
S96	151	file adj segmentation	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:52
S99	3120	reed adj solomon adj coding	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 15:16
S100	52	reed adj solomon adj coding and distributed adj storage	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 15:17
S102	103	g06f11/1092.cpc. and distributed adj storage	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 15:18
S101	512	g06f11/1092.cpc.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 15:18
S105	13	distributed near storage near10 (bits or bytes) and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT;	AND	OFF	2014/03/31 12:06

			EPO; IBM_TDB			
S104	10	(distributed adj storage) file (segmentation OR splitting OR separation) same bits and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/03/31 12:06
S103	70	(distributed adj storage) file (segmentation OR splitting OR separation) same bits	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/03/31 12:06

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S106	0	713/153.ccls. and (splitting adj information).clm.	USPAT; UPAD	AND	OFF	2014/03/31 12:03
S107	42	(splitting adj information).clm.	USPAT; UPAD	AND	OFF	2014/03/31 12:04

4/25/2014 6:03:22 PM
C:\Users\mchao\Documents\EAST\Workspaces\13371363.wsp

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-6,473,860	10-29-2002	Chan	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	04/25/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature	/Michael Chao/	Date Considered	04/28/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

40745623_1

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Xu et al.; Highly Available Distributed Storage Systems; 1999; Retrieved from the Internet <URL: link.springer.com/chapter/10.1007%2FBFb0110096?LI=true>; pp 1-24 as printed.
	V	Plank, James; A Tutorial on Reed-solomon Coding for Fault-Tolerance in RAID-like systems; 1997; Retrieved from the Internet <URL: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.160.4742&rep=rep1&type=pdf>; pp. 1-18 as printed.
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 09/25/2014

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
09/25/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*.

(2) *Regina Sam (Reg. No. 67,362)*.

(3) *George Ligler*.

(4) _____.

Date of Interview: *22 September 2014*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☐ applicant ☒ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Krawczyk*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and the Examiner discussed the context of the claimed 'splitting information'. Examiner agreed that a proposed amendment: "wherein each share is based on one or more, but not all, of the units of data of the encrypted data set" would overcome the Krawczyk references. No other agreement was reached.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Michael Chao/ Primary Examiner, Art Unit 2492	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	1252	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**780**

REMARKS

Claims 1-27 are pending. Claims 1-3, 5-12, 14-21, and 23-27 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Krawczyk, *Secret Sharing Made Short* ("SSMS"), Krawczyk *Distributed Fingerprints and Secure Information Dispersal* ("DFSID"). In the alternative, claims 1-3, 5-12, 14-21, and 23-27 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of SSMS, DFSID, and Xu et al. *Highly Available Distributed Storage Systems* ("Xu"). Claims 4, 13, and 22 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of SSMS, DFSID, and Kubiatowicz, *OceanStore* ("Kubiatowicz"). In the alternative, claims 4, 13, and 22 stand rejected under 35 U.S.C. § 103 as being allegedly unpatentable in view of SSMS, DFSID, Xu, and Kubiatowicz. Claims 1-27 stand rejected under nonstatutory obviousness-type double patenting over claims 1-6, 8-15, 17-25, and 27-30 of U.S. Patent Application No. 13/371,364.

In order to expedite prosecution, and without concurring in the rejections, Applicants have amended independent claims 1, 10, and 19 to clarify the claimed subject matter. The amendments do not add new matter and are fully supported by the original application. Furthermore, these amendments are submitted without prejudice to the pending claims, and should not be construed as an admission by Applicants that the cited references render the pending claims obvious. The rejections are respectfully traversed.

Summary of Examiner Interview

On September 22, 2014, Applicants' representatives (Regina Sam (Reg. No. 67,362), and technical expert Dr. George Ligler) conducted an in-person interview with the Examiner. The undersigned wishes to thank Examiner Chao for the courtesies extended during the interview. During the interview, the Examiner and Applicants' representatives discussed the rejections under § 103 and the declaration under 37 CFR 1.132 previously submitted by Applicants' technical expert Dr. Ligler. Applicants and the Examiner also discussed a clarifying amendment along the lines presented herein. The Examiner agreed that the discussions and the amendments made herein render moot the rejections under § 103. Accordingly, Applicants respectfully request

reconsideration and withdrawal of the rejections under § 103 for independent claims 1, 10, and 19 and all claims that depend thereon.

Applicants' Reply to the Provisional Double Patenting Rejections

Claims 1-27 were provisionally rejected on the ground of obviousness-type non-statutory double patenting over claims 1-6, 8-15, 17-25, and 27-30 of U.S. Patent Application No. 13/371,364 ("the '364 application"). Applicants respectfully requests that the Examiner hold the provisional double patenting rejection in abeyance until allowable subject matter is identified in the instant application. Upon identification of allowable subject matter, Applicants will consider whether the allowed claims are patentably distinct from the claims in the '364 application and, if appropriate, file a Terminal Disclaimer.

Conclusion

For at least the reasons set forth above, Applicants respectfully submit that claims 1-27 are allowable and that this application is in condition for allowance. Reconsideration and prompt allowance of this application are respectfully requested.

Applicants believe no fee is due with this response other than as indicated on the Fee Transmittal submitted concurrently herewith. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: September 29, 2014

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

PTO/SB/22 (03-13)
Approved for use through 03/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-105
Application Number 13/371,363	Filed February 10, 2012
For SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	
Art Unit 2492	Examiner M. W. Chao

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☒ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600.00
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card. ~~Form PTO-2038 is attached.~~

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration number 70,069 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Christopher J. Han/	September 29, 2014
Signature	Date
Christopher J. Han	(617) 951-7000
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.

45953012_1

Abstract of Cited Ref 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2007-334836
(43)Date of publication of application : 27.12.2007

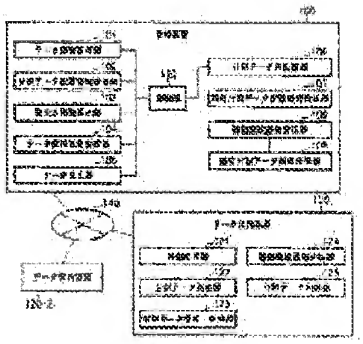
(51)Int.Cl. *G06F 3/06 (2006.01)*
G06F 12/00 (2006.01)

(21)Application number : 2006-169385
(22)Date of filing : 19.06.2006

(71)Applicant : CANON INC
(72)Inventor : INOSE ATSUSHI

(54) INFORMATION PROCESSOR, DATA HOLDING DEVICE AND CONTROL METHOD THEREFOR, COMPUTER PROGRAM, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To secure high data maintainability without applying a load onto a network and a storage device, in the plurality of storage devices and controllers connected to the network serving as objects.
SOLUTION: This information processor communicated with the plurality of data holding devices via the network confirms the presence of operations for the data holding devices for holding one of the second data obtained by redundancy-dividing the first data, compares the number of the operation confirmed data holding devices with the number of the second data required for restoring the first data, and requests the transmission of the second data to the device when the device number is less than a threshold value and the data number or more. The first data are restored from the second data obtained in response to the request, and the first data is thereafter redundancy-divided to be transmitted to the data holding device in a redistributed side.



AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application.

Listing of Claims

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. (Original) The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. (Original) The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. (Previously Presented) The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

7. (Original) The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. (Original) The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. (Original) The method of claim 1, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

10. (Currently Amended) A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. (Original) The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. (Previously Presented) The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

16. (Original) The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. (Original) The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. (Original) The non-transitory computer readable medium of claim 10, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

19. (Currently Amended) A computer system for securing a data set, the system comprising:

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. (Original) The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. (Original) The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. (Previously Presented) The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir secret sharing algorithm.

25. (Original) The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. (Original) The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. (Original) The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/371,363	Filing Date 02/10/2012	☒ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	09/29/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 27	Minus	** 20	= 7	X $80 =	560
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**560**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/MONICA FRANCIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Espacenet

Bibliographic data: JP2008103936 (A) — 2008-05-01

SECRET INFORMATION MANAGEMENT DEVICE, AND SECRET INFORMATION MANAGEMENT SYSTEM

Inventor(s): TATEOKA MASAMICHI; TANAKA TOMOYA ± (TATEOKA MASAMICHI, ; TANAKA TOMOYA)

Applicant(s): TOSHIBA CORP; TOSHIBA SOLUTIONS CORP ± (TOSHIBA CORP, ; TOSHIBA SOLUTIONS CORP)

Classification: **- international:** ***H04L9/08***
- cooperative: **H04L9/085**

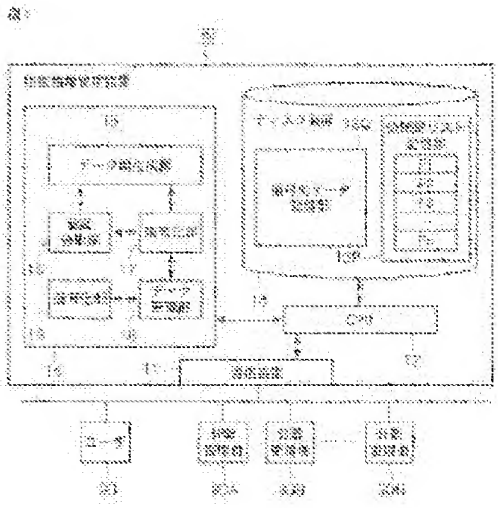
Application number: JP20060284087 20061018

Priority number (s): JP20060284087 20061018

Also published as: US2008095375 (A1) US7873168 (B2) CN101166089 (A) CN101166089 (B)

Abstract of JP2008103936 (A)

PROBLEM TO BE SOLVED: To provide a secret information management device and a secret information management system, capable of decrypting encrypted data even when a user loses an encryption key. ; SOLUTION: In the secret information management system, a secret information management device 10 comprises: a secret dispersion part 16 for secretly dispersing data keys K based on a (k, n) type secret dispersion system upon encrypting data D input from a user terminal 20 to generate n dispersion keys B1, B2, ..., Bn; an encryption part 17 for generating n encrypted dispersion keys E<SB>P1</SB>(B1), E<SB>P2</SB>(B2)... E<SB>Pn</SB>(Bn) based on n



dispersion manager public keys P1, P2...
Pn; and an encrypted data storage part
13Q for storing encrypted data
E<SB>K</SB>(D)*encrypted data key
E<SB>Px</SB>(K)*n encrypted
dispersion keys while correlating them. ;
COPYRIGHT: (C)2008,JPO&INPIT

Abstract of Cited Ref 2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-185573
(43)Date of publication of application : 02.07.2004

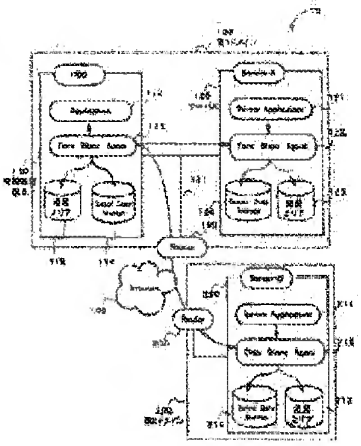
(51)Int.Cl. G06F 13/00
G06F 15/00

(21)Application number : 2002-355286
(22)Date of filing : 06.12.2002

(71)Applicant : NEC INFRONTIA CORP
(72)Inventor : ANDO MINAO

(54) DATA WRITING METHOD AND DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data writing method and a data writing device for stably and reliably storing data generated in an information equipment terminal in a data storage at a remote place connected thereto via the Internet or the like.
SOLUTION: Important data such as sales data generated in an information equipment terminal 110 such as a POS terminal are stored in an internal local data storage 114, and also stored in a server data storage 214 in a server 210 at a remote place connected thereto via the Internet 133. When no data writing takes place due to abnormalities in line or the like, a data store agent 113 saves the writing command in a saving area 115. After return to the normal state, the data store agent 114 acquires this stored writing command and retries it.



Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed more than three months after the U.S. filing date, OR more than three months after the date of entry of the national stage of a PCT application, AND after the mailing date of the first Office Action on the merits, whichever occurs first, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of foreign patents in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: September 29, 2014

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

Electronic Acknowledgement Receipt

EFS ID:	20271042
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/joanne ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	29-SEP-2014
Filing Date:	10-FEB-2012
Time Stamp:	16:57:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$780
RAM confirmation Number	3976
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	104093-0002-105_Extension.pdf	89188 49627a2222b2f489e0fad2598b8ae6dd3f5b3612	no	1
Warnings:					
Information:					
2		104093-0002-105_NonFinal_Response.pdf	118811 32c7fdd33e8d80a191e7f72220e29b94585dcf7f	yes	9

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	9

Warnings:					
Information:					
3	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	81188 b5fe934b4aba102079leac50eac0ce7a7e0dd9a2	no	2
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	132515 9132fc57fe8ca5a383ebb501853de886c258eb8c	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Foreign Reference	JP2004-185573_English_Abstract.pdf	52468 eecfc8bfb140ca968e9f1c6efd9c3c3bc74d7f4f	no	1
Warnings:					
Information:					
6	Foreign Reference	JP2005267520A_English_Abstract.pdf	697061 6180479524d805f7e95ab112e5a4d6f539800c90	no	1
Warnings:					
Information:					

7	Foreign Reference	JP2007-334836_English_Abstract.pdf	55565 ce638736c5c5ac58bd3696d75305b1cdfcf9c209	no	1
Warnings:					
Information:					
8	Foreign Reference	JP2008103936_English_Abstract.pdf	130589 bb1edd5f6eff442e359d089356c617b7ec9b3bab	no	2
Warnings:					
Information:					
9	Foreign Reference	JP2008250931A_English_Abstract.pdf	127856 7fa9368e33ed2daa8039cd70165cd89e4e2abfc8	no	1
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	32443 1f189bd937ed964de60edd884dd399dc032284a5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1517684		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2005267520 A**

(43) Date of publication of application: **29.09.05**

(51) Int. Cl **G06F 15/00**
G09C 1/00
H04L 9/32

(21) Application number: **2004082419**

(22) Date of filing: **22.03.04**

(71) Applicant: **NTT COMWARE CORP**

(72) Inventor: **WATANABE MASAHIRO**

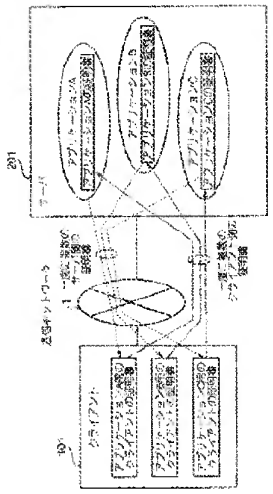
(54) **MUTUAL CERTIFICATE AUTHENTICATION SYSTEM, AND MUTUAL CERTIFICATE AUTHENTICATION METHOD**

COPYRIGHT: (C)2005,JPO&NCIPI

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a mutual certificate authentication system capable of mutually authenticating a plurality of certificates with one-time communication route establishment processing, and suppressing the increase of time and computer resources for establishing a communication route, and suppressing the increase of a communication route management cost.

SOLUTION: A client 101 being a communication route establishment demander transmits a communication route establishment demand to a server 201 and receives the plurality of certificates from the server. Then the certificates received from the server 201 are authenticated and a plurality of kinds of client certificates are transmitted to the server 201. The server 201 authenticates the plurality of certificates received from the client 101 and transmits a communication route establishment report to the client 101.



Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated May 1, 2014, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,615,084	12-24-2013	Schneider	
		US-8,396,895	03-12-2013	Miloushev et al.	
		US-8,205,090	06-19-2012	Oom Temudo de Castro et al.	
		US-7,260,727	08-21-2007	Fougeroux et al.	
		US-2010/0293380-A1	11-18-2010	Wiseman et al.	
		US-2010/0268966-A1	10-21-2010	Leggette et al.	
		US-2010/0153686-A1	06-17-2010	Frank	
		US-2010/0046750-A1	02-25-2010	Asfour	
		US-2009/0316892-A1	12-24-2009	Candelore	
		US-2008/0297326-A1	12-04-2008	Chakraborty et al.	
		US-2007/0122111-A1	05-31-2007	Yamamoto et al.	
		US-2003/0236943-A1	12-25-2003	Delaney	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		JP-2004-185573-A	07-02-2004	Nec Infrontia Corp		√
		JP-2005-267520-A	09-29-2005	Ntt Comware Corp		√
		JP-2007-334836-A	12-27-2007	Canon Kk		√
		JP-2008-103936-A	05-01-2008	Toshiba Corp		√
		JP-2008-250931-A	10-16-2008	Toshiba Corp		√

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

45953482_1

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2008250931 A

(43) Date of publication of application: 16.10.08

(51) Int. Cl: G06F 21/24 20060101
G09C 1/00 20060101

(21) Application number: 2007094907

(22) Date of filing: 30.03.07

(71) Applicant: TOSHIBA CORP

(72) Inventor: UMEZAWA KENTARO
YAMANAKA SHINJI
TAKAHASHI TOSHINARI

(54) SYSTEM FOR RESTORING DISTRIBUTED INFORMATION, INFORMATION UTILIZING DEVICE, AND VERIFICATION DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent tracking by a malicious subject while entrusting restoration processing to a restoring device.

SOLUTION: A distributed information management device 2 stores each of the n-number of distributed information generated from secret information to be kept secret using a (k, n) threshold secret sharing scheme. An information utilizing device 1 generates and stores the n-number of random numbers, and makes an information restoration request including a distributed information identifier for uniquely identifying the requested distributed information, and the respective random numbers. A distributed information management device 2 conceals the distributed information by the random numbers and transmits it to a restoring device 3. Upon receiving the k-number of concealed distributed information, the restoring device 3 performs restoration processing of the (k, n) threshold secret sharing scheme to restore the concealed secret information. The information utilizing device obtains the secret information by decoding the restored concealed secret information using the random numbers.

COPYRIGHT: (C)2008,JPO&INPIT



Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 67/108	4/25/2014	mc
G06F 11/1092	4/25/2014	mc

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/17/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	4/25/2014	mc
google searched "array coding" and "erasure OR error coding raid"	4/25/2014	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	10/3/2014	mc

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
google searched "RAID 0+1" "RAID storage randomize"	10/3/2014	mc

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	26 (with claim terms)	10/3/2014	mc

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	h04L67/108.cpc. and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025") and (bit$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/10/03 12:56
L3	1	reed adj solomon adj coding and distributed adj storage and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; USOCR	OR	OFF	2014/10/03 12:56
L4	0	(distributed adj storage) file (segmentation OR splitting OR separation) same bits and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/10/03 12:56
L5	0	g06f11/1092.cpc. and distributed adj storage and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; USOCR	OR	OFF	2014/10/03 12:56
L6	0	distributed near storage near10 (bits or bytes) and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/10/03 12:56
L7	183	array adj coding	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/10/03 12:56
L8	118	array adj coding and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/10/03 12:56
L9	41	726/26.ccls. and @pd>"20140501" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2014/10/03 12:57
L13	1	"7391865".pn.	USPAT	AND	OFF	2014/10/03 13:03
L14	2	("5910987" "5450099").pn.	USPAT	OR	OFF	2014/10/03 13:10

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L10	1	726/26.ccls. and splitting adj information	USPAT; UPAD	AND	OFF	2014/10/03 12:58
L11	43	(splitting adj information).clm.	USPAT; UPAD	AND	OFF	2014/10/03 12:58
L12	3	(splitting adj information and threshold adj number).clm.	USPAT; UPAD	AND	OFF	2014/10/03 12:59

10/3/2014 1:17:44 PM
C:\Users\mchao\Documents\EAST\Workspaces\13371363.wsp

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0167408	09-2003	Fitzpatrick et al.	713/201
*	B	US-6,557,123	04-2003	Wiencko et al.	714/701
*	C	US-5,991,414	11-1999	Garay et al.	713/165
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Wells; The OceanStore Archive: Goals, Structures, and Self-Repair; 2001; Retrieved from the Internet <URL: .oceanstore.org/publications/papers/pdf/>; pp. 1-20 as printed.
	V	Wylie et al.; Selecting the right data distribution scheme for a survivable storage system; 2001; Retrieved from the Internet <URL: repository.cmu.edu/compsci/2164/?utm_source=repository.cmu.edu%2Fcompsci%2F2164&utm_medium=PDF&utm_campaign=PDFCoverPages>; pp. 1-25 as printed.
	W	Buckhard et al.; Disk Array Storage System Reliability; 1993; Retrieved from the Internet <URL: ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=627346&tag=1>; pp. 1-26 as printed.
	X	Tewari et al.; High Availability in Clustered Multimedia Servers; 1996; Retrieved from the Internet <URL: ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=492215>; pp. 1-10 as printed.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-8,615,084	12-24-2013	Schneider	
/M.C./		US-8,396,895	03-12-2013	Miloushev et al.	
/M.C./		US-8,205,090	06-19-2012	Oom Temudo de Castro et al.	
/M.C./		US-7,260,727	08-21-2007	Fougeroux et al.	
/M.C./		US-2010/0293380-A1	11-18-2010	Wiseman et al.	
/M.C./		US-2010/0268966-A1	10-21-2010	Leggette et al.	
/M.C./		US-2010/0153686-A1	06-17-2010	Frank	
/M.C./		US-2010/0046750-A1	02-25-2010	Asfour	
/M.C./		US-2009/0316892-A1	12-24-2009	Candelore	
/M.C./		US-2008/0297326-A1	12-04-2008	Chakraborty et al.	
/M.C./		US-2007/0122111-A1	05-31-2007	Yamamoto et al.	
/M.C./		US-2003/0236943-A1	12-25-2003	Delaney	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/M.C./		JP-2004-185573-A	07-02-2004	Nec Infrontia Corp		√
/M.C./		JP-2005-267520-A	09-29-2005	Ntt Comware Corp		√
/M.C./		JP-2007-334836-A	12-27-2007	Canon Kk		√
/M.C./		JP-2008-103936-A	05-01-2008	Toshiba Corp		√
/M.C./		JP-2008-250931-A	10-16-2008	Toshiba Corp		√

Examiner Signature	/Michael Chao/	Date Considered	10/03/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature	/Michael Chao/	Date Considered	10/03/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

45953482_1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 11/26/2014

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
11/26/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No. 13/371,363	Applicant(s) ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/29/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-27* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This action is in response to argument filed 9/29/2014. Application 13/371,363 claims priority to 9/29/2014. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Response to Arguments

The present amendment to the claims (9/29/2014) has obviated the double patenting issue, the rejection has been withdrawn.

As previously agreed in the in person interview on 9/22/2014, the amendment stating that shares are based on some, but not all, of the units of data overcomes the Krawczyk references as previously cited.

As Applicant has not argued the amendment or otherwise discussed the change in scope (Rem. on 9/29/2014) it is necessary for the Examiner to state his understanding of the current scope of the claims.

Examiners previous response (5/01/2014) and position during the interview (9/22/2014) is that Applicant's claimed (1) "data splitting information" merely implicated the genus of all systems which otherwise fulfill the requirement that (2) "the data set is restorable by accessing less than all, but at least a threshold number of the plurality of

shares." Ostensibly, the Examiner reasons that any system which fulfills the requirement (2) must separate the data in a particular manner in order to achieve the properties of (2); thus the "data splitting information" (1) is either inherent or generic to all systems which accomplish (2).

The Examiner (Office Action 5/01/2014 p. 5 discussing the Krawczyk references) and Applicant (Affidavit on 2/13/2014) agree that the Krawczyk references transform the input data into shares by a computation which takes the entire input data to formulate each output share. Hence, by stating that each share cannot be "based on" or "contain" all the units of data the claim avoids the coding mechanisms of Krawczyk references. This is because Krawczyk contemplates a computation which requires all the input units, thereby "basing" or "containing" in the output shares data from all the input units.

(A) (Note that the Examiner suggested the language "based on" rather than "contains")

The result is that the amended claim (9/29/2014) now avoids the Krawczyk references and contemplates embodiments in which the units of data are merely "mapped" to output shares without computations which require all the units of data, see e.g. Applicant's fig. 35.

(B) (During the interview 9/22/2014 Applicant also made reference to ¶¶ 291, 303-304, 311-312, 319-324, 333-336).

(A) Scope of "based on one or more, but not all, of the units of data" compared with "contains one or more, but not all, of the units of data".

A claim which recites "contains" merely requires that some of the units, which the Examiner will discuss as bits for simplicity, are found in each share, but no share comprises all of them. Presumably this would avoid Krawczyk since each share of Krawczyk is formulated based on all of the units and must either be considered to "contain" either all or none of the input units. (Because the data of Krawczyk is transformed, it might either be considered to "comprise" all the input or none of the input since the input is not verbatim contained in the shares. This would therefore distinguish over the previously cited art (Krawczyk) by limiting what input data forms the shares.

A claim which recites "based on" differentiates from Krawczyk more specifically excludes the type of computation of Krawczyk (as described above) which implies that each share must contain data which is only related to a subset of the input (again e.g. Applicant's Fig. 23). This therefore distinguishes over the previously cited art by limiting either the input or the mechanism of computation.

This may seem to be a pointless discussion; however, a search of the prior art revealed that the distinction is actually quite significant.

As an Example of the types of splitting the prior art contains see Wylie (Selecting the right data distribution scheme for a survivable storage system) in which Wylie surveys the different "threshold" methods of creating the "shares" as "replication, Decimation (Striping), Splitting (XORing), Information Dispersal, Secret Sharing, Ramp Schemes" (Wylie § 2.1).

Most of these systems generate output shares "**based** on" all the data (Information Dispersal, Secret Sharing, Ramp Schemes) the splitting scheme does not tolerate failure (Splitting "all n shares are needed to recover the original data." Wylie § 2.1), lastly replication and decimation are both techniques contemplated by RAID.

Among RAID schemes many utilize "parity" where the parity is located in each share (See e.g. Xu B-Code § 2.5). When the parity is in each share then the share is arguably "based on all the units of data".

Conversely a claim reciting "**contains**" would only require that the input data were mapped to the various shares without modification or coding that was dependent upon all the data. This would therefore not exclude a majority of RAID algorithms.

Both embodiments exclude all "information dispersal, secret sharing, and Ramp schemes" as contemplated by Wylie.

There is also the related issue of whether a "share" can be "based on" less than all of the input data when the "share" must have "hash information" which is defined by the claim to be based on all of the input data.

The Examiner would therefore retract his previous suggestion of the wording "based on" and suggest the original wording, while slightly broader, "contains" be adopted. This would broaden the claims slightly to allow references such as Plank et al. (A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems) to be applicable to the claims, but would improve the form of the claims.

To summarize, the phrase "based on one or more . . ." appears to exclude commonly used RAID parity information, but also the claimed "data indicative" since the data indicative is by definition based on all the data. Using the term "comprises one or more, but not all of the units of data" would be more logically consistent with the intent of the claim.

(B) The referenced sections of the specification discussing how "splitting data" is utilized.

The Examiner has previously suggested that the Applicant define how the "data splitting information" is used (Office Action 5/01/2014 p. 7) and would again note that Applicant has avoided any reference to a particular embodiment describing the use of "data splitting information"; presumably to avoid prosecution history estoppel. Further, the present amendment, while overcoming the prior rejection, distinguishes based on the output, or product, of the system, rather than how the system operates (e.g. how the "data splitting information" is used). This yields some issues of claim interpretation that require discussion.

(1) When the result of a system, the product, is claimed rather than how it is achieved, the Examiner should consider all methods of achieving that result.

This merits consideration of numerous methods of achieving the product where no method is more appropriate to cite in a grounds of rejection. Therefore, note the plurality of potential combinations described below as co-equal methods of achieving the claimed result.

Additionally it is difficult to discern the exact properties of systems which would accomplish those stated results. For example, those portions referenced by Applicant during the interview on 9/25/2014 (¶¶ 291, 303-304, 311-312, 319-324, 333-336) do not illustrate a threshold system, as claimed: "wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares." The only section of the specification which describes a scheme which allows recovery of data with "less than all of the shares" is found in Applicant's specification ¶¶ 292-294. These particulars are not required by the claim, nor can the Examiner read the specification into the claims, MPEP 2111. However, as Applicant's specification describes no other embodiments which comply with the claim it bears additional consideration.

The particular method of ¶¶ 292-294 was not found in the prior art, however, as the particulars are unclaimed, it is substantially identical to a RAID mirroring system. The claimed "shares", broader still than the embodiment of ¶¶ 292-294, are analogous to several RAID type systems premised on Array Coding.

The Examiner concedes that it could be argued that "is based on" might be read to exclude the "parity" disks of Xu and Burkhard since the use of the parity is that it represents all the data inputs. However, such that there exist some shares that do not include "parity" in both these references it fairly discloses that "each share is based on one or more, but not all, of the units of data" since the parity disks might be viewed as extra data that is not a "share" and the transitional phrase comprising does not exclude additional elements, MPEP 2111.03.

The Examiner has reviewed Applicant's product disclosures. While not illustrating how the process is actually performed, the diagrams of <https://www.securityfirstcorp.com/sharcdc.php> are analogous to the RAID schemes currently cited. "Advanced Secure" appears to be the RAID system of Xu or Burkhard and "Advanced Multi-site" appears to be a RAID 0+1 system discussed in Wiencko.

The Examiner would further note that none of the references cited, nor those seen in the present search revealed any art in which "the encryption key is used as data splitting information". However, note that the act of encryption inherently "transforms" the data and thereby acts to determine which units of encrypted data a share is "based on". This is because a public key encryption system works in the same way as Krawczyk's IDA scheme.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 6-11, 15-20, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred

to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)

With respect to claims 1, 10, 19, SSMS teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

Encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set; ("1. Choose a random encryption key K. Encrypt the secret S using the encryption function ENC under the key K, let E = $ENC_K(S)$" SSMS p. 6).

[creating hash information based on a hash operation using the data set;]

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; (SSMS discloses information used to split the data into shares)

("We assume a generic information dispersal algorithm that we denote by IDA, and which works for parameters n (number of file fragments) and m (number of required fragments to reconstruct the file)." SSMS p. 6)

("we outline the following simple information dispersal scheme based on Reed Solomon erasure codes. The information to be shared is partitioned into m equal parts where each part is viewed as an element over a finite field (e.g. GF@), for a large enough prime p) . These m elements are then viewed as coefficients of a polynomial of degree m - 1, and the n fragments for distribution are obtained by evaluating this polynomial in n different points." SSMS pp. 5-6. This details how the information used to determine into which of a plurality of shares data will be placed.)

separating the encrypted data set into the plurality of shares based on the data splitting information; ("2. Using IDA partition the encryption file E into n

fragments, E_1, E_2, . . . , E_n." SSMS p. 6)("3. Using PSS generate n shares for the key K" SSMS p. 6)

including in the plurality of shares (a) data indicative of the encryption key and [(b) the hash information]; and ("4. Send to each participant P_i, I = 1, 2, . . . , n the share $S_i = (E_i, K_i)$. The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 7)

causing the plurality of shares to be stored in respective separate storage locations; (to each participant. SSMS p. 7. "The distribution process gets ~ 1 sin put the secret S (and the values of n and m) and generates n shares Sl, Sz, . . , , Sn, which are privately delivered to the system participants." SSMS p. 3) (where the system is a set of distributed servers "These constructions have many applications, especially in distributed scenarios where secrecy and integrity of information are to be protected. For example, consider a group of five servers sharing a data base of confidential information such that no pair of servers is allowed to learn about the information without the collaboration of a third one. (That is, the system tolerates up to two corrupted servers without compromising the information)." SSMS p. 2)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The reconstruction process reconstructs the correct secret when input with any subset of m shares." SSMS p. 3)

SSMS does not disclose:

creating hash information based on a hash operation using the data set;

(b) the hash information;

Wherein each share is based on one or more, but not all, of the units of data of the encrypted data set; (see above for explanation)

DFSID discloses an analogous algorithm purposed for use with SSMS (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]").

DFSID further creating hash information based on a hash operation using the data set;

(b) the hash information:

"1. Use IDA to distribute the file among the n processors. Denote by F_i the piece distributed to processor p_i.

2. Fingerprint each piece F_i, i = 1, . . , n, by the DFP method (as described in Section 3). That is, for each i, compute $H(F_i)$ and then distribute this value among all processors using the coding function C. (Each processor p_j gets a share s_{ij} corresponding to $H(F_i)$)." (DFSID § 4.1, see also § 4.1 generally)

A fingerprint is a hash, see DFSID § 3.

A person of ordinary skill in the art at the time of invention would have modified SSMS by including the fingerprint of DFSID. It would have been obvious to one of ordinary skill in the art at the time of invention to modify SSMS with DFSID since it was suggested explicitly by DFSID (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]") and to solve the information integrity problem (DFSID Abstract).

SSMS in view of DFSID does not disclose:

Wherein each share is based on one or more, but not all, of the units of data of the encrypted data set; (see above for explanation)

SSMS and DFSID both contemplate an IDA scheme to divide the data (see above) which is generic to any scheme that allows recovery with only m required fragments/shares out of n total.

"We assume a generic information dispersal algorithm that we denote by IDA, and which works for parameters n (number of file fragments) and m (number of required fragments to reconstruct the file)." (SSMS § 3)

"The basic approach taken in IDA is to distribute the information being protected among n active processors, in such a way that the recovery of the information is possible in the presence of up to t failed (inactive) processors at the time of reconstruction." (DFSID § 1.1) (SSMS § 3)

(A) Xu also contemplates the concept of restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("Erasure-correcting codes are a mathematical means of representing data so that lost information can be recovered. With an (n,k) erasure-correcting code, we represent k symbols of the *original* data with n symbols of *encoded* data (n – k is called the amount of *redundancy* or *parity*)." Xu § 2.1)

Xu further teaches that: ("The complexity of the computations needed to construct the encoded data (a process called *encoding*) and to recover the original data

(a process called *decoding*) is an important consideration for practical systems. Array codes are ideal in this respect. Array codes have been studied extensively." Xu § 2.1)

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; ("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimentional array of size l x n. In a distributed storage system, the bits in the same column are stored in the same disk. If any bit in a disk is corrupted, then the disk is considered to be a failure disk and needs repair, i.e., the corresponding column of the code is considered to be an erasure." Xu § 2.1)

separating the encrypted data set into the plurality of shares based on the data splitting information ("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimentional array of size l x n. In a distributed storage system, the bits in the same column are stored in the same disk. If any bit in a disk is corrupted, then the disk is considered to be a failure disk and needs repair, i.e., the corresponding column of the code is considered to be an erasure." Xu § 2.1)

, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set; ("The EVENODD code has a very simple structure; all bits are placed in an array of size (p-1) x (P+2), where p is a prime number, i.e., it has p+2 columns. All the information bits are placed in the first p columns, and the last 2 columns contain all parity bits" Xu § 2.2)

See also Xu § 2.4.1 ("In X-Code, information bits are placed in array of size (n-2) x n. Like other array codes [2][3][5][11], parity bits are constructed by adding the information bits along several parity check *lines* or *diagonals* of given slopes." Alternative methods of splitting the data)

See also Xu § 2.5 B-codes for an additional method of splitting data.

A person of ordinary skill in the art at the time of invention would have modified the Information Dispersal Algorithm of Krawczyk with Xu by utilizing any of the array coding methods disclosed in Xu as a substitute erasure coding method for that disclosed in SSMS. It would have been obvious to one of ordinary skill in the art at the time of invention to use an alternate erasure coding method in order to obtain efficient encoding and decoding, for which array codes are ideal Xu § 2.1.

(B) Burkhard discloses a similar array coding system in which "MDS disk organizations are described in terms of two parameters n and m. MDS organizes a file into n equal-sized pieces, referred to as fragments, with each stored as an ordinary file on a different disk. The second MDS parameter m specifies the number of fragments such that any m suffice to reconstruct the file." (Buckhard § 2)

Buckhard further discloses data splitting information (Buckhard § 2 "An example dispersal matrix").

A person of ordinary skill in the art at the time of invention would have modified the IDA algorithm of Krawczyk with Buckhard by utilizing the MDS organization method of Buckhard (§ 2). It would have been obvious to one of ordinary skill in the art at the

time of invention to utilize the MDS method of Buckhard as the IDA scheme of Krawczyk because they are methods which share the common property that is disclosed as desirable in the references ("m of n" Buckhard § 2. DFSID § 1.1. SSMS § 3).

(C) Wiencko discloses that RAID 0+1, while not a true m of n scheme, allows for data recoverability (Wiencko background).

Wiencko discloses that RAID 0+1 is: "In a "0+1" array, two striped arrays of five disks each mirror the other." (Wiencko background)(illustrated in Fig. 2).

Wiencko then discloses a proposed m of n scheme to improve RAID (Wiencko summary)

A person of ordinary skill in the art at the time of invention would have modified the IDA algorithm of Krawczyk with Wiencko by selecting either the RAID 0+1 system, or the Wiencko improvement thereupon as the IDA scheme of Krawczyk. It would have been obvious to one of ordinary skill in the art at the time of invention to utilize the RAID 0+1 or the m of n Wiencko improvement as the IDA scheme of Krawczyk because they are methods which share the common property of recoverability in the face of failures (Wiencko Background and Summary. DFSID § 1.1. SSMS § 3).

With respect to claims 2, 11, 20, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. (determinism is a necessary feature of any system that will retrieve obfuscated data)

With respect to claims 3, 12, 21, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2)

With respect to claims 5, 14, 23, SSMS in view of DFSID discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2)

With respect to claims 6, 15, 24, SSMS in view of DFSID discloses: wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm. ("In order to achieve a space efficient secret sharing scheme we

combine an information dispersal scheme with a secure encryption scheme and a perfect (e.g. Shamir's) secret sharing scheme." SSMS § 3)

With respect to claims 7, 16, 25, SSMS in view of DFSID discloses: wherein the step of including data indicative of the encryption key comprises:
encrypting the encryption key with a second key; and
including in the plurality of shares data indicative of the encrypted encryption key. ("The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 6. See also p. 7. Encryption requires a key of some kind.)

With respect to claims 8, 17, 26, SSMS in view of DFSID discloses: further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("Send to each participant . . . portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS § 3. A second encryption, a second key, to transmit the share, and therefore not contained within the share.)

With respect to claims 9, 18, 27, SSMS in view of DFSID discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Send to each participant . . ." SSMS § 3.)

Claims 1, 2, 6-11, 15-20, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells (The OceanStore Archive: Goals, Structures, and Self-Repair) in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)}.

With respect to claims 1, 10, 19, Wells discloses:

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, by processing circuitry, the data set based on an encryption key to produce an encrypted data set; ("In a digital archive, end-to-end encryption can be used to preserve the privacy of documents" Wells § 2.1 Security)

creating hash information based on a hash operation using the data set; ("As mentioned in Section 3.3, the GUID of a block is the root hash in a hierarchical verification tree over the block's data and its fragments." Wells § 3.1)

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed; (Wells § 3.2 RAID, as combined below)

separating the encrypted data set into the plurality of shares based on the data splitting information, (Wells "distributed archive")

wherein each share is based on one or more, but not all, of the units of data of the encrypted data set; (Wells § 3.2 RAID, as combined below)

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and (a) ("We produce a hash over each fragment, concatenate the corresponding hash with a sibling hash to produce a higher level hash, and continue the algorithm until there is a topmost hash. We then store with each fragment all of the sibling hashes to the topmost hash, a total of log n hashes" Wells § 3.4) (b) ("That is, there must be a key which the responsible party stores in addition to the GUID of an erasure-encoded object, and this key must validate the GUID of any server claiming to store a fragment" Wells § 8 Future work)

causing the plurality of shares to be stored in respective separate storage locations; (Wells "distributed archive")

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. (Wells § 3.2)

Wells does not disclose that the distribution scheme (erasure coding in Wells) creates shares which are not based on all the units of data, as claimed:

wherein each share is based on one or more, but not all, of the units of data of the encrypted data set.

As cited above, each of Weincko, Buckhard and Xu contemplate splitting data in a RAID system "wherein each share is based on one or more, but not all, of the units of data of the encrypted data set".

A person of ordinary skill in the art at the time of invention would have used any of the RAID mechanisms discussed in Weincko, Buckhard or Xu in the system of Wells

as a method of separating data to recover from faults and including the further encryption and hashing of Wells to archive the other archival goals (Wells § 2.1).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Wells with any of Weincko, Buckhard or Xu since Wells himself contemplates that a RAID system is a related storage method (Wells § 7.1).

With respect to claims 2, 11, 20, Wells discloses a deterministic method.

With respect to claims 7, 16, 25, Wells discloses a encrypting the encryption key. ("One simple mechanism for an individual who wished to pass on his key would be to encrypt it using his inheritors' keys, and place the results in the care of his estate's executor, but this scheme relies on the trustworthiness of the executor." Wells § 2.1 Usability)

With respect to claims 8, 17, 26, Wells discloses storing the encrypted key (Wells § 2.1 Usability)

With respect to claims 9, 18, 27, Wells discloses separate physical storage (Wells "distributed archive").

Claims 3, 5, 12, 14, 21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as

SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)} in view of either {Fitzpatrick (US 2003/30167408) or Tewari et al. (High Availability in Clustered Multimedia Servers)}.

The above combination (Krawczyk in view of any of {Wiencko, Buckhard or Xu} does not discuss that the RAID distribution scheme is random.

Tewari discloses a method of randomizing the parity placement (see § 4.3.2) in RAID (Tewari Abstract).

A person of ordinary skill in the art at the time of invention would have modified Krawczyk as modified by any of Wiencko, Buckhard or Xu with Tewari by further optimizing the RAID system according to Tewari. It would have been obvious to one of ordinary skill in the art at the time of invention to further modify the combination in order to optimize the RAID system (Tewari § 1.2).

Fitzpatrick discloses a method of randomizing data placement in a storage system such as RAID (Fitzpatrick ¶ 3) for the purpose of data security (Fitzpatrick ¶ 5).

A person of ordinary skill in the art at the time of invention would have modified Krawczyk as modified by any of Wiencko, Buckhard or Xu with Fitzpatrick by further optimizing the RAID system according to Fitzpatrick. It would have been obvious to one

of ordinary skill in the art at the time of invention to further modify the combination in order to secure the data (Fitzpatrick ¶ 5).

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over SSMS in view of DFSID in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)} in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, SSMS in view of DFSID does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a

form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified SSMS in view of DFSID with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 3, 5, 12, 14, 21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells (The OceanStore Archive: Goals, Structures, and Self-Repair) in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)} in view of either {Fitzpatrick (US 2003/30167408) or Tewari et al. (High Availability in Clustered Multimedia Servers)}.

The above combination (Wells in view of any of {Wiencko, Buckhard or Xu} does not discuss that the RAID distribution scheme is random.

Tewari discloses a method of randomizing the parity placement (see § 4.3.2) in RAID (Tewari Abstract).

A person of ordinary skill in the art at the time of invention would have modified Wells as modified by any of Wiencko, Buckhard or Xu with Tewari by further optimizing the RAID system according to Tewari. It would have been obvious to one of ordinary skill in the art at the time of invention to further modify the combination in order to optimize the RAID system (Tewari § 1.2).

Fitzpatrick discloses a method of randomizing data placement in a storage system such as RAID (Fitzpatrick ¶ 3) for the purpose of data security (Fitzpatrick ¶ 5).

A person of ordinary skill in the art at the time of invention would have modified Wells as modified by any of Wiencko, Buckhard or Xu with Fitzpatrick by further optimizing the RAID system according to Fitzpatrick. It would have been obvious to one of ordinary skill in the art at the time of invention to further modify the combination in order to secure the data (Fitzpatrick ¶ 5).

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells (The OceanStore Archive: Goals, Structures, and Self-Repair) in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); or Xu (Highly Available Distributed Storage Systems)} in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, Oceanstore as disclosed in Wells does not describe rearranging the storage.

Kubiatowicz further discloses elements of an Oceanstore system.

Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have combined Wells in view of { Wiencko, Buckhard or Xu} with Kubiatowicz by including a method for versioning the

files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage or, alternatively, because Kubiatowicz explicitly contemplates that it is intentioned for the same type of system (Oceanstore).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Garay et al. (US 5,991,414) is a publication which contemplates a further extension of the Krawczyk references.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Chao/
Primary Examiner, Art Unit 2492

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/02/2012	07/16/2012	03/12/2013	09/06/2013	10/03/2014				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				
	17	✓	✓	✓	✓	✓				
	18	✓	✓	✓	✓	✓				
	19	✓	✓	✓	✓	✓				
	20	✓	✓	✓	✓	✓				
	21	✓	✓	✓	✓	✓				
	22	✓	✓	✓	✓	✓				
	23	✓	✓	✓	✓	✓				
	24	✓	✓	✓	✓	✓				
	25	✓	✓	✓	✓	✓				
	26	✓	✓	✓	✓	✓				
	27	✓	✓	✓	✓	✓				

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,041,875	10-18-2011	Shah et al.	
		US-8,095,800	01-10-2012	Creary et al.	
		US-8,578,076	11-05-2013	van der Linden et al.	
		US-7,213,158	05-01-2007	Bantz et al.	
		US-6,807,649	10-19-2004	Murthy	
		US-2003/0188153-A1	10-02-2003	Demoff et al.	
		US-2003/0055905-A1	03-20-2003	Nishiyama et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

47607385_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

47607385_1

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed after the mailing date of a Final Office Action or Notice of Allowance, whichever occurred first, but on or before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Supplemental Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(2), that no item of information contained in this Supplemental Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Supplemental Information Disclosure Statement

was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Supplemental Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: December 3, 2014

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	20856657
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	03-DEC-2014
Filing Date:	10-FEB-2012
Time Stamp:	17:40:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	4401
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	81338 6fc2e5f4f7ac33c5879c7c9bab4c2ac80b3aac55	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	131660 8a7082de504c8d79d58ac66d2b33b062ad689a66	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (SB06)	fee-info.pdf	30500 17a1967508d5de1e2efc314b4db655f7586daefb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	243498		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Lise Ann Ruggeri-Kalil
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,662,299	12-09-2003	Price, III	
		US-7,499,905	03-03-2009	Jaschek et al.	
		US-6,853,988	02-08-2005	Dickinson et al.	
		US-7,260,724	08-21-2007	Dickinson et al.	
		US-5,239,659	08-24-1993	Rudeseal et al.	
		US-6,381,331	04-30-2002	Kato	
		US-6,009,173	12-28-1999	Sumner	
		US-20040078542	04-22-2004	Fuller et al.	
		US-20030084397	05-01-2003	Peleg	
		US-6,519,262	02-11-2003	Stephens et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		CN-101375284-A	02-25-2009	Orsini Rick L		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

47976134_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Kim et al., "Secure Group Key Management for Storage Area Networks," IEEE Communications Magazine, August 2003, pp. 92-99.	
		Bendix, "RAID and Informix Databases," White Paper, Advanced **T**echnology Group, June 1995; Retrieved from the Internet <URL: informix.com.ua/articles/raid/raid.htm>; retrieved from the internet on December 3, 2014, pp. 1-15 as printed	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

47976134_1

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (SIDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed after the mailing date of a Final Office Action or Notice of Allowance, whichever occurred first, but on or before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(2), that no item of information contained in this Supplemental Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Supplemental Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075.

Dated: January 21, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
1900 University Avenue
6th Floor
East Palo Alto, California 94303-2284
(650) 617-4000
(617) 235-9492 (Fax)
Agent For Applicants

Espacenet

Bibliographic data: CN101375284 (A) — 2009-02-25

Secure data parser method and system

Inventor(s): ROGER DAVENPORT [US]; STEVEN WINICK [US] ± (DAVENPORT ROGER, ; WINICK STEVEN)

Applicant(s): ORSINI RICK L [US] ± (ORSINI RICK L)

Classification: - international: *G06F21/00*
- cooperative: G06F21/602; G06F21/606; G06F21/62; H04L63/04; H04L63/08; H04L63/0876; H04L69/14; H04L9/085; H04L9/3226; H04L9/3263; H04L2209/80

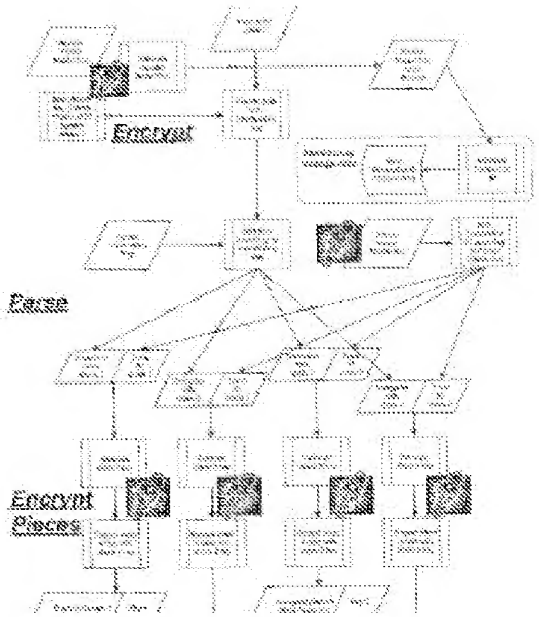
Application number: CN2005841868 20051025

Priority number (s): WO2005US38806 20051025 ; US20040622146P 20041025 ; US20050718185P 20050916

Also published as: CN101375284 (B) WO2006047694 (A1) US2014372770 (A1) US2013283065 (A1) US2013275768 (A1) more

Abstract of CN101375284 (A)

A secure data parser is provided that may be integrated into any suitable system for securely storing and communicating data. The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly. Encryption of the original data, the portions of data, or both may be employed for additional security. The secure data parser may be used to protect data in motion by splitting original data into portions of data, that may be communicated using multiple communications paths.




Obfuscate

Electronic Acknowledgement Receipt

EFS ID:	21264877
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Lise Ann Ruggeri-Kalil
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	21-JAN-2015
Filing Date:	10-FEB-2012
Time Stamp:	15:50:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	2250
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_SB08.pdf	132616 69666140e30ff617b0b438a3694107eed3ca9123	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	CN101375284.pdf	139475 23b489050f91890fdfed8a07d2f9172521b16aa1	no	2
Warnings:					
Information:					
3	Non Patent Literature	Bendix_RAID_and_Informix_Databases.pdf	1123926 db9c74f18bcf26672f1712ea20c3d9fe903431e6	no	15
Warnings:					
Information:					
4	Non Patent Literature	Kim_et_al_Secure_Group_Key_Management.pdf	1206245 1a0f7edf657d1dce63770ca5ef099fd25837a4da	no	8
Warnings:					
Information:					
5	Transmittal Letter	104093_0002_105_SIDS.pdf	81723 366a9f17fad423f25d7bcd9658ddc0441e496e70	no	2
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	30810 19d6c548b4783bc4c12bb942c6251b579f7856dd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2714795		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 03/18/2015

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
03/18/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*. (3) *George Ligler*.

(2) *Christopher Han (Reg. No. 70069)*. (4)_____.

Date of Interview: *12 March 2015*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☐ applicant ☒ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *SSMS in view of DSFID in view of various Array (RAID) coding references*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner agrees that if Shamir Secret Sharing is a principle of operation of the SSMS reference that the properties of Secret Sharing would be lost by modification with an array coding (RAID type) system.Examiner agrees that the discussed citation to Wells § 3.2 suggests that the combination of Wells with a RAID scheme would not be obvious.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Michael Chao/ Primary Examiner, Art Unit 2492	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,473,858	10-29-2002	Shimomura et al.	
		US-7,206,250	04-17-2007	Groux	
		US-20050289218	12-29-2005	Rothman et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

49325380_1

Electronic Acknowledgement Receipt

EFS ID:	21962359
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	06-APR-2015
Filing Date:	10-FEB-2012
Time Stamp:	15:20:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$780
RAM confirmation Number	1717
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_SB08.pdf	106212 a25332aa9abf3c5e723e324e975c1c3f3fec3ff6	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Transmittal Letter	104093_0002_105_IDS_Transmittal.pdf	81221 5e0b6d2858020932fad4e7a3e94fdcb37466ead4	no	2
Warnings:					
Information:					
3	Extension of Time	104093_0002_105_EOT.pdf	89246 0232fff5204589fb92c6d9bfb7d2f4a6835f5399	no	1
Warnings:					
Information:					
4		104093_0002_105_Amendment.pdf	135586 d4754fa5b6997acd4cfe705d17196ee84519408c	yes	5

Multipart Description/PDF files in .zip description

Document Description	Start	End
Response After Final Action	1	1
Applicant Arguments/Remarks Made in an Amendment	2	5

Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	32718 4a75e71fe2a21933e170746d036d871e03e8668a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	444983		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-105
Application Number 13/371,363	Filed February 10, 2012
For SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	
Art Unit 2492	Examiner M. W. Chao

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☒ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600.00
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card. ~~Form PTO-2038 is attached.~~

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration number 70,069 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Christopher J. Han/	April 6, 2015
Signature	Date
Christopher J. Han	(617) 951-7000
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☒ * Total of 1 forms are submitted.

49326315_1

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed after the mailing date of a Final Office Action, but before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(2), that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in

a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: April 6, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: Michael W. Chao

RESPONSE AFTER FINAL OFFICE ACTION

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

In response to the Office Action dated November 26, 2014, Applicants respectfully request reconsideration and withdrawal in view of the following remarks:

Remarks/Arguments begin on page 2 of this paper.

REMARKS

Claims 1-27 are pending in this application. Independent claims 1, 10, and 19 stand finally rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Krawczyk, *Secret Sharing Made Short* ("SSMS"), Krawczyk, *Distributed Fingerprints and Secure Information Dispersal* ("DFSID"), and one of U.S. Patent No. 6,557,123 ("Wiencko"), Burkhard, *Disk Array Storage System Reliability* ("Burkhard"), or Xu, *Highly Available Distributed Storage Systems* ("Xu"). In the alternative, independent claims 1, 10, and 19 stand rejected under 35 U.S.C. §103 as being allegedly obvious in view of Wells, *The OceanStore Archive: Goals, Structures, and Self-Repair* ("Wells") and one of Wiencko, Burkhard, or Xu. The dependent claims are also finally rejected under § 103 based on one or more combinations that include the above-identified references.

Summary of Examiner Interview

The undersigned wishes to thank Examiner Chao for the courtesies extended during the in-person interview conducted on Thursday, March 12, 2015. During the interview, the Examiner, the undersigned, and Applicants' expert, Dr. George Ligler, discussed the cited references and the rejections under § 103.

Regarding the rejection based on SSMS in combination with other references, tentative agreement was reached that the currently claimed inventions are not obvious from the combination of SSMS with DFSID and Wiencko, Burkhard, or Xu. Specifically, the undersigned and Applicants' expert presented arguments that secret sharing and maintaining security of the data are key principles of operation of the system described in SSMS, and that the Office Action's proposed combination of SSMS with Wiencko, Burkhard, or Xu would destroy these key principles and render SSMS inoperable for its intended purpose. The purpose of SSMS is clearly to provide a secure secret sharing scheme, as indicated by the title, "**Secret Sharing** Made Simple" (emphasis added). For example, SSMS pg. 137 states:

> In this note we present a solution to the above question which is surprising in two senses
>
> - The resultant scheme is extremely space (and communication) efficient. It realizes an *m*-threshold scheme, where *m* shares recover the secret **but *m*-1 shares give no (computational) information on the secret** . . .

> - The resultant solution is strikingly simple. It just **combines in a natural way traditional secret sharing schemes, with encryption and information dispersal techniques.**
>
> Our scheme is simple, practical and **provable secure** given a secure private key encryption system (in particular, it just requires the existence of a one-way function).

See SSMS, pg. 137 (emphasis added). This cited section of SSMS makes clear that at the core of SSMS is the principle of combining traditional secret sharing schemes with information dispersal techniques to provide a space-efficient secret sharing scheme that is "simple, practical, and provably secure." The Office Action proposes it would have been obvious to a person of ordinary skill in the art to replace these secret sharing features of SSMS (which are directed toward security) with features from Wiencko, Burkhard, or Xu that are directed towards error correction and fault tolerance.[1] However, this would be antithetical to SSMS's premise of using traditional secret sharing techniques for a "simple, practical, and provably secure" scheme. For example, as discussed in the Expert Declaration filed on February 13, 2014, SSMS uses each character of an original file F in the calculation of every one of the pieces F_i.[2] Furthermore, secret sharing algorithms include an "m of n" security feature, where the secret S may be recoverable using any m shares, but where no information about S may be determined from less than m shares. *See, e.g.,* SSMS pp. 138, 142. These aspects of secret sharing – *i.e.*, the manner in which the secret is held by multiple parties and the requirement that no information be recovered with less than m shares – are both critical to achieving the security provided by SSMS. *See* SSMS, abstract, pg. 137.

The Office Action's suggested combination of SSMS with Wiencko, Burkhard, or Xu would result in the loss of both of these fundamental security features, which would impermissibly change the operation of SSMS. For instance, the Office Action suggests modifying SSMS with Wiencko, Burkhard, or Xu so that the alleged shares are based on portions of the original data, rather than the entire original data as discussed in SSMS. But this is inconsistent with the fundamental principle of secret sharing that the shares be based on the entire original data. Moreover, the proposed combination would also result in the loss of the "m of n" security feature because each of the

[1] *See* Office Action, pp. 13-15. *See also* Wiencko col. 4 lines 55-58, Burkhard § 2, and, Xu § 2.1
[2] *See* Expert Declaration filed February 13, 2014, pp. 8-11.

alleged portions in Wiencko, Burkhard, or Xu reveal *some* of the original data, as discussed in the cited portions below.

> "…a disk array has n disks with a stripe set stored across the n disks…A "stripe" is that part of a stripe set that resides on a single disk. Every stripe of a stripe set is **an integer number of chunks**, and starts and ends at chunk boundaries…A "chunk" is the **maximum contiguous collection of data** that is treated as an indivisible unit by the Wiencko code." - Wiencko col. 7 line 15 to col. 8 line 54 (emphasis added)

> "Then the five fragments contain the following byte value expressed in octal notation: Fragments F_0, F_1, and F_2 consist of **every third value** in the file as demonstrated in figure 1… the three fragments F_0, F_1, and F_2 allow **very easy file reconstruction since merging them is all that is necessary**." - Burkhard, § 2 (emphasis added)

> "In an array code, the information (original) and parity bits are placed in a 2-dimensional array of size l x n. In a distributed storage system, the bits in the **same column** are stored in the same disk." - Xu, § 2 (emphasis added)

As seen above, each of the portions in Wiencko, Burkhard, and Xu contain portions of the original data. An adversary with knowledge of how the original data is arranged in the portions (e.g., contiguously in Wiencko, every third value in Burkhard, every column in Xu) would be able to recover the portion of original data without having access to a threshold number of other shares. In contrast, secret sharing, as discussed in SSMS, requires that *no information* about the original data be available to an adversary with less than the threshold number of shares. Therefore, if SSMS were combined with Wiencko, Burkhard or Xu, then the principles of secret sharing would be completely lost, and SSMS would become inoperable for its intended purpose. During the interview, the Examiner agreed that the currently claimed inventions would not be obvious from the combination of secret sharing, as discussed in SSMS, with the error correction and fault tolerance techniques of Wiencko, Burkhard, or Xu, and the Examiner agreed to reconsider the rejections under § 103 after receiving Applicants' written reply set forth above.

Regarding the Office Action's alternate rejection based on Wells in combination with other references, the Examiner agreed that § 3.2 of Wells disparages a combination with a RAID scheme (the basis for the combination suggested on pp. 19-20 of the Office Action). Therefore, in view of Wells' explicit teachings against combination with a RAID scheme, a person of ordinary skill in the

art would not have found it obvious to combine Wells with the RAID mechanisms discussed in Wiencko, Burkhard, or Xu, as suggested on pp. 19-20 of the Office Action.

For at least the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejections under § 103.

Conclusion

In view of the above, Applicants believe the pending application is in condition for allowance.

Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: April 6, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/371,363	Filing Date 02/10/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/06/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/EVELYN NIMMONS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**780**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed after the mailing date of a Final Office Action but before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(1), that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent

office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

Applicant submits herewith a copy of the foreign patent in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 06-1075, under Order No. 104093-0002-105.

Dated: April 15, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicant

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO-2004001561-A2	12-31-2003	Armoursoft Ltd		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	22068231
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	15-APR-2015
Filing Date:	10-FEB-2012
Time Stamp:	19:14:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	5289
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO2004001561.pdf	1357840 7937d402659fda5e5f440ab89b0186b5b66d7ea5	no	37
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_SB08.pdf	90448 74c0e858ac7508260f04d62288a2de049bf33544	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Transmittal Letter	104093_0002_105_IDS_Statement.pdf	83958 30227cda5bde07e5dc5b05377c29aed3a936ea7	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30752 db14ae24282fe1 1fa467a59fba560d5aa03db8cc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1562998		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 December 2003 (31.12.2003)

PCT

(10) International Publication Number
WO 2004/001561 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/GB2003/002656

(22) International Filing Date: 20 June 2003 (20.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0214414.5 21 June 2002 (21.06.2002) GB

(71) Applicant *(for all designated States except US)*: **ARMOURSOFT LIMITED** [GB/GB]; 1st Floor, Unit 1, Warren Court, Feldspar Close, Warren Park Way, Endersby, Leicester (GB).

(72) Inventors; and

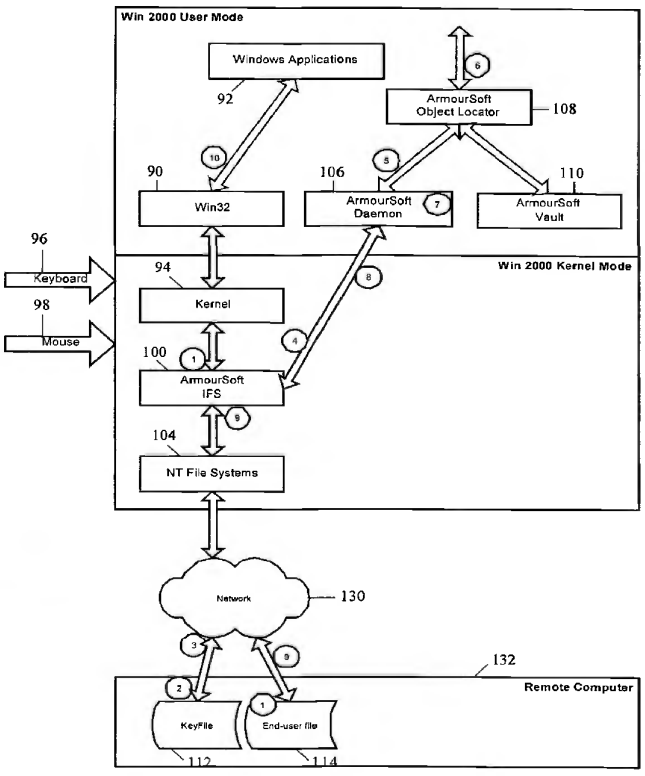
(75) Inventors/Applicants *(for US only)*: **CRITTEN, Richard** [GB/GB]; 2 Lime Grove, Bagworth, Coalville, Leicestershire LE67 1DT (GB). **CHARLESWORTH, James, Edward** [GB/GB]; 27 Cromarty Drive, Hinckley, Leicestershire LE10 0RX (GB). **LARTER, Andrew** [GB/GB]; 22 Stevenson Gardens, Cosby, Leicestershire LE9 1SN (GB). **GREEN, Peter** [GB/GB]; 14 Anderson Avenue, Rugby, Warwickshire CV22 5PE (GB). **DALE, Tracy, John** [GB/GB]; Woodale, Newton Road, Tollerton, York YO61 1QT (GB).

(74) Agent: **LLOYD, Patrick, Alexander, Desmond**; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: COMPUTER ENCRYPTION SYSTEMS



(57) Abstract: A system for encrypting computer files associates a key file with the encrypted file. Operations performed on the encrypted file are also performed on the key file. The key file includes a list of users to whom the encrypted file is available together with the public key certificates for those users. The symmetric key is held in the key file wrapped with the authorised user certificates.

WO 2004/001561 A2

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Computer Encryption Systems

This invention relates to computer encryption systems.

Computer encryption systems known in the art fall broadly into two categories: hard disk or partition-based systems, and file-based systems. Each type has associated advantages and disadvantages.

Hard disk-based systems have the advantage that the entire disk is guaranteed to be encrypted. Within the disk there can be no leaked clear files which may not have been encrypted. Furthermore, if the system partition is encrypted then the hard disk encryption system must obtain the key from the end user before the computer is able to boot.

Hard disk-based systems have the disadvantage that the encryption driver must be running on the computer before the operating system has loaded. Thus, the encryption driver cannot access operating system resources such as the GUI interface and hardware that needs operating system drivers. For the same reason external secure media such as smart cards cannot be accessed without the hard disk encryption system developer writing specific code to support the smart media and any other system device the smart media needs to be able to function.

A weakness in hard disk-based systems is that the protection key is only protected by the users' pass phrase. These cannot be stored on smart media and so are vulnerable to social engineering attacks. Hard disk encryption systems are also time consuming to install. As the whole disk has to be encrypted, the encryption process may take hours during which the computer cannot be used.

In file-based systems, only those files and folders that need encryption are encrypted. This reduces the time required for encryption and takes place after the operating system has loaded and the end user has been authenticated. As a result, any smart media, readers, and other hardware that are supported by the operating system can be used by

the encryption process. Moreover, there is no post installation encryption phase as required by the hard disk encryption method. New files may be encrypted automatically and existing clear files that require encryption can be encrypted either individually or in bulk.

File based systems have the disadvantage that there is always a potential leakage of unencrypted files. These may be temporary files the permanent versions of which will be encrypted. This problem can usually be avoided by a correct set up of the computer and encryption system.

It will be appreciated from the above discussion that both systems have advantages and disadvantages. However, neither permit end users to share access to their encrypted files without releasing the key used to encrypt the file. Neither can they allow users to grant encrypted access to files to other users without access to the other user's key.

In all areas of work, people work in groups and collaborate. They need to share files and data. To maintain security whilst allowing this type of access, a system must permit end-users to encrypt their files, allow their encrypted files to be accessed by others and work together on a group of encrypted files. Organisations maintaining and operating the computer systems need to be able to recover encrypted files when the end-user is no longer available, for example they have left the company.

The invention aims to address the problem with the prior art discussed above and to provide a system and method which can meet the requirements discussed.

Broadly, the invention uses a key file associated with a file to be encrypted. The key file holds the decryption key and all file handling, such as moving, copying etc. performed on the file to be encrypted is also performed on the key file. The key file may hold decryption keys for a number of users making multiple access possible.

More specifically there is provided a method for encrypting computer files comprising: encrypting at least one file within a folder; for each encrypted file, creating

an associated key file containing the decryption key, wherein the association between an encrypted file and its key file is such that any file handling operation performed on the encrypted file is also performed on the key file.

In one preferred embodiment, folders are marked to indicate that files within that folder are to be encrypted. Preferably a file is placed in the folder containing default encryption setting for files created in the folder.

Preferably, the associated key files are hidden from a user by a file system driver. The file system driver also ensures that when an operation is performed on a file, the same operation is performed on the key file. The file and the key file may have the same file name but different extensions.

In one preferred embodiment of the invention the key file contains decryption keys for a plurality of users. This allows an encrypted file to be made available to a plurality of users.

Preferably, the key file comprises a wrapped symmetric key for the associated encrypted file. The symmetric key may be wrapped by an end-user's public key.

Preferably, the default encryption settings include a list of end-users for which a file is to be encrypted.

Preferably, on receipt of a file encryption request, the file system driver reads the directory encryption settings file and retrieves the end-user list for which the file needs to be encrypted. The certificates for all the end-users on the list are located and the key file is created from the symmetric file encryption key wrapped end-user's by the public key for each end-user in the end-user list.

Where a file is to be encrypted in a directory that has not been marked for encryption, on receipt of a request to encrypt a file, the end-user may be asked for a list of end-users for whom the file is to be encrypted, the certificates for each end-user on the list are then retrieved, and a symmetric file encryption key generated. The file

encryption key is then wrapped with the certificate for each user, the wrapped encryption keys comprising the key file.

In this preferred embodiment, the step of encrypting the file may include saving the file in a temporary file to the name of the key file. The symmetric file key may then be requested and the original clear file read. The temporary encrypted temporary file may then be written and the clear file renamed to a further temporary file. The encrypted temporary file is then renamed to the original file name and the further temporary file deleted.

Embodiments of the invention may be used to encrypt files over a network. In that case, in one embodiment the directory encryption settings file is stored in a network folder and an encrypted network file is created at a local user computer and sent over the network in encrypted form.

In another case, the encrypted temporary file is stored in a network folder, and the further temporary file is stored at a local computer, whereby the clear file is not transmitted over the network.

The invention also provides a method of reading or writing a file encrypted according to the method defined above, comprising detecting the key file associated with the encrypted file, retrieving the decryption key from the key file, decrypting the file using the decryption key, and reading and/or writing the decrypted file.

Preferably, retrieving the decryption key comprises finding a private key, and using the private key to unwrap a wrapped key in the key file. Where the file has been encrypted for group access, the key file may include a list of users for whom the file is encrypted. Finding a private key then comprises finding a private key that corresponds to the list of users.

In one preferred embodiment, the key file is a network key file, the key file is opened at the local user's computer and the file is decrypted at the local computer after is has been read across the network. This has the advantage that

the file is always transported across the network in encrypted form so maintaining security.

The invention also provides a system for encrypting computer files comprising an installable file system driver transparent to the computer operating system for reading directory encryption settings and retrieving an end user list for which the file is to be encrypted, a daemon, a vault, the daemon operating to retrieve certificates stored in the vault, means for generating a symmetric encryption key, the key being sent by the daemon to the file system driver, the file system driver including means for creating a key file from the end-user certificates and the symmetrical encryption key and for associating the key file with the encrypted file.

Preferably, the system includes an object locator, wherein the object locator communicates between the vault and the daemon for retrieval of certificates. The vault may comprise a smart media and/or a soft vault on an end-user's computer.

A preferred embodiment of the invention comprises an operating system shell extension for retrieving certificates, generating the symmetric file encryption key and wrapping the symmetric key with the certificate of each user who has access to an encrypted file.

Embodiments of the invention use file or folder-based encryption. This means that the encryption within a computer system is selected. Such a system can use any smart media that is supported by the operating system. By allowing the computer to boot before accessing the smart-media, no manufacture specific interface need be written to access the smart media. This allows industry standard APIs to be used. Thus, the end user has the choice of any smart media supported by the operating system and can choose the smart media to be compatible with other applications required by the system.

This sort of flexibility would not be possible in a hard disk-based encryption system. In these systems, when

the computer boots, the encryption needs the decryption key before the operating system can be loaded. The device drivers needed to provide access to smart media or files on a card disk have not yet been loaded and so are not available to the encryption system. As a result, these systems must rely on pass phrase-based protection or can only support a limited number or range of smart media products.

The key files generated are not visible to the user and are associated with the encrypted files such that the two are always operated on together. The key files are small and so do not significantly affect the total file size or response times.

Whilst the advantages of the invention have been discussed in conjunction with smart media, end-users do not always want to use smart media to gain access to systems. For example, they may consider that the cost of smart media security is not justified in their environment. Embodiments of the present invention use a soft vault which is stored on the end-user computer. Preferably, this vault will have many of the characteristics of smart media. The file-based encryption system can use this vault instead of or in addition to smart media.

Embodiments of the invention will now be described, by way of example, and with reference to the accompanying drawings, in which:

Figure 1 shows how an embodiment of the invention may be integrated into a Microsoft Windows (RTM) operating system such as Windows 2000;

Figure 2 is a schematic diagram showing how an encrypted file is created in a folder marked for encryption;

Figure 3 is a schematic diagram showing how an encrypted file is created from an existing unencrypted File:

Figure 4 is a schematic diagram showing how an existing encrypted file can be read;

Figure 5 is a schematic diagram showing how an existing encrypted file can be written;

Figure 6 is a schematic diagram showing how a new encrypted file can be created across a network in a folder marked for encryption;

Figure 7 is a schematic diagram showing how a new encrypted file can be created across a network from an existing unencrypted File:

Figure 8 is a schematic diagram showing how an existing encrypted file can be read across a network; and

Figure 9 is a schematic diagram showing how an existing encrypted file can be written across a network.

The embodiments to be described use a file-based encryption system. This allows smart-media to be used in the system simply. End user files can be protected by a combination of the smart media and the PIN (Personal Identification Number) for the smart media. In practice, the PIN is not necessarily a number but, for example, a series of alphanumeric or other characters. A soft vault internal to the system may be used instead of the smart media in order to reduce costs.

The system to be described allows file sharing by different users. To achieve this using a single user encryption system, that is where the file is originally encrypted by a single user, the end-user files are first decrypted for the first user and then re-encrypted for the second user. End-user files must be clear, or unencrypted, to be shared and another copy made for the second, or each further, user. Such an approach makes collaboration difficult. The embodiment to be described allows simultaneous encryption of end-user files for multiple users without an increase in file size allowing authorised users to access the same files without copies having to be made for each user. Thus, efficient and secure multi-user and group encryption is achieved.

Embodiments to be described also permit encryption across a network. The encryption system sits above the operating file system drivers on the computer system and so has transparent access both to files on the local computer

and the network allowing files available on the network to be encrypted, shared by group encryption and have recovery encryption applied to them. The encryption and decryption take place on the computer local to the user. This means that files cross the network in encrypted form so there is no vulnerability to a clear file being intercepted on the network.

Embodiments of the present invention use an Installable File System (IFS) that acts as a low-level file driver. When handling encrypting files, it acts as a virtual file system handling all file operation transparently to the operating system, applications and users.

Figure 1 illustrates how the system may integrate into an operating system such as Windows 2000.

The manner in which files are encrypted will now be described.

Applications are provided which set a default file and folder encryption settings for the computer and for each folder. The computer default application stores default settings for encrypting new files and folders centrally on the computer. The stored information includes the identity of the user or users for which new folders or files should be encrypted. This information can be pre-loaded on the computer when it is first set up or by the end-user at some later time. This application accesses end-user certificates and presents a list of available users for selection. Once selected, the certificate identities are stored on the computer as the default encryption settings. These settings may be imported or exported to other computers allowing quick configuration.

The default encryption settings for the computer are stored in the computer's registry. The format of these settings is:

```
DefaultEncryptionSettings\{identity}
    EntityIdentifer={identity}
    Description={end-user description}
```

RecoveringKey={identity}

The above settings then repeated for each identity used for default encryption.

The application that sets the folder settings stores the folder settings on the end-user's computer. New files are then automatically encrypted. On set up of the default conditions for a folder, the user is presented with the default encryption settings for the computer. The end-user may modify this list to add or remove users by selecting their certificates. The settings may be propagated down a tree of folders.

Folders on an end-users computer system are not in themselves encrypted. Instead they are marked to indicate then any files created in them should be created encrypted. This marking is done by placing a file

ASEF_Dir_Default.dat

into the folder. The file is hidden from the end-user by the system driver. The file contains the default encryption setting for all new files created in the folder. The contents of the file are formatted as follows:

ASEF_Dir_Default.dat:	<SuniveralData_Header> <SDirectorySettingsFile_V1_HeaderInfo> <SUniversalData_V1_EncryptionInfo> <encrypting_entity_collection> <padding> <SUniversalData_V1_Checksum>
SUniversalData_Header:	<Identifier> <Version>`
SDirectorySettingsFile_V1_HeaderInfo:	<TotalFileLength>

SUniversalData_V1_EncrpytionInfo:	<EncryptionAlgorithm>
Encrpyting_entity_collection:	[<encrypting_entity>} <encrypting_entity_sentinal>
Encrypting_entity:	<SUniversalData_V1_EntityInfo> <SEncrpytedFile_V1_Entity_User>
SUniversal_V1_EntityInfo:	<Entity Type>
SEncrpytedFile_V1_Entity_User:	<UserIDLength> <UserNameLength> <KeyBlockLength> <UserID> <UserName> <KeyBlock>
Identifier:	<integer>
Version:	<integer>
TotalFileLength:	<long integer>
EntityType:	<integer>
UserIDLength:	<integer>
UserIDLength:	<integer>
KeyBlockLength:	<integer>
UserID:	[<byte>]
UserName	[<byte>]
Keyblock:	[<byte>]

A group-based encryption setting may be created by creating an identity for a group of users and providing this group with a private key for the group, as well as their own

key. This effects a simple, but powerful group encryption scheme. By ensuring that all files to which members of the group require access are included, in folders that include the group identity in the default settings, files in these folders will be encrypted for the group. Files are encrypted for all users in the folder's or computer's encryption settings.

When files are encrypted the decryption key for each user is stored in a companion file with a known but different file extension, for example if MyData.doc is encrypted then the key file MyData.as_enc is created to hold the wrapped encryption/decryption keys. The file system driver hides this file from the end-user.

If the end-user's file is moved, copied or renamed then the file system driver moves, copies or renames the file as appropriate. Thus, any file handling operation performed on the end-user's file is also performed on the associated key file.

The contents of the file are formatted as follows:

Key_file.as_enc	<SUniversalData_Header><SEncryptedFile_V1_HeaderInfo><SUniversalData_V1_EncryptionInfo><encrypting_entity_collection><padding><SUniversalData_V1_Checksum>
SUniversalData_Header	<Identifier><Version>
SEncryptedFile_V1_HeaderInfo	<TotalFileLength>
SUniversalData_V1_EncryptionInfo	<EncryptionAlgorithm>

encrypting_entity_collection	[<encrypting_entity>]<encrypting_entity_sentinal>
Encrypting_entity:	<SUniversalData_V1_EntityInfo><SEncryptedFile_V1_Entity_User>
SUniversalData_V1_EntityInfo:	<EntityType>
SEncryptedFile_V1_Entity_User:	<UserIDLength><UserNameLength><KeyBlockLength><UserID><UserName><KeyBlock>
Identifier:	<integer>
Version:	<integer>
TotalFileLength:	<long integer>
EntityType:	<integer>
UserIDLength:	<integer>
UserIDLength:	<integer>
KeyBlockLength:	<integer>
UserID:	[<byte>]
UserName	[<byte>]
KeyBlock:	[<byte>]

The file system driver creates this file whenever a file is created in a folder marked for encryption.

The KeyBlock is the wrapped symmetric key for the file. The symmetric key is wrapped by an end-users public key (contained in a certificate) and can only be decrypted by the user's private key. As public certificates are available to all end-users, any end-user may encrypt a file for any other end-user providing the first end-user can decrypt the file in the first place. Once the first end-user using their private key has managed to decrypt their wrapped key

they may wrap the symmetric file key for any other end-user and append a new encrypting_entity to the encryption file.

The group-based encryption may be used to implement a file recovery scheme. A recovery user identity (key pair and certificate) is created and this identity identifier is included on all a computer's default encryption settings. Any encrypted files created will automatically be encrypted for this recovery user. If access is required to files that have been encrypted, but for which the end-user's key is not available, the recovery key can be used in its place.

When a file is encrypted, a key file is created to hold the wrapped encryption/decryption keys for the file. This key file has the same name but a different extension from the end-user file. When the end-user file is moved, copies, deleted or renamed, the key file is moved, deleted or renamed as appropriate. The encryption system file system driver treats the two files as if they were one. The user is not aware of the second file containing the wrapped keys.

When a new file is created in an encrypted folder, the end-user needs to have certificates available for all end-user identities in the default setting for the folder. If these are all available, the new file is created using the keys from the end user certificates. If any certificates are missing, the user is prompted to retrieve them.

Having selected an existing file, the end-user may request that the file is encrypted. The default encryption settings for the folder are used or if the folder is not encrypted then the default settings for the computer are used. In both cases the end-user needs to have available the certificates for all the end-user identities contained in the default settings (folder or computer as appropriate). If all these certificates are available (which they normally would be) then the file is encrypted for the list of end-users. If any certificates are not presently available then the end-user is prompted to try to retrieve the missing certificates. This may be done in a variety of methods. If

the end-user still cannot provide all the required certificates the file may optionally still be encrypted.

Having selected an existing encrypted file the end-user may request for the file to be decrypted. To achieve this, the end-user must have available the private key corresponding to any of the identities used to encrypt the file. If one of these private keys is available the file is decrypted. If none of the corresponding private keys is available to the end-user, the end-user is prompted to retrieve one of the required keys. If one of the required private keys can be made available, the file is decrypted. If however none of the private keys can be obtained by the end-user then access is denied to the file and the file is not decrypted.

Third party applications (e.g. MS-Word) create, delete, read and write files. When performing these file operations on encrypted files or creating new files in encrypted folders the user is not aware that the encryption/decryption process is happening. The end-user is only required to intervene if the encryption system does not have all the required keys available. When the third party application tries the open an encrypted file, the file is decrypted as it is read from the disk and into memory. To achieve this, the end-user must have the private key corresponding to any of the identities used to encrypt the file. If one of these private keys is available then the file is decrypted as it is read into memory by the application. If none of the corresponding private keys is available to the end-user, the end-user is prompted to retrieve one of the required keys. If one of the required private keys can be made available, the file is decrypted as it is read into memory by the application, if however none of the private keys can be obtained by the end-user then access is denied to the file and the file is not decrypted. The third party application will usually present the end-user with an access denied message; obviously the details of the message depend upon

the application.

Once the file has been opened the application can continue to read from or write to the file without further intervention being required from the end-user.

By way of a further example, figures 2 to 9 describe some of the above-mentioned processes in greater detail.

Referring now to figure 2, the manner in which a new encrypted file is created in a folder marked for encryption will be described. Figure 2 shows Windows 2000 user mode with the WIN32 operating 90 system communicating with Windows applications 92 and with the kernel 94 in kernel mode. The system in kernel mode can accept external user inputs via a keyboard 96 and a mouse 98. These are, of course, only exemplary and other data inputs may be provided.

At 1, the file system driver embodying the invention 100 receives a >create= request for the end-user file. The request asks for an encrypted file to be created. At 2, the file system driver 100 reads the directory encryption settings 102 via the Windows NT File Systems 104 and retrieves the list of end users for which the file needs to be encrypted. At 3, the IFS driver 100 transmits this list of users to a daemon 106 which, at step 4 uses the system object locator 108 to try and find all the certificates for the end users on the list from the system vault 110. The daemon is a process running in the background that performs operations in response to certain events. If any certificates are missing, at step 5, the object locator 108 prompts the user to find any certificates that the object locator has not been able to retrieve.

Once all the certificates are present, the daemon 106 generates the symmetric file encryption key at step 6. At step 7, the daemon wraps the file encryption key for each user in the user list using the corresponding certificate which provides the public key. At step 8, the daemon 106

returns the file encryption key with the list of users with the wrapped keys attached to the file system driver 100. The driver 100 then at step 9 uses the user list and the wrapped keys to create a key file 112 for the end-user file being created. Following this the end user file 114 is created at step 10 and at step 11 any data written to the end user file 114 is encrypted with the file encryption key.

Figure 3 is a similar diagram to figure 2 showing how a new encrypted file can be created from an existing unencrypted file.

Initially, the user selects, at step 1, the file to be encrypted. This may be done, for example, via Windows Explorer 116. At step 2, a system shell extension 118 prompts the end user to choose the end-users for which the file is to be encrypted. It is important to understand that the file may be encrypted for a single user or a group of users.

At step 3, the shell extension retrieves certificates for the users chosen by the end user. If the certificates cannot be retrieved, the shell extension prompts the user to provide them. At step 4, the shell extension then generates the symmetric file encryption key, which it wraps at step 5, for each selected end-user. The shell extension then writes at step 6, the key file to the system disk with a temporary name (T_1) 120. At step 7 the file originally selected in Windows Explorer 116 is copied to the temporary file name T_1 which causes the file system driver 100 to encrypt the file to create an encrypted file (T_1) 122. The original clear file 124 is then by the file system driver 100 at step 8. The driver 100 sees that the destination file is encrypted and requests, at step 9, the symmetric file key from the daemon 106. The daemon retrieves the file key from the shell extension 118 and, at step 11, returns the key to the file system driver 100. The driver 100 can then read the original clear file and writes the new encrypted temporary file T_1. At step 13, the original clear file is renamed to a new

temporary file T_2 by the shell extension 118 and at step 14 the encrypted file is renamed by the shell extension. The user now has the original file encrypted saved as T_1 which is then saved back to its original name at step 15. When this is successfully completed, the second temporary file, T_2, is deleted leaving the user with just the original file encrypted.

Figure 4 shows how an existing encrypted file may be read. The file system driver 100 receives a request from the user to open a file, for example by a combination of the mouse 98, and a Windows application 92. The file system driver 100 detects that a key file exists for the file that has been requested and therefore that the file is encrypted (step 2). The file system drive opens the key file and retrieves and reads the list of users contained within it at step 3 and, at step 4, passes the retrieved user list together with the wrapped keys contained in the key file to the daemon 106. The daemon at step 5 searches for a private key that corresponds to the user list received from the file system driver. This search is conducted via the object locator 108 and the vault 110. At step 6, if the private key is not found by the daemon, a prompt is sent to the user to provide a private key. When the private key has been found, at step 7, the daemon unwraps the wrapped key corresponding to the retrieved private key. The step 8 this unwrapped key is returned to the file system driver 100 which, at step 9, uses the unwrapped key to decrypt the encrypted file 124 and return a clear file to the application via the kernel 94 at step 10.

The routine shown in figure 5 writes to an existing encrypted file. The routine is identical to steps 1 to 9 of the encrypted file routine described above with respect to figure 4 above. Once the unwrapped key has been used to decrypt the file at step 9, the application can write clear data to the file. This is then encrypted by the file system drive 100 and encrypted data can be written to the file.

The routines shown in figures 6 to 9 correspond to figures 2 to 5 where files are encrypted or decrypted across a network. In the example of figure 6 a new encrypted file is created at a remote computer 132 across a network 130 in a folder marked for encryption. At step 1, the file system driver 100 at a local computer receives a create request for the end-user file to be created over the network on another computer, shown in the figure as the remote computer 132. The end-user file is shown as file 114 at the remote computer 132. The file system driver 100 on the local computer at step 2 reads the directory encryption settings file 102 from the network folder and retrieves the list of end-users for which the network file needs to be encrypted. At step 3, the file system driver 100 on the local computer sends this user list to the daemon 106 on the local computer. The daemon, at step 4, uses the object locator 108 and the vault 110 to retrieve the certificates for the users on the user list. If those certificates are not all received, the user, at step 5, is prompted for the missing certificates. The daemon at step 6 then generates the symmetric file encryption key and at step 7 wraps the file encryption key for each user in the user list using the corresponding certificate, that is the public key. At step 8, the file encryption key and the user list, together with the wrapped keys is sent back from the daemon 106 on the local computer to the local computer file system driver 100. The driver 100 then creates the key file 112 from the user list and the wrapped keys in the network folder for the end-user remote file being created. The local system driver then creates the end-user network file 114 over the network. Data now written to the network file is encrypted with the file encryption key by the local file system driver. All data sent over the network is encrypted.

Figure 7 is a network version of figure 3 where a new encrypted file is created at the remote computer from an existing, clear, file residing on that remote computer. The

end-user at the local computer selects a file to be encrypted, for example via Windows Explorer 116 at step 1. At step 2, the shell extension 118 at the local computer prompts the user to choose the end-users for whom the file is to be encrypted. At step 3, the shell extension 118 retrieves certificates for the selected users, using the object locator 108 and the vault 110. If they cannot be found, the local computer user is prompted to provide the certificates. At step 4, the shell extension generates the symmetric file extension key and at step 5, the local computer shell extension wraps the file encryption key for each selected end user.

At step 6, the shell extensions 118 on the local computer writes the key file 120 to the network folder with a temporary name T_1. At step 7, the shell extension 118 copies the end-user network file originally selected by the user to the temporary file name T_1 in the network folder. The new network file T_1 is then encrypted by the local computer file system driver. The clear original network file is then read at step 8 by the file system driver which, at step 9, sees that the destination network file is encrypted and requests the symmetric file key from the local daemon 106. At step 10, the local computer daemon retrieves the file key from the local shell extension 118 and at step 9 passes the key to the local computer file system driver 100. At step 12, the file system driver 100 on the local computer reads the original clear network file and writes the new encrypted temporary network file T_1. At step 13, when the file is completely written, the original clear network file is renamed to a new temporary network file T_2. The shell extension 118 on the local computer renames the encrypted network file T_1, back to the original network file name at step 14. Once this has been completed, at step 15, the second temporary network file (the clear file) is deleted and at step 16 the end user is left with the original network file encrypted.

Figure 8 shows how an existing encrypted file may be read across a network. At step 1 the local computer file system driver receives a request to open a network file. The file system driver 100 at step 2 detects that there is a network key file for the file to be opened, and that, therefore, the file is encrypted. The file system driver opens the network key file 112 at step 3 and reads the list of users over the network. This list is passed by the file system driver 100 at step 4 to the local system daemon 106 together with the wrapped keys. At step 5 the local daemon tries to find a private key that corresponds to the list of users passed to it by the local file system driver. At step 6, the end user is prompted, on the local computer for a private key if no private key can be found. At step 7, when a private key has been found, the local computer daemon unwraps the wrapped symmetric key that corresponds to the private key retrieved and at step 8 this unwrapped key is returned to the local computer file system driver. At step 9, the file system driver uses the unwrapped key to decrypt the file after it has been read across the network. Clear data can then be returned to the application on the local computer.

Figure 9 shows how to write an existing encrypted file across a network. Steps 1 to 8 are identical to the read process of figure 14 above. At step 9, the local computer file system driver uses the unwrapped key to encrypt the data being sent to the file before it is transmitted across the network and at step 10 the local application writes clear data to the file. The local computer encrypts that data and sends encrypted data over the network.

CLAIMS

1. A method for encrypting computer files comprising:

encrypting at least one file within a folder;

for each encrypted file, creating an associated key file containing the decryption key,

wherein the association between an encrypted file and its key file is such that any file handling operating performed on the encrypted file is also performed on the key file.

2. A method according to claim 1, comprising marking folders to indicate that files within that folder are to be encrypted.

3. A method according to claim 2, wherein marking a folder comprising placing a file in the folder containing default encryption setting for files created in the folder.

4. A method according to claim 1, 2 or 3, wherein the associated key files are hidden from a user by a file system driver.

5. A method according to claim 4, wherein when an operation is performed on an encrypted file, the file system driver performs the same operations on the key file.

6. A method according to any preceding claim, wherein the key file contains decryption keys for a plurality of users.

7. A method according to any preceding claim, wherein the key file has the same file name as the encrypted file and a different extension.

8. A method according to any preceding claim, wherein the key file comprises a wrapped symmetric key for the associated encrypted file.

9. A method according to claim 8, wherein the symmetric key is wrapped by an end-user=s public key.

10. A method according to claim 3, wherein the default encryption settings includes a list of end-users for which a file is to be encrypted.

11. A method according to claim 10, comprising, on receipt of an encryption create request, the file system driver reads the directory encryption settings file and retrieves the end-user list for which the file needs to be encrypted.

12. A method according to claim 11, wherein the certificates for all the end-users on the list are located.

13. A method according to claims 9 and 12 wherein the key file is created from the symmetric file encryption key is wrapped by the end-user's public key for each end-user in the end-user list.

14. A method according to claim 1, comprising, on receipt of a request to encrypt a file, requesting from the end-user a list of end-users for whom the file is to be encrypted, retrieving the certificates for each end-user on the list, generating a symmetric file encryption key, and wrapping the file encryption key with the certificate for each user, the wrapped encryption keys comprising the key file.

15. A method according to claim 14, wherein encrypting the file comprises saving the file in a temporary file to the name of the key file.

16. A method according to claim 15, comprising requesting the symmetric file key, reading the original clear file, writing the encrypted temporary file, renaming the clear file to a further temporary file, renaming the encrypted temporary file to the original file name and deleting the further temporary file.

17. A method according to claim 3, wherein the directory encryption settings file is stored in a network folder and the file is a network file and wherein encrypted network file is created at a local user computer and sent over the network in encrypted form.

18. A method according to claim 15, wherein the encrypted temporary file is stored in a network folder, and the further temporary file is stored at a local computer, whereby the clear file is not transmitted over the network.

19. A method of decrypting a file encrypted according to the method of any of claims 1 to 18, comprising opening the key file and retrieving the decryption key, retrieving a certificate corresponding to the decryption key, and decrypting the file.

20. A method according to claim 19, wherein the key file comprises a list of users and wrapped keys, and wherein the step of retrieving the list of users from the key file, together with the wrapped keys, retrieving a private key corresponding to the user list, unwrapping the wrapped keys using the private key and using the unwrapped keys to decrypt the file.

21. A method of reading or writing a file encrypted according to the method of any of claims 1 to 20, comprising detecting the key file associated with the encrypted file, retrieving the decryption key from the key file, decrypting the file using the decryption key, and reading and/or writing the decrypted file.

22. A method according to claim 21, wherein retrieving the decryption key comprises finding a private key, and using the private key to unwrap a wrapped key in the key file.

23. A method according to claim 22, wherein the key file includes a list of users for whom the file is encrypted, and finding a private key comprises finding a private key that corresponds to the list of users.

24. A method according to any of claims 21, 22 or 23, wherein the key file is a network key file, the key file is opened at the local user=s computer and the

file is decrypted at the local computer after is has been read across the network.

25. A computer program for encryption and/or decryption of computer files comprising computer code, which when run on a computer or a computer network, performs the steps of any of claims 1 to 24.

26. A computer program for encryption and/or decryption of computer files comprising a program storage medium having recorded thereon computer code, which when run on a computer or a computer network, performs the steps of any of claims 1 to 24.

27. A system for encrypting computer files comprising an installable file system driver transparent to the computer operating system for reading directory encryption settings and retrieving an end user list for which the file is to be encrypted, a daemon, a vault, the daemon operating to retrieve certificates stored in the vault, means for generating a symmetric encryption key, the key being sent by the daemon to the file system driver, the file system driver including means for creating a key file from the end-user certificates and the symmetrical encryption key and for associating the key file with the encrypted file.

28. A system according to claim 27, comprising an object locator, wherein the object locator communicates between the vault and the daemon for retrieval of certificates.

29. A system according to claim 27 or 28, wherein the vault comprises a smart media.

30. A system according to claim 27, 28 or 29 , wherein the vault comprises a soft vault on an end-user=s computer.

31. A system according to any of claims 27 to 30, comprising an operating system shell extension for retrieving certificates, generating the symmetric file encryption key and wrapping the symmetric key with the certificate of each user who has access to an encrypted file.

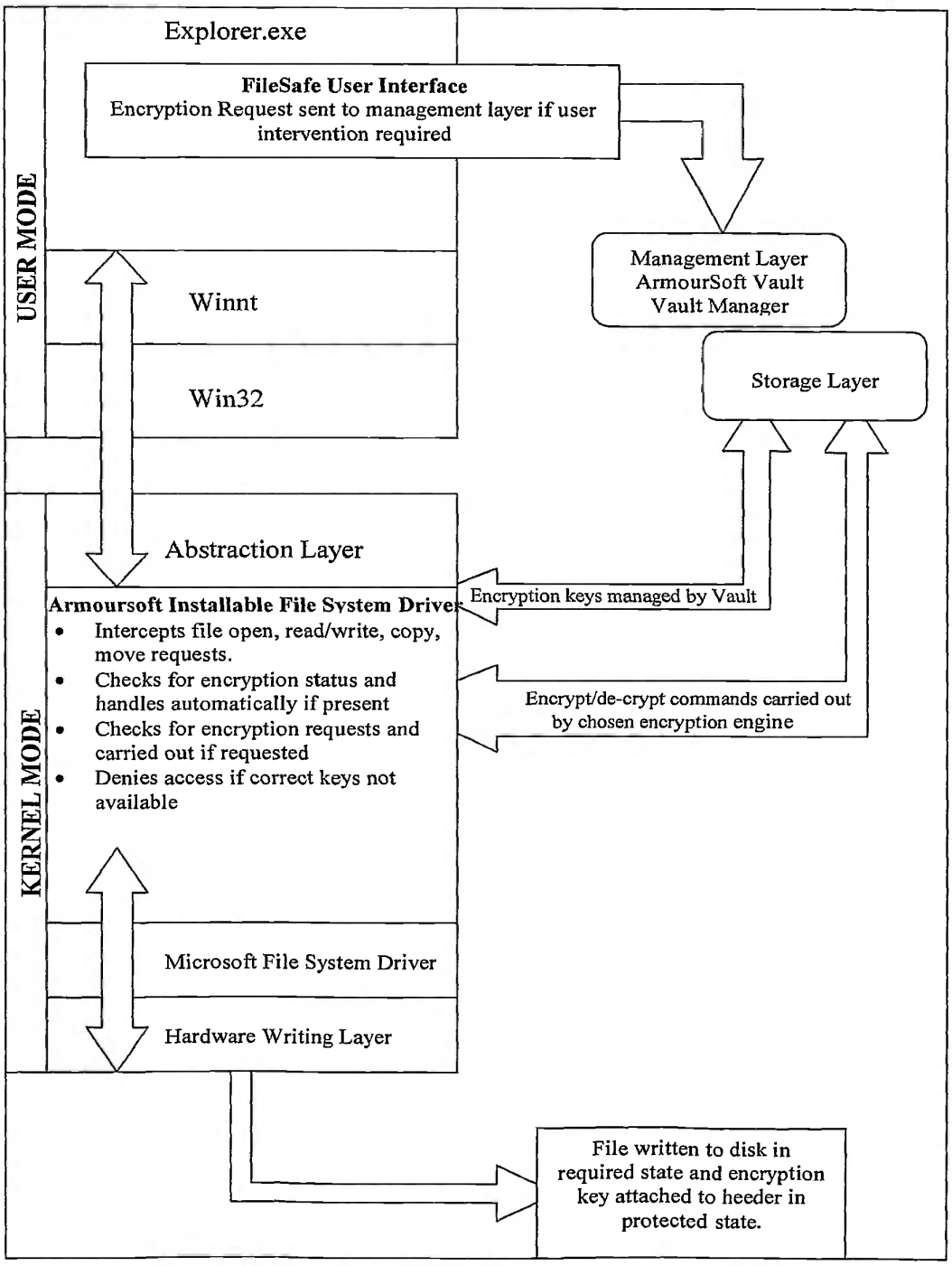

Explorer.exe
FileSafe User Interface
Encryption Request sent to management layer if user intervention required
USER MODE
Winnt
Win32
Management Layer
ArmourSoft Vault
Vault Manager
Storage Layer
Abstraction Layer
Encryption keys managed by Vault
Armoursoft Installable File System Driver
Intercepts file open, read/write, copy, move requests.
Checks for encryption status and handles automatically if present
Checks for encryption requests and carried out if requested
Denies access if correct keys not available
Encrypt/de-crypt commands carried out by chosen encryption engine
KERNEL MODE
Microsoft File System Driver
Hardware Writing Layer
File written to disk in required state and encryption key attached to heeder in protected state.

Figure 1

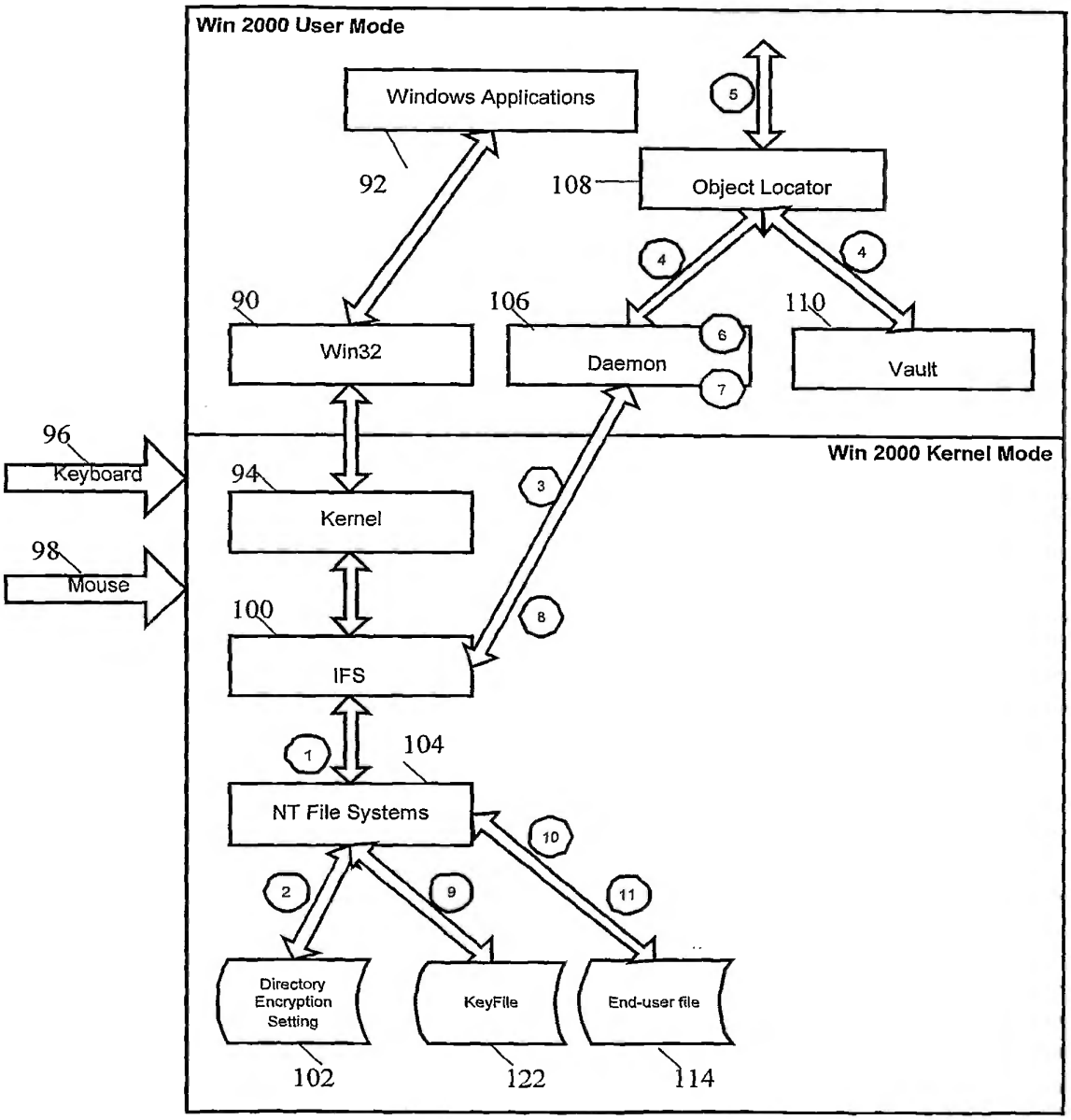

Win 2000 User Mode
Windows Applications
92
108
Object Locator
5
4
4
90
106
110
Win32
Daemon
6
7
Vault
96
Keyboard
Win 2000 Kernel Mode
94
Kernel
3
98
Mouse
100
8
IFS
1
104
NT File Systems
10
2
9
11
Directory Encryption Setting
KeyFile
End-user file
102
122
114

Figure 2

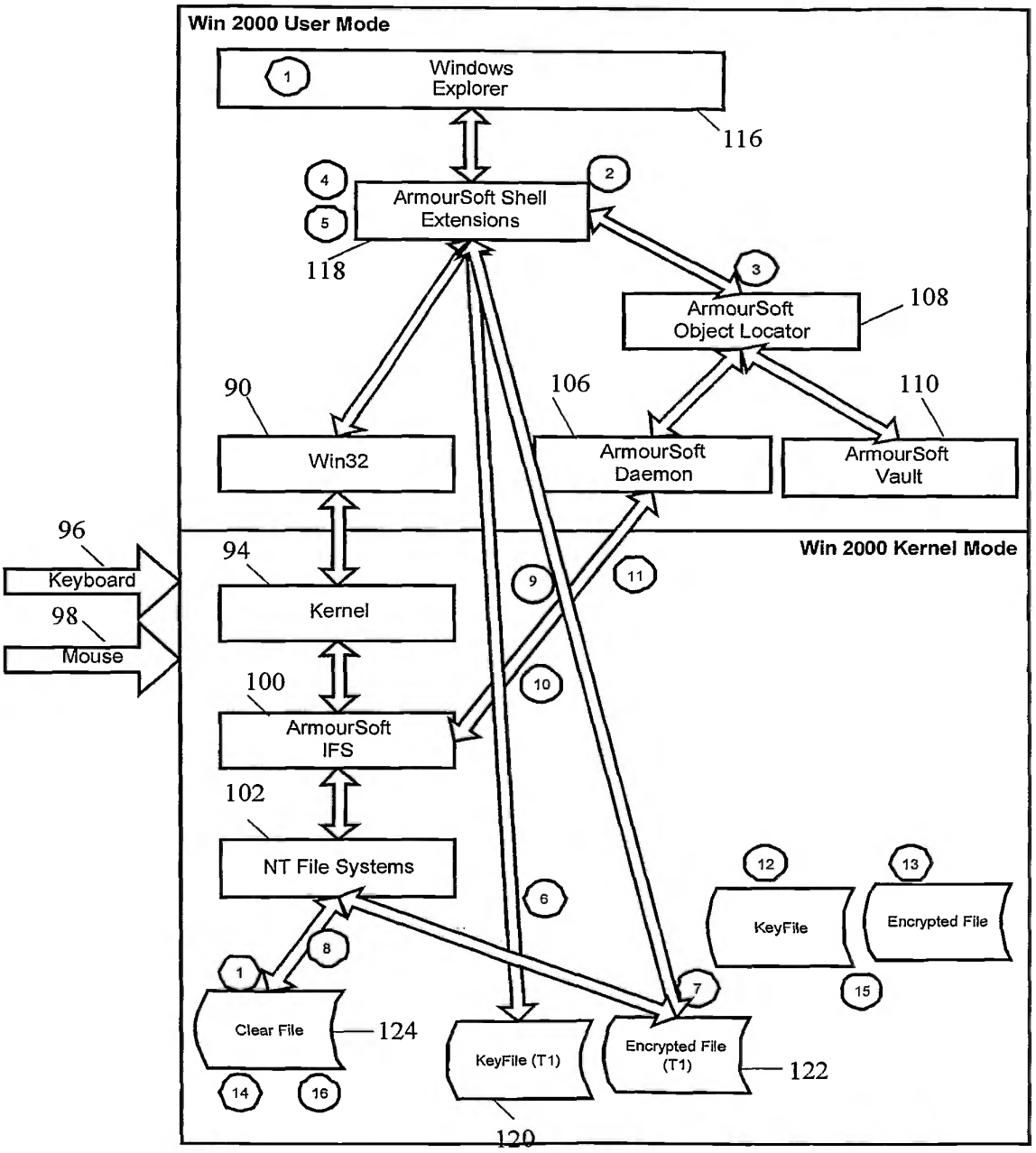

Win 2000 User Mode
Windows Explorer
1
116
ArmourSoft Shell Extensions
2
3
4
5
118
ArmourSoft Object Locator
108
90
106
110
Win32
ArmourSoft Daemon
ArmourSoft Vault
96
Keyboard
98
Mouse
94
Win 2000 Kernel Mode
Kernel
9
11
100
10
ArmourSoft IFS
102
NT File Systems
6
12
13
KeyFile
Encrypted File
15
8
1
7
Clear File
124
KeyFile (T1)
Encrypted File (T1)
122
14
16
120

Figure 3

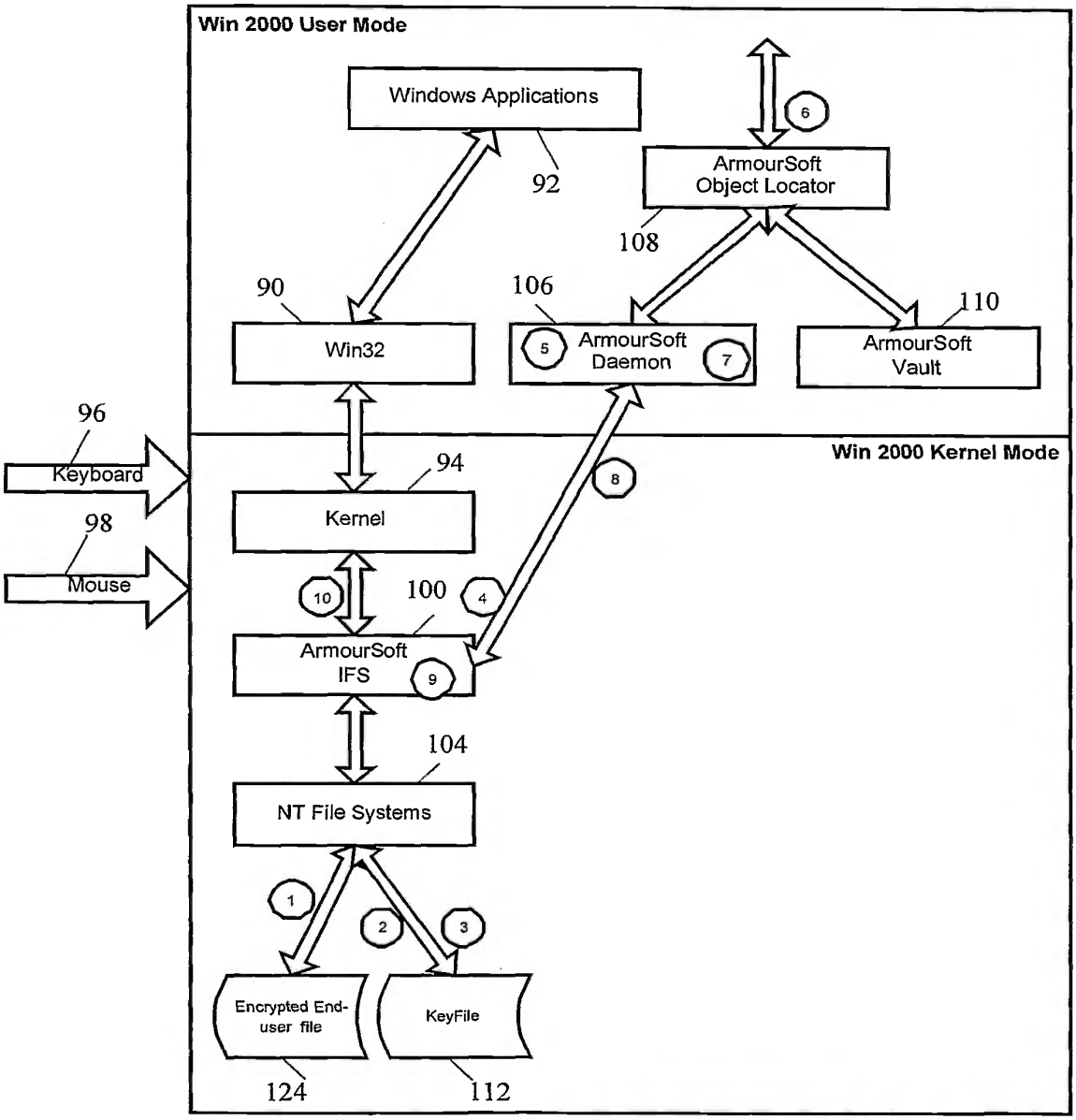

Win 2000 User Mode
Windows Applications
92
6
ArmourSoft
Object Locator
108
90
106
110
Win32
5
ArmourSoft
Daemon
7
ArmourSoft
Vault
96
Keyboard
98
Mouse
Win 2000 Kernel Mode
94
Kernel
8
10
100
4
ArmourSoft
IFS
9
104
NT File Systems
1
2
3
Encrypted End-
user file
KeyFile
124
112

Figure 4

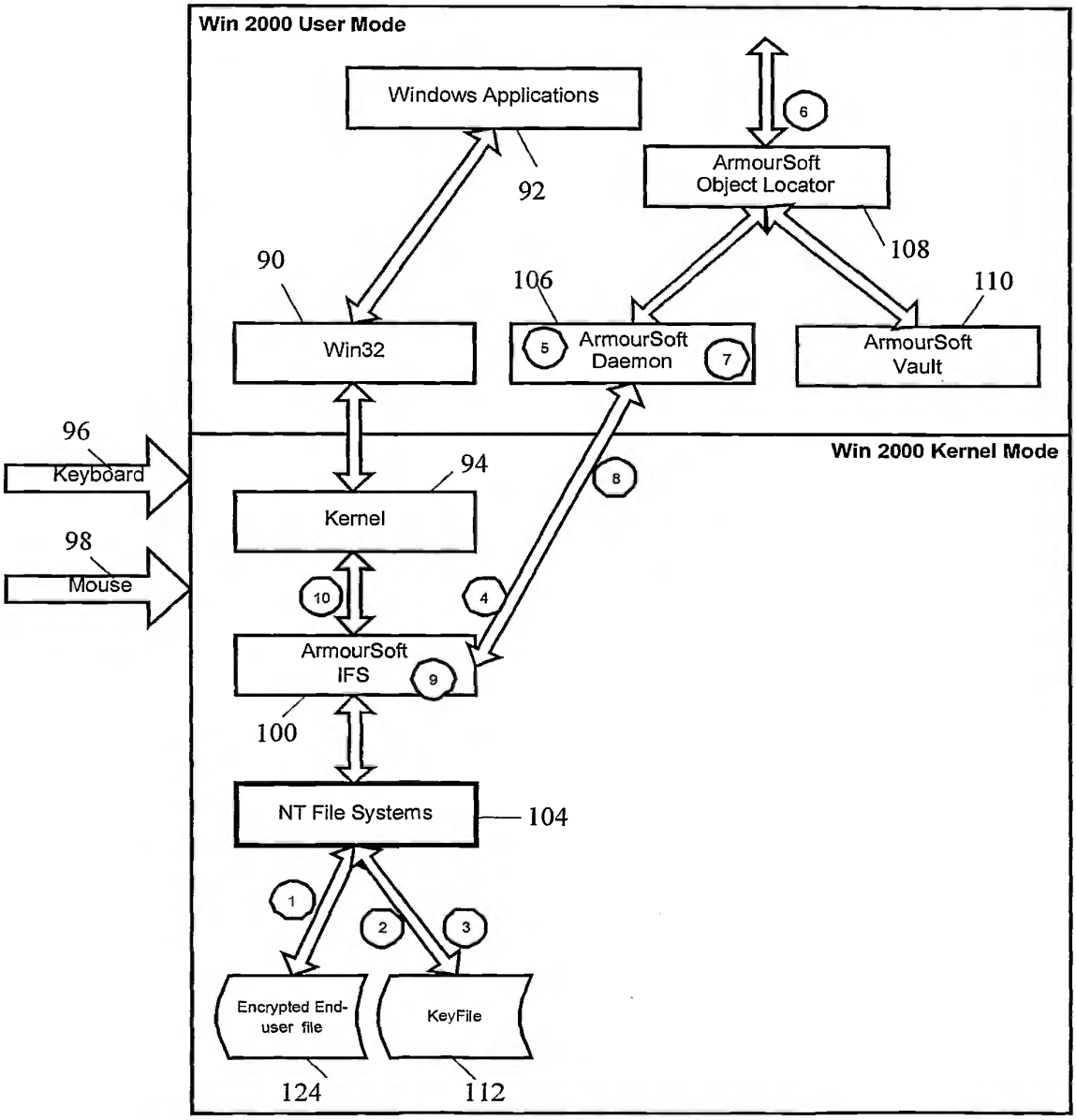

Win 2000 User Mode
Windows Applications
92
6
ArmourSoft
Object Locator
108
90
106
110
Win32
5
ArmourSoft
Daemon
7
ArmourSoft
Vault
96
Keyboard
Win 2000 Kernel Mode
94
8
Kernel
98
Mouse
10
4
ArmourSoft
IFS
9
100
NT File Systems
104
1
2
3
Encrypted End-
user file
KeyFile
124
112

Figure 5

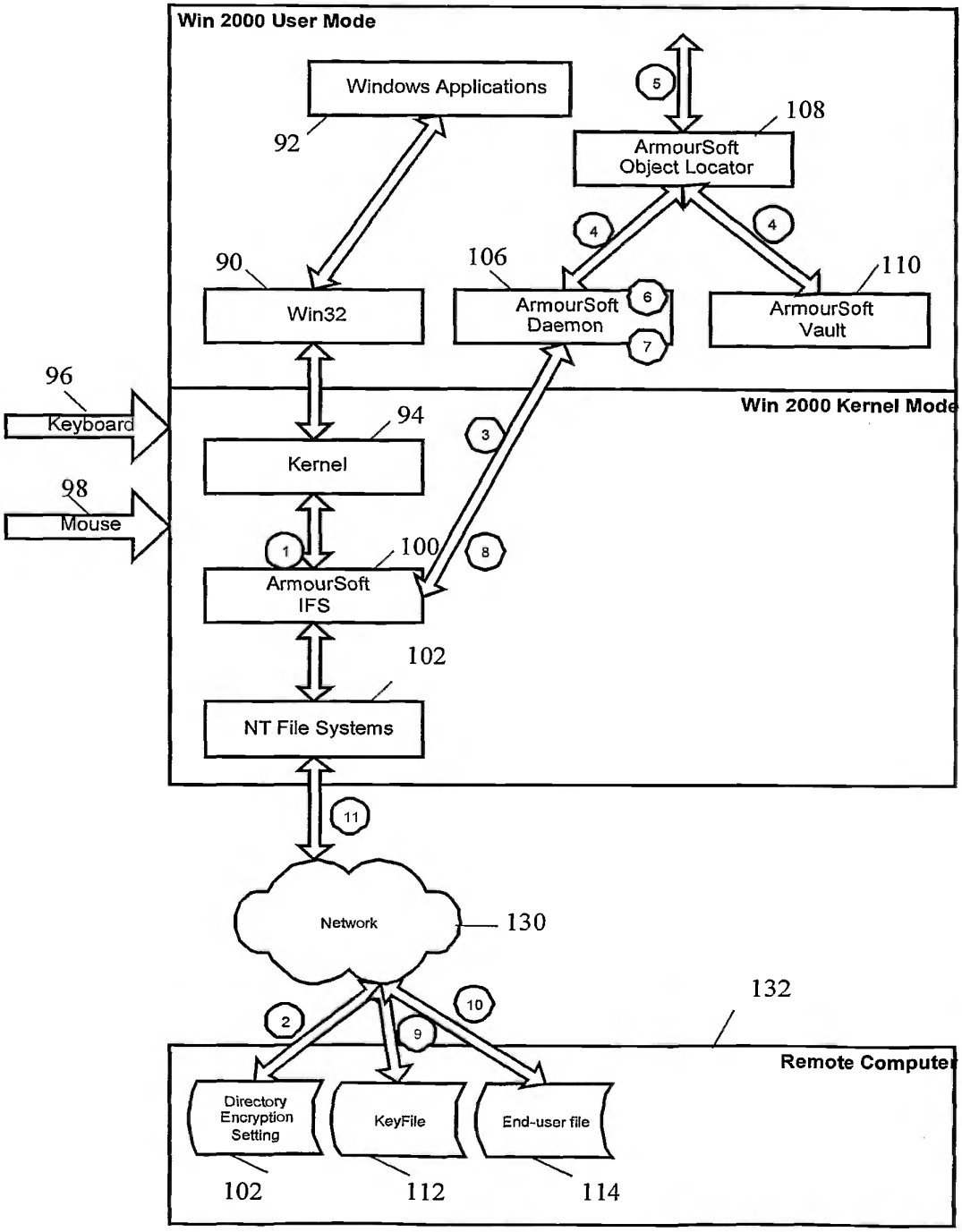

Win 2000 User Mode
Windows Applications
92
5
108
ArmourSoft Object Locator
4
4
90
106
110
Win32
ArmourSoft Daemon
6
7
ArmourSoft Vault
96
Keyboard
Win 2000 Kernel Mode
94
3
Kernel
98
Mouse
1
100
8
ArmourSoft IFS
102
NT File Systems
11
Network
130
132
2
9
10
Remote Computer
Directory Encryption Setting
KeyFile
End-user file
102
112
114

Figure 6

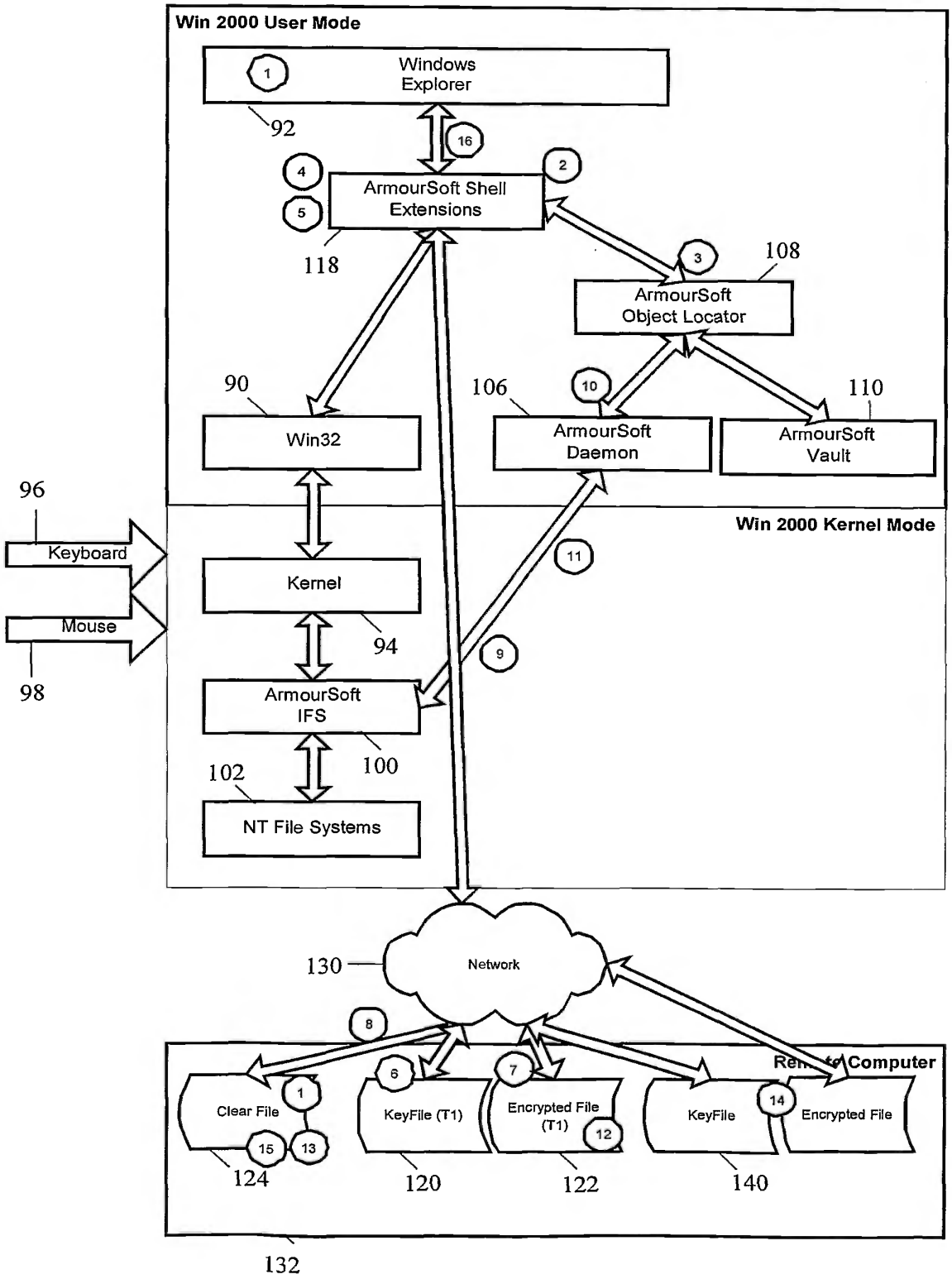

Win 2000 User Mode
Windows Explorer
1
92
16
4
5
ArmourSoft Shell Extensions
2
118
3
108
ArmourSoft Object Locator
90
Win32
106
10
110
ArmourSoft Daemon
ArmourSoft Vault
96
Keyboard
Mouse
98
Win 2000 Kernel Mode
Kernel
94
11
9
ArmourSoft IFS
100
102
NT File Systems
130
Network
8
Remote Computer
Clear File
1
15
13
124
6
KeyFile (T1)
120
7
Encrypted File (T1)
12
122
KeyFile
14
Encrypted File
140
132

Figure 7

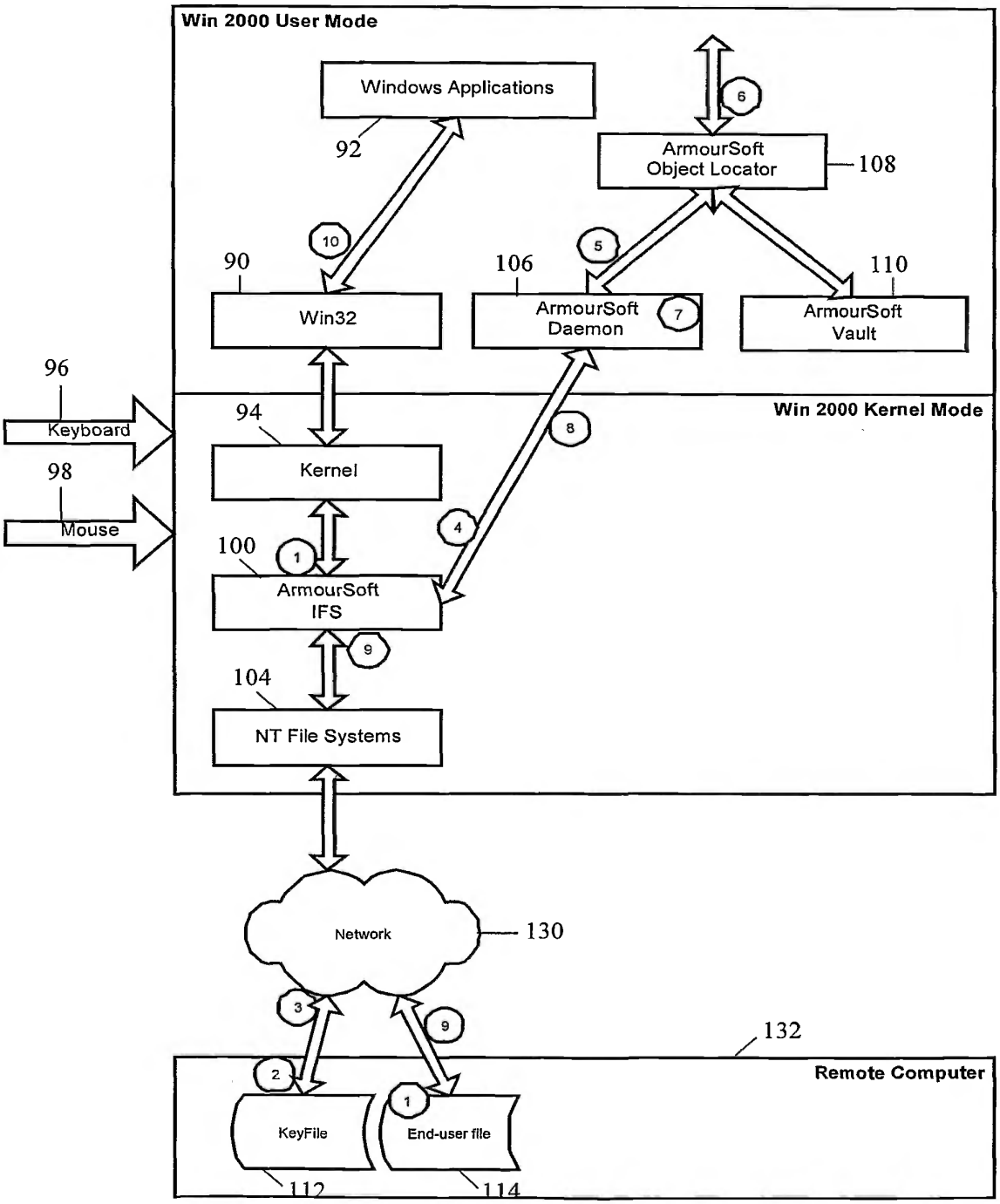

Win 2000 User Mode
Windows Applications
92
6
ArmourSoft
Object Locator
108
10
90
106
5
110
Win32
ArmourSoft
Daemon
7
ArmourSoft
Vault
96
Keyboard
94
Win 2000 Kernel Mode
8
Kernel
98
Mouse
4
100
1
ArmourSoft
IFS
9
104
NT File Systems
Network
130
3
9
132
2
Remote Computer
1
KeyFile
End-user file
112
114

Figure 8

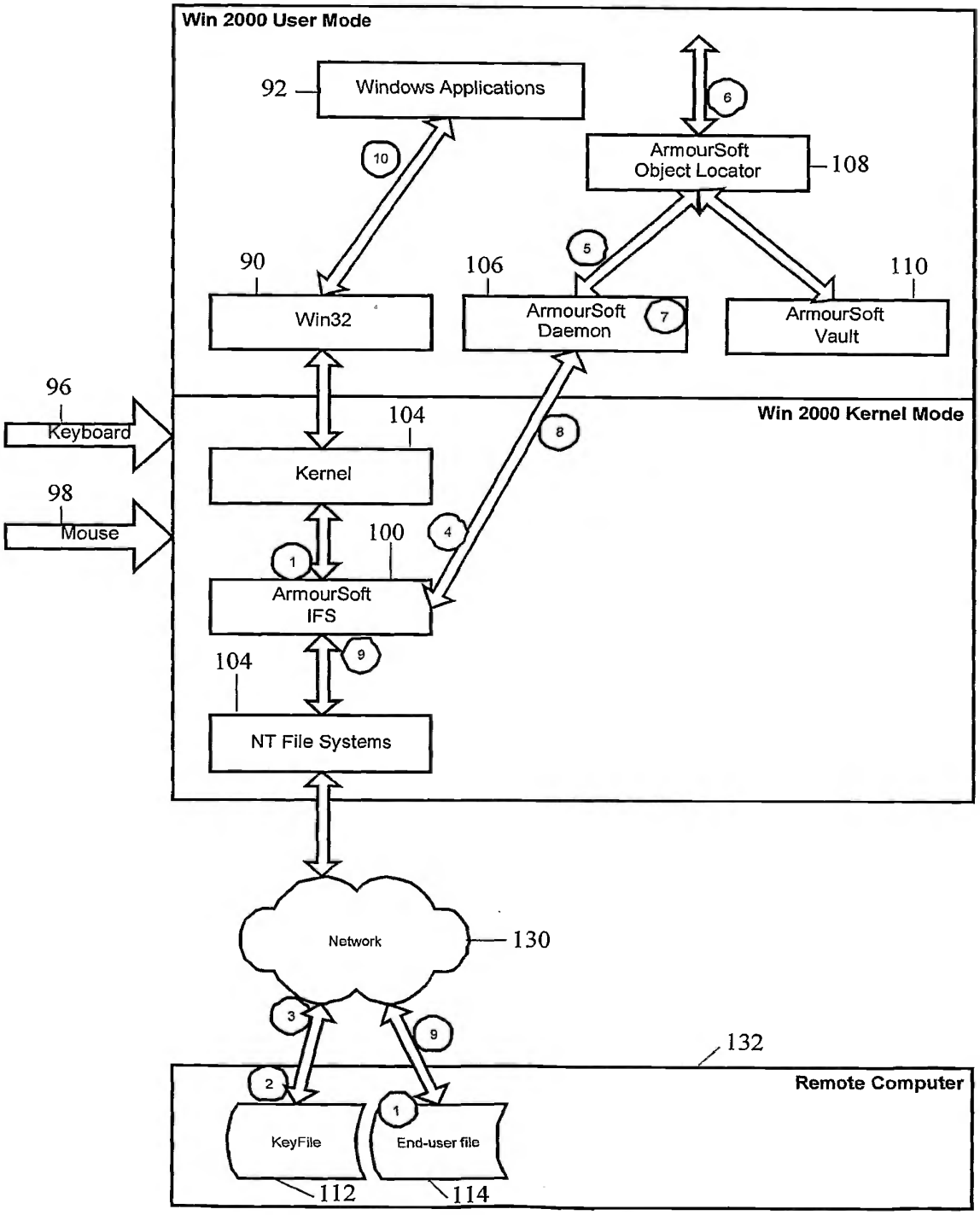

Win 2000 User Mode
92
Windows Applications
6
10
ArmourSoft
Object Locator
108
90
106
110
5
Win32
ArmourSoft
Daemon
7
ArmourSoft
Vault
96
Keyboard
104
Win 2000 Kernel Mode
8
Kernel
98
Mouse
100
4
1
ArmourSoft
IFS
9
104
NT File Systems
Network
130
3
9
132
2
Remote Computer
1
KeyFile
End-user file
112
114

Figure 9

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/371,363
				Filing Date	February 10, 2012
				First Named Inventor	Rick L. Orsini
				Art Unit	2492
(Use as many sheets as necessary)				Examiner Name	M. W. Chao
Sheet	1	of	1	Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/M.C./		WO-2004001561-A2	12-31-2003	Armoursoft Ltd		

Examiner Signature	/Michael Chao/	Date Considered	04/17/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-6,473,858	10-29-2002	Shimomura et al.	
/M.C./		US-7,206,250	04-17-2007	Groux	
/M.C./		US-20050289218	12-29-2005	Rothman et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	04/09/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

49325380_1

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-8,041,875	10-18-2011	Shah et al.	
/M.C./		US-8,095,800	01-10-2012	Creary et al.	
/M.C./		US-8,578,076	11-05-2013	van der Linden et al.	
/M.C./		US-7,213,158	05-01-2007	Bantz et al.	
/M.C./		US-6,807,649	10-19-2004	Murthy	
/M.C./		US-2003/0188153-A1	10-02-2003	Demoff et al.	
/M.C./		US-2003/0055905-A1	03-20-2003	Nishiyama et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	04/09/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

47607385_1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 04/22/2015

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
04/22/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/371,363	**Applicant(s)** ORSINI ET AL.	
	Examiner Michael Chao	**Art Unit** 2492	**AIA (First Inventor to File) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 06 April 2015 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *5* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.
   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☒ Applicant's reply has overcome the following rejection(s): Wells in view of Burkhard.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
13. ☒ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). See Continuation Shee
14. ☐ Other: _____.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
    Claim(s) allowed: .
    Claim(s) objected to: .
    Claim(s) rejected: 1-27.
    Claim(s) withdrawn from consideration: .

/Michael Chao/
Primary Examiner, Art Unit 2492

Continuation of 12. does NOT place the application in condition for allowance because:

Applicant's argument, first presented during the in person interview on 3/18/2015, is ostensibly that modifying Shamir's Secret Sharing algorithm, as used in the SSMS reference ("Secret Sharing Made Short" by Krawczyk et al.), with any of the error correcting/erasure coding methods of Wiencko et al., Buckhard et al. or Xu would change the principle of operation of Shamir's Secret Sharing. This is because if you have less than a threshold number of shares in a secret sharing scheme you cannot recover any information on the secret (see SSMS § 2 1); however, Wiencko/Buckhard/Xu are based on error correcting/erasure coding methods that do not obfuscate the base data and thereby yield information with less than a threshold number of shares. As phrased by Applicant's characterization of Shamir's secret sharing discussed in SSMS on p. 2 of the response on 4/6/2015:

"m-1 shares give no (computational) information on the secret . . .

- The resultant solution is strikingly simple. It just combines in a natural way traditional secret sharing schemes, with encryption and information dispersal techniques."

Examiner agrees with Applicant's premise that modifying a Shamir's Secret Sharing scheme with the error correcting/erasure coding methods of Wiencko/Buckhard/Xu would change the principle of operation of Shamir's Secret Sharing. But, the Examiner cannot agree that the combination of SSMS (in view of DSFID) and Wiencko/Buckhard/Xu is non-obvious due to the above reasons because the combination as stated in the office action on 11/26/2014, specifically: p. 12 ll. 3-12, p. 14 l. 7, p. 15 l. 1, p. 15 l. 13 (and on 5/01/2014 p. 20 l. 2), did not modify Shamir's Secret Sharing.

As reproduced above, SSMS uses traditional secret sharing schemes, with encryption and information dispersal techniques. It was the information dispersal technique (IDS) that was modified by Wiencko/Buckhard/Xu. Thus, any principle of operation argument would necessarily be premised on changing the principle of operation of the IDS scheme discussed in SSMS. However, if we apply Applicant's argument that the secrecy is not maintained by modifying the SSMS' IDS with Wiencko/Buckhard/Xu (as opposed to SSMS' Shamir's secret sharing) the argument fails as Krawczyk explicitly disclaims the need for secrecy by stating:

"(this is essential in Shamir's scheme to provide perfect secrecy but not for information dispersal where secrecy is not a concern)" Krawczyk p. 141 1.

Note additionally that had the Examiner modified Shamir's Secret Sharing of SSMS then the combination would fail to disclose claim 6 which requires Shamir's Secret Sharing.

As a further comment on the obviousness of the combination, Krawczyk discloses in SSMS § 3 2 that: "Information dispersal schemes can be implemented in a variety of ways, all corresponding to the notion of erasure codes in the theory of error correcting codes (see [15, 13, 91). We note that basic information dispersal schemes do not deal with malicious parties or with secrecy of information."

Where all of Wiencko/Buckhard/Xu are directed to erasure codes (Xu § 2.1) or error correcting codes (Wiencko col. 19 ll. 35-42; Burkhard Abstract; Xu § 3). Thus the references themselves suggest combination.

As to the argument directed toward § 3.2 of the Wells reference (Oceanstore) on p. 4 submitted 4/06/2015. Having notice of the argument and time to review the Wells reference, § 3.2 is titled "A Case for Erasure Codes" where the remaining section generally states that RAID systems are less appropriate than a system based on erasure codes because they "do[] not provide the robustness necessary to survive the high rate of failures expected in the wide area."

Concerning the Wiencko reference, Weincko similarly states that prior art RAID is insufficient and proposes an improvement Wiencko col. 7 ll. 1-14. Since Wells and Wiencko commonly disparage the use of RAID it is not evident that Wiencko's improvement would be incompatible with Wells. Additionally, Wiencko's described improvement is described in a strikingly similar manner to that of erasure coding, see Wiencko col. 7 ll. 1-14.

As noted above Xu discloses Erasure-correcting codes as suggested by the Wells reference which states in § 3.2: "Erasure codes are a superset of these classic mechanisms which provide extremely high durability and availability without imposing an unreasonable overhead in storage space."

Further, Wells states that erasure codes are a genus of RAID and replication and designates their use for his system while Xu discloses a type of erasure code that might improve RAID (Xu p. 3 3). With this background, Applicant's argument can be summarized as: "Wells intended species of erasure codes excludes the species of erasure code disclosed in Xu"; while the Examiner's necessary retort is that "the species of erasure code disclosed in Xu is fairly interpreted to be combinable with the genus of erasure codes designated by Wells". The Examiner is unable to determine the better argument as the Wells disclosure of what the intended genus of erasure codes comprises is ambiguous. This provides an important lesson with regard to particularly pointing out and distinctly describing systems using generic (genus) terms such as "erasure codes" and "data splitting information": that illustrative definitions are necessary to avoid unintended interpretations. See e.g. Interview Summary on 7/11/2013; Office Action on 9/17/2013 p. 4 ll. 11-12; Interview Summary on 5/01/2014; Office Action on 5/01/2014 p. 7 ll. 16-17; Interview Summary on 9/25/2014; Office Action on 11/26/2014 p. 2 ll. 20-21, p. 8 ll. 8-13..

Continuation of 13. 12/03/2014; 1/21/2015; 4/06/2015; 4/15/2015.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-6,662,299	12-09-2003	Price, III	
/M.C./		US-7,499,905	03-03-2009	Jaschek et al.	
/M.C./		US-6,853,988	02-08-2005	Dickinson et al.	
/M.C./		US-7,260,724	08-21-2007	Dickinson et al.	
/M.C./		US-5,239,659	08-24-1993	Rudeseal et al.	
/M.C./		US-6,381,331	04-30-2002	Kato	
/M.C./		US-6,009,173	12-28-1999	Sumner	
/M.C./		US-20040078542	04-22-2004	Fuller et al.	
/M.C./		US-20030084397	05-01-2003	Peleg	
/M.C./		US-6,519,262	02-11-2003	Stephens et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/M.C./		CN-101375284-A	02-25-2009	Orsini Rick L		

Examiner Signature	/Michael Chao/	Date Considered	04/09/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

47976134_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.C./		Kim et al., "Secure Group Key Management for Storage Area Networks," IEEE Communications Magazine, August 2003, pp. 92-99.	
/M.C./		Bendix, "RAID and Informix Databases," White Paper, Advanced Technology Group, June 1995; Retrieved from the Internet <URL: informix.com.ua/articles/raid/raid.htm>; retrieved from the internet on December 3, 2014, pp. 1-15 as printed	

Examiner Signature	/Michael Chao/	Date Considered	04/09/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

47976134_1

Supplemental Application Data Sheet

Application Information

Application number::	13/371,363
Filing Date::	02/10/12
Application Type::	Regular
Subject Matter::	Utility
Suggested Group Art Unit::	~~2432~~2492
CD-ROM or CD-R?::	None
Sequence submission?::	None
Computer Readable Form (CRF)?::	No
Title::	~~SECURE DATA PARSER METHOD AND SYSTEM~~SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
Attorney Docket Number::	104093-0002-105
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	36
Small Entity?::	No
Petition included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	~~Rick~~Mark
Middle Name::	[[L.]]S.
Family Name::	~~Orsini~~O'Hare
City of Residence::	~~Flower Mound~~Coto De Caza
State or Province of Residence::	[[TX]]CA
Country of Residence::	US
Street of mailing address::	~~2100 Kings Forest Lane~~8 Kennedy Court
City of mailing address::	~~Flower Mound~~
State or Province of mailing address::	[[TX]]CA
Postal or Zip Code of mailing address::	~~75028~~92679

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	~~Mark~~Rick
Middle Name::	[[S.]]L.
Family Name::	~~O'Hare~~Orsini
City of Residence::	~~Coto De Caza~~Flower Mound

State or Province of Residence::	[[CA]]TX
Country of Residence::	US
Street of mailing address::	~~8 Kennedy Court~~2100 Kings Forest Lane
City of mailing address::	~~Coto De Caza~~Flower Mound
State or Province of mailing address::	[[CA]]TX
Postal or Zip Code of mailing address::	~~92679~~75028

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Roger
Middle Name::	S.
Family Name::	Davenport
City of Residence::	Campbell
State or Province of Residence::	TX
Country of Residence::	US
Street of mailing address::	3204 CR 4119
City of mailing address::	Campbell
State or Province of mailing address::	TX
Postal or Zip Code of mailing address::	75422

Applicant Authority Type::	Inventor

Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Steven
Family Name::	Winick
City of Residence::	Roslyn Heights
State or Province of Residence::	NY
Country of Residence::	US
Street of mailing address::	3 Expressway Plaza
City of mailing address::	Roslyn Heights
State or Province of mailing address::	NY
Postal or Zip Code of mailing address::	11577

Correspondence Information

Correspondence Customer Number::	01473
E-Mail address::	USPatentMail@ropesgray.com

Representative Information

Representative Customer Number::	01473

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	11/258,839	10/25/05
11/258,839	An application claiming the benefit under 35 USC 119(e)	60/718,185	09/16/05
11/258,839	An application claiming the benefit under 35 USC 119(e)	60/622,146	10/25/04

Foreign Priority Information

Assignee Information

Assignee name::	Security First Corp.
Street of mailing address::	29811 Santa Margarita Parkway, Suite 600
City of mailing address::	Rancho Santa Margarita
State or Province of mailing address::	CA
Postal or Zip Code of mailing address::	92688

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.			
Signature	/Christopher J. Han/	Date	April 30, 2015
Name (Print/Type)	Christopher J. Han	Registration No. (Attorney/Agent)	70,069

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Christina Genoveze
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**140**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: Chao, Michael W.

REQUEST TO UPDATE THE ORDER OF THE NAMES OF JOINT INVENTORS UNDER 37 CFR 1.48(f)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Due to a typographical error, the order of the names of joint inventors was incorrectly listed in the above-identified application.

In accordance with 37 C.F.R. §1.48(f), Applicants hereby update the order of the names of joint inventors as indicated in the attached supplemental Application Data Sheet.

Applicants respectfully request that all PTO records related to this application be updated to reflect this change.

The Director is hereby authorized to charge the processing fee of $140.00 per 37 CFR 1.17(i) to our Credit Card. The Director is also hereby authorized to charge any additional fees which may be required, or credit any overpayment, to our Deposit Account Number 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: April 30, 2015

Respectfully submitted,

By /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	22216900
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Christina Genoveze
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	30-APR-2015
Filing Date:	10-FEB-2012
Time Stamp:	20:01:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$140
RAM confirmation Number	6893
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request under Rule 48 correcting inventorship	104093_0002_105_Change_of_Inventorship_Request.pdf	82403 92de66e904731e9707a55047cd35e211a48858a8	no	2
Warnings:					
Information:					
2	Application Data Sheet	104093_0002_105_Change_of_Inventorship_ADS.pdf	62426 5c877778f734e07e81dc2d8135695f911385a01b	no	6
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Fee Worksheet (SB06)	fee-info.pdf	30807 6a97f1922519a8495b5ad9ceaf08ed159e259e00	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	175636		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/371,363	02/10/2012	2492	2590	104093-0002-105	27	3

CONFIRMATION NO. 7984

CORRECTED FILING RECEIPT

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

OC00000074973948

Date Mailed: 05/08/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

Applicant(s)

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

Assignment For Published Patent Application

Security First Corp., Rancho Santa Margarita, CA

Power of Attorney: The patent practitioners associated with Customer Number 1473

Domestic Priority data as claimed by applicant

This application is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 02/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/371,363**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-105
Application Number 13/371,363	Filed February 10, 2012
For SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	
Art Unit 2492	Examiner M. W. Chao

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
X	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ $800.00 ($600.00 paid 4/6/15)
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

X Payment by credit card. ~~Form PTO-2038 is attached~~.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

X The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075 .

X Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

X attorney or agent of record. Registration number 70,069 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Christopher J. Han/	May 26, 2015
Signature	Date
Christopher J. Han	(617) 951-7000
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

X * Total of 1 forms are submitted.

50799658_1

REMARKS

Claims 1-27 are pending in this application. Independent claims 1, 10, and 19 stand finally rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Krawczyk, *Secret Sharing Made Short* ("SSMS"), Krawczyk, *Distributed Fingerprints and Secure Information Dispersal* ("DFSID"), and one of U.S. Patent No. 6,557,123 ("Wiencko"), Burkhard, *Disk Array Storage System Reliability* ("Burkhard"), or Xu, *Highly Available Distributed Storage Systems* ("Xu"). In the alternative, independent claims 1, 10, and 19 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Wells, *The OceanStore Archive: Goals, Structures, and Self-Repair* ("Wells") and one of Wiencko or Xu. The dependent claims are also finally rejected under § 103 based on one or more combinations that include the above-identified references. The Examiner withdrew the rejection under 35 U.S.C. § 103 of independent claims 1, 10, and 19 based on Wells and Burkhard in the advisory action mailed April 22, 2015.

Applicants have amended independent claims 1, 10, and 19 to clarify the claimed subject matter. The amendments do not add new matter and are fully supported by the original application (*see, e.g.,* ¶¶ 290-299, 434-439, and 447-448). Applicants traverse the rejections and request reconsideration and withdrawal of the same in light of the following remarks.

Summary of Examiner Interview

The undersigned wishes to thank Examiner Chao for the courtesies extended during the telephonic interview conducted on May 21, 2015. During the interview, the Examiner and the undersigned discussed the references, claim amendments similar to those shown in this reply, and arguments for overcoming the rejections under § 103.

Independent Claims 1, 10, and 19 Patentably Distinguish Over the Cited References

In order to expedite prosecution, and without concurring in the rejections, Applicants have amended independent claim 1 to recite, *inter alia*, separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set, and wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set. Amended independent claims 10

and 19, which recite a non-transitory computer readable medium and a computer system, respectively, have been amended to recite similar subject matter as independent claim 1.

The cited references, either alone or in combination, fail to teach or suggest separating encrypted data into a plurality of shares, wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set. For example, in the Office Action, the Examiner acknowledges that SSMS and DFSID "transform the input data into shares by a computation which takes the **entire** input data to formulate each output share." *See* Office Action, pg. 3 (emphasis added). Since each of the alleged shares in SSMS and DFSID is based on the *entire* input data, i.e., contiguous data, the alleged shares do not contain a "non-contiguous subset" of the input data, as required by Applicants' claims.

The Examiner acknowledges that Wells fails to teach shares which are based on less than all of the units of data of the encrypted data set. *See* Office Action, pg. 19. Since Wells does not teach shares based on a subset of the encrypted data set, it follows that Wells also does not teach shares that contain a *non-contiguous* subset of the encrypted data set. Therefore, Wells fails to remedy the deficiencies of SSMS and DFSID.

Each of Wiencko, Burkhard, and Xu also fail to teach shares that contain a non-contiguous subset of the encrypted data set. Wiencko discusses a data storage apparatus comprising a disk array of n disks, each disk storing a "stripe set" comprising H data bits and Q redundancy bits. *See* Wiencko, col. 7 lines 15-18 and col. 8 lines 37-44. However, Wiencko does not specify that the H data bits comprise a non-contiguous subset of an encrypted data set, as claimed. In fact, in RAID systems, which are referenced throughout Wiencko, a data "stripe" consists of contiguous, sequential segments of the original data.[1] Therefore, one of ordinary skill in the art would understand Wiencko's stripes to be contiguous sequential data, and not a non-contiguous subset of an encrypted data set, as claimed.

Burkhard discusses the use of a dispersal matrix which maps *m* data byte values to *n* fragment byte values. *See* Burkhard, § 2. As with SSMS and DFSID, Burkhard utilizes the *entire*

[1] *See, e.g., Common RAID Disk Data Format Specification*, Storage Networking Industry Association (March 27, 2009), http://www.snia.org/sites/default/files/SNIA_DDF_Technical_Position_v2.0.pdf.

input data, through its dispersal matrix, to transform the input *m* data bytes into fragments, and thus also fails to teach shares that contain a "non-contiguous subset" of the input data, as claimed.

Xu discusses storing data through the use of an array code, wherein data bits and parity bits are placed in a 2-dimensional array, and wherein bits in the same column are stored in the same disk. *See* Xu, § 2.1. During the telephonic interview, the Examiner contended that "bits in the same column" comprise a "non-contiguous subset" of the original data. Specifically, the Examiner asserted that the information bits, when placed in a 2-dimensional array as taught by Xu, formed a sequence such that each row of the 2-dimensional array formed a contiguous subset of the original data, but that columns of the 2-dimensional array did not form a contiguous subset of the original data. Applicants respectfully disagree. Contrary to the Examiner's assertions, both the rows and the columns of Xu's 2-dimensional array comprise a *contiguous* subset of the 2-dimensional array. That is, each of the rows and columns in Xu's 2-dimensional array comprises a sequential portion of adjacent elements of the 2-dimensional array. In contrast, Applicants' claims recite shares that contain a non-contiguous subset of the data. This serves to improve security because an adversary that obtains one or more shares would require knowledge of the data splitting information used to separate the units of data in order recover any portion of the original data.

For at least the foregoing reasons, the cited references, either alone or in combination, fail to teach the subject matter of independent claims 1, 10, and 19, and all claims dependent thereon. Applicants respectfully request reconsideration and withdrawal of the rejections under § 103.

Conclusion

In view of the foregoing, Applicants believe the pending application is in condition for allowance.

Applicants believe no fee is due with this response other than as indicated on the Fee Transmittal submitted concurrently herewith. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: May 26, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	22445087
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	26-MAY-2015
Filing Date:	10-FEB-2012
Time Stamp:	18:59:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$2500
RAM confirmation Number	9746
Deposit Account	061075
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		104093_0002_105_Amendment.pdf	140023 1384faa2cebb233ff0c607413bd9df7856a12848	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	11

Warnings:

Information:

2	Request for Continued Examination (RCE)	104093_0002_105_RCE.pdf	94403 8be1807aaf6f09fe28b378c19176c2f39d5536de	no	1

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

3	Extension of Time	104093_0002_105_EOT.pdf	89254 6da523b93f3c391e50878284a948b82a684b1a9a	no	1

Warnings:

Information:

4	Fee Worksheet (SB06)	fee-info.pdf	32617 4fe011cd98d5dd25b36734401a88dd6ffc148347	no	2

Warnings:

Information:

Total Files Size (in bytes):	356297

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

USED IN LIEU OF PTO/SB/30 (07-09)

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. [ ] Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. [ ] Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. [ ] Other _____

   b. [x] Enclosed

      i. [x] Amendment/Reply

      ii. [ ] Affidavit(s)/Declaration(s)

      iii. [ ] Information Disclosure Statement (IDS)

      iv. [ ] Other _____

2. Miscellaneous

   a. [ ] Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. [ ] Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. [x] The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 06-1075 .

      i. [x] RCE fee required under 37 CFR 1.17(e)

      ii. [x] Extension of time fee (37 CFR 1.136 and 1.17)

      iii. [ ] Other _____

   b. [ ] Check in the amount of $ _____ enclosed

   c. [x] Payment by credit card (~~Form PTO-2038 enclosed~~)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Christopher J. Han/	Date	May 26, 2015
Name (Print/Type)	Christopher J. Han	Registration No.	70,069

50800123_1

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $600 paid	1253	1	800	800
Miscellaneous:				
RCE- 2nd and Subsequent Request	1820	1	1700	1700
		Total in USD ($)		**2500**

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application.

Listing of Claims

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, ~~by processing circuitry~~ using a hardware processor, the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set, and wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. (Original) The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. (Original) The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. (Previously Presented) The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

7. (Original) The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. (Original) The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. (Original) The method of claim 1, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

10. (Currently Amended) A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set, and wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. (Original) The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. (Previously Presented) The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

16. (Original) The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. (Original) The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. (Original) The non-transitory computer readable medium of claim 10, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

19. (Currently Amended) A computer system for securing a data set, the system comprising:

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share is based on one or more, but not all, of the units of data of the encrypted data set, and wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set;

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. (Original) The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. (Original) The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. (Previously Presented) The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir secret sharing algorithm.

25. (Original) The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. (Original) The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. (Original) The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
O'Hare et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

REPLY ACCOMPANYING REQUEST FOR CONTINUED EXAMINATION (RCE) UNDER 37 C.F.R. 1.114

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

In response to the Office Action dated November 26, 2014, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

1473 7590 05/28/2015

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
05/28/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com
pair_rg@firsttofile.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	O'HARE ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*. (3)_____.

(2) *Christopher Han (Reg. No. 70,069)*. (4)_____.

Date of Interview: *21 May 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *(see OA 11/26/2014)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and Examiner discussed possible claim amendments, no agreement reached..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Michael Chao/ Primary Examiner, Art Unit 2492	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
O'Hare et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed before the mailing date of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114 (37 C.F.R. § 1.97(b)(4)).

51250391_1

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Dated: June 22, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	22698317
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	22-JUN-2015
Filing Date:	10-FEB-2012
Time Stamp:	16:25:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	104093_002_105_IDS_Transmittal.pdf	81989 6dcaa443b42ef09139629a462393699a637e4a69	no	2

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	104093_002_105_SB08.pdf	118266 dac1a812f2a7bb556cc27212223ff1f6963f7adc	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	DArco_Fault_Tolerant_and_Distributed_Broadcast_Encryption.pdf	15967090 92ee221522a82462acccb4e283b3501c1393d47f	no	18
Warnings:					
Information:					
4	Non Patent Literature	Schwartz_Using_field_encryption_in_applications.pdf	20644110 73f0606352f7fdc4a0fb0b394ce6ab5da5fe2cc3	no	16
Warnings:					
Information:					
		Total Files Size (in bytes):	36811455		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2003/0126434	07-03-2003	Lim et al.	
		US-7,730,543	06-01-2010	Nath	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		D'Arco et al.: "Fault Tolerant and distributed Broadcast Encryption"; 2003: Retrieved from the Internet<URL:link.springer.com/chapter/10.1007/3-540-36563-x18#page-1>; pp. 1-18 as printed.	
		Schwartz, Richard; "Using field encryption in applications"; 2001; Retrieved from the Internet<URL:ibm.com/developerworks/lotus/library/ls-filed_encryption/>; pp. 1-16 as printed.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/M.C./		US-2003/0126434	07-03-2003	Lim et al.	
/M.C./		US-7,730,543	06-01-2010	Nath	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	06/26/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at **www.uspto.gov** or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.C./		D'Arco et al.: "Fault Tolerant and distributed Broadcast Encryption"; 2003: Retrieved from the Internet<URL:link.springer.com/chapter/10.1007/3-540-36563-x18#page-1>; pp. 1-18 as printed.	
/M.C./		Schwartz, Richard; "Using field encryption in applications"; 2001; Retrieved from the Internet<URL:ibm.com/developerworks/lotus/library/ls-filed_encryption/>; pp. 1-16 as printed.	

Examiner Signature	/Michael Chao/	Date Considered	06/26/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S131	17	RAID (bit adj masking OR byte adj masking)	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2015/06/12 16:20
S133	443	RAID (stripe or block) same random same (secret OR secure OR security)	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2015/06/12 16:23
S134	95	(orsini adj2 rick).in.	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2015/06/12 16:24
S135	97	(security adj first).asn.	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2015/06/12 16:24

EAST Search History (Interference)

<This search history is empty>

6/26/2015 11:00:07 AM
C:\Users\mchao\Documents\EAST\Workspaces\13371363.wsp

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination O'HARE ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Goodson et al.; Efficient consistency for erasure-coded data via versioning servers; 3-2003; Retrieved from the Internet <URL: oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461126>; pp. 1-25 as printed.
	V	Long et al.; Swift/RAID: A Distributed RAID System; 1994; Retrieved from the Internet <URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7183>; pp. 1-20 as printed.
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

1473 7590 07/01/2015

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
07/01/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com
pair_rg@firsttofile.com

Office Action Summary	Application No. 13/371,363	Applicant(s) O'HARE ET AL.	
	Examiner Michael Chao	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/26/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-27* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *6/22/2015*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Although Applicant and Examiner agree on how Applicant's system differs from the prior art RAID/array-coding systems the following action is provided to elaborate the Examiner's position and to clarify the record regarding Applicant's position on the applicability of RAID type splitting to the claimed "splitting" Step.

Claims 1-27 are pending.

Argument Summary

The newly cited reference Swift (Long et al.) discloses a species of RAID where an input file is first separated into a stripe (A) and the stripe is then decomposed into blocks (B) where the blocks of multiple stripes are assigned to a disk (share) (C). See Figure 2 which represents the RAID as a two dimensional array with rows forming stripes and columns forming drives/nodes.

SSMS discloses a method for distributing data using secret sharing appended to an Information Dispersal Algorithm where the IDA works on some file, which may be a large file (A), formed by the concatenation of multiple IDAs (SSMS p. 6 ¶ 1: "We stress that for large files, it is not necessary to work on a huge field but just to view the information as the concatenation of different polynomials.")(B) Such that each IDA forms a portion of a share, which is concatenated to form the whole (C) (SSMS p. 6 step 2).

Xu discloses an analogous IDA mechanism (Erasure Correcting Code, Xu § 2.1) where original data (A) is represented by a two dimensional array (B) and the columns thereof are used to compose a share (C) ("In an array code, the information (original) and parity (redundant) bits are placed in a 2-dimensional array of size 1 x n. In a distributed storage system, the bits in the same column are stored in the same disk." Xu § 2.1).

Although SSMS was modified by Xu, they collectively share the property that some "original" data or "large file" (A) is decomposed into an intermediate representations(B) {different polynomials (SSMS), rows (Xu)} which are concatenated (SSMS) or placed in the same column (Xu) to form an IDA share (C).

Applicant's system works in a similar manner retrieving an input file, placing it into an intermediate data store, and finally outputting the shares. "FIG. 31 . . . . (A) At step 3100 data to be secured is identified and a call is made to the secure data parser. . . . (B) It outputs the data shares into split shares buffers 3010. . . . (C) Wrapper layer 3022 then writes the output shares (obtained from split shares buffers 3010) appropriately (e.g., written to one or more storage devices, communicated onto a network, etc.)." (¶ 432 as published 2012/016681)

Applicant avers that the new limitation "wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set;" is not shown by Xu

because (Rem. p. 10 ¶ 2 on 5/26/2015) the intermediate array representation of the data (B) in Xu, which assigns a column to a share, only contains "contiguous" data.

In other words, Applicant argues that the data in each column is "contiguous" because it is intermediately stored (B) in an array where the column bits are represented as next to each other.

Examiner's position is that it is a reasonable interpretation that contiguity is judged solely by the relationship of the data to its original input form. Thus, the data in the columns cannot be contiguous because they are from successive bytes (Xu) or stripes (Swift) and are missing the intermediate data found in other drives or nodes. This interpretation is supported by Swift which states that "Data within each data stripe is logically contiguous." (p. 2 ¶ 1) As data within a stripe is contiguous, then data in the set of blocks at any given node (Swift Figure 2) must be non-contiguous as it lacks the contiguous blocks of the stripe stored at other nodes.

Additionally, if the layout or orientation of the data in intermediary processing steps (B) could render the data contiguous or non-contiguous then Applicant's own system, which breaks the data into “shares buffers 3010” and then without further computations uses said shares buffers to constitute the claimed output shares would also contain solely contiguous data.

Response to Arguments

Applicant's arguments filed 5/26/2015 have been fully considered but they are not persuasive.

The only claim term currently at issue is the requirements for "separating the encrypted data into a plurality of shares based on the data splitting information". While no particular method is required Applicant further narrows this limitation by stating two properties of the separation:

(1) wherein each share is based on one or more, but not all, of the units of data of the encrypted data set.

(2) wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set.

Since the set of all possible data separation mechanisms are circumscribed by the claim limitations (1) and (2) the issue is determining whether prior art examples of data separation mechanisms conform to the requirements of the claim (1) and (2) or are excluded thereby. Since the claims must be "given their broadest reasonable interpretation consistent with the specification," *Phillips v. AWH Corp.*, 415 F.3d 1303, 1316, 75 USPQ2d 1321, 1329 (Fed. Cir. 2005), our inquiry begins with Applicant's detailed description.

[0443] It will be understood that any other suitable parsing and splitting approach may be used to generate portions of data from an original data set in accordance with the present invention. For example, parsing and splitting may be randomly or pseudo-randomly processed on a bit by bit basis. A random or pseudo-random value may be used (e.g., session key, cipher feedback session key, etc.) whereby for each bit in the original data, the result of a hash function on corresponding data in the random or pseudo-random value may indicate to which share to append the respective bit. In one suitable approach the random or pseudo-random value may be generated as, or extended to, 8 times the size of the original data so that the hash function may be performed on a corresponding byte of the random or pseudo-random value with respect to each bit of the original data. Any other suitable algorithm for parsing and splitting data on a bit by bit level may be used in accordance with the present invention. It will further be appreciated that redundancy data may be appended to the data shares such as, for example, in the manner described immediately above in accordance with the present invention.

(as published US 2012/0166815, emphasis Examiners.)

Although Applicant's Figure 35 shows a two shares with consecutive bits the above paragraph supports shares with a plurality of non-consecutive bits.

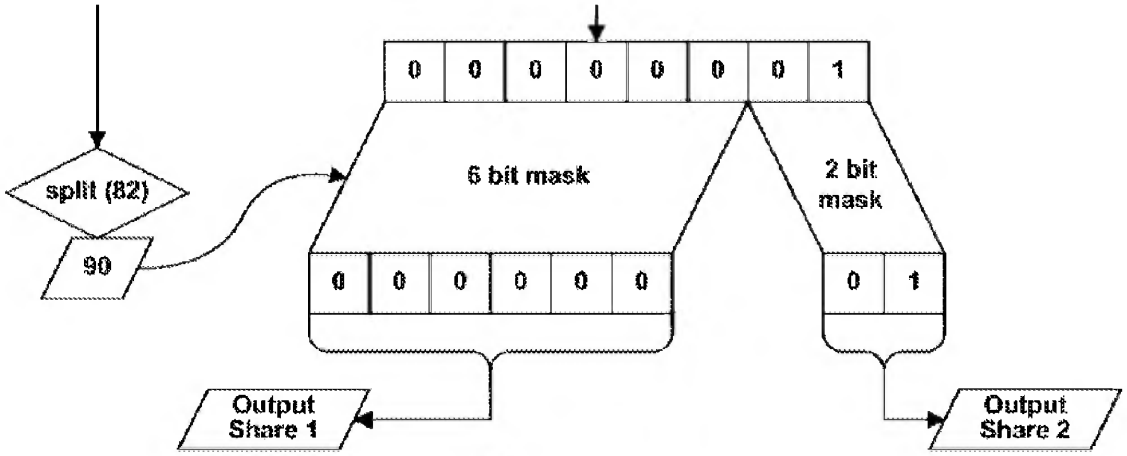
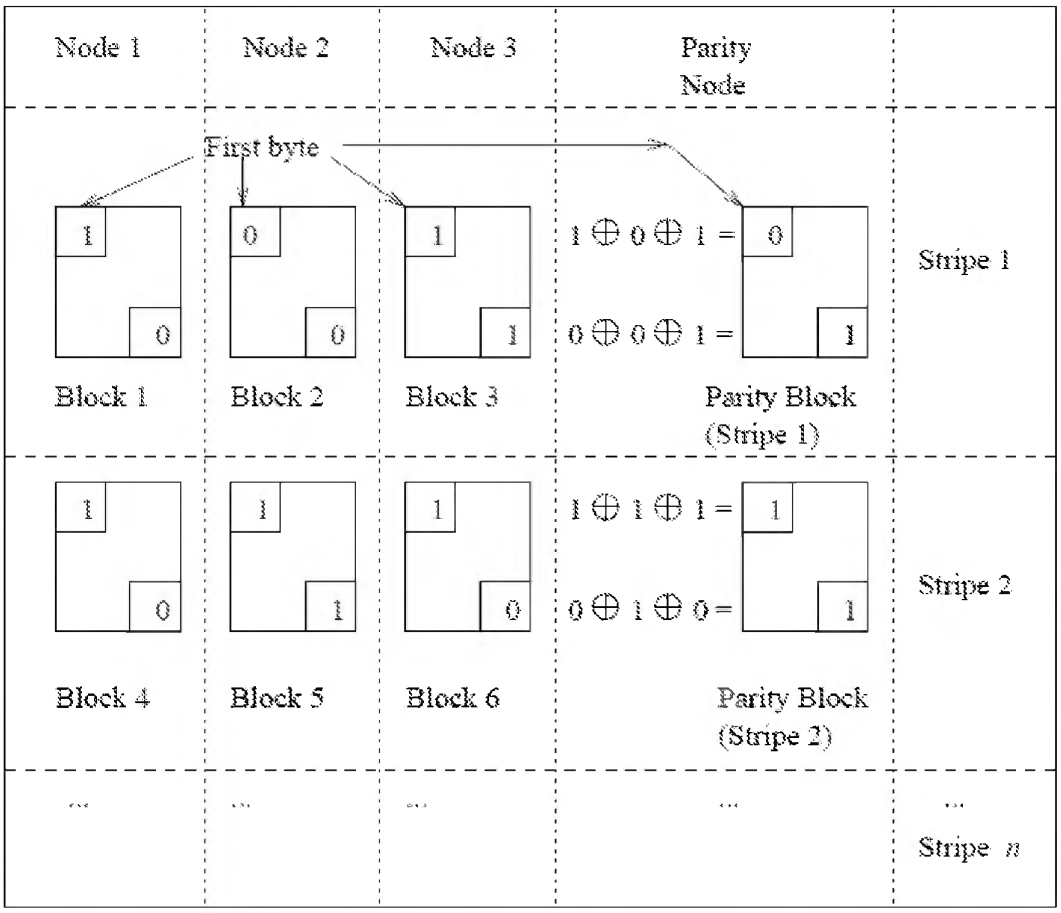


FIG. 35

Swift discloses how a RAID-4 system functions to break the data up into a multitude of disks (nodes) in Figure 2.



Here each stripe is analogous to the full byte input in Applicant's cropped Figure 35 (above) and each block is analogous to one or more bits. Both systems take some arbitrary length input file and break it into a plurality of stripes (Swift) or bits (Applicant).

Clearly, each bit of Applicant's input byte are contiguous and each block in the stripe of Swift is contiguous (Swift p. 2 ¶ 1). Further, as to the individual shares (Applicant's figure 35) or nodes (Swift) the data within is contiguous as it is merely a partition of a larger input stripe (Swift) or byte (Applicant).

Applicant's ¶ 443 discloses a further modification where the bits for a given share are (N.1) not consecutive bits of the input byte but rather "random or pseudo-randomly" selected for a given share. Applicant's Figure 35 also discloses (N.2) that the shares may have disparate amounts of data.

The prior art Swift differs from both (N.1) and (N.2) in that the nodes have equal amounts of data in each stripe and further that the data of the blocks for a given stripe are consecutive respective to the input (Swift p. 2 ¶ 1).

All the other art cited in the alternative to Swift (Xu, Buckhard, Weincko) is similarly distinct from (N.1) and (N.2).

Applicant presently asserts that the claim limitation "wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set" excludes the prior art Xu because the columns of the two dimensional arrays of Xu (and Swift) are "contiguous". In other words, Applicant argues that multiple blocks resident in each column (Swift) or bytes of each column of Xu are contiguous by virtue of the two dimensional array.

If the intermediary representations of data, between the original input file and the output shares (nodes-Swift, disks-Xu) rendered data contiguous then Applicant's own intermediary step of storing data within the "split shares buffers 3010" (Applicant's ¶ 432 as published) would similarly render all data within the "share" contiguous.

Furthermore, in asserting that the data of the prior art is contiguous Applicant focuses on where the data is stored, rather than what the data represents. Asserting

that the storage of the intermediary data in two dimensional arrays of the prior art (Xu, Swift) render the data contiguous focuses solely on how the data is stored and ignores what the data represents (e.g. if the data in the share was contiguous, consecutive, or adjacent in the original data set). The issue with Applicant's interpretation is that data will always be "contiguous" to some other data; if the logical representation of the data is ignored (Swift p. 2 ¶ 1) it is uncertain how contiguousness, or lack thereof, could be determined.

Applicant is free to define the claims using any terms he desires (MPEP 2111.01(IV) and the Examiner is not opposed to expressions/arguments which invoke prosecution history estoppel from avoiding the prior art (MPEP 2173.02(III)(B). The question therefore becomes what exactly is included or excluded by the explanatory properties of the claimed "splitting" step:

(1) wherein each share is based on one or more, but not all, of the units of data of the encrypted data set.

(2) <u>wherein at least some of the plurality of shares contain a non-contiguous subset of the encrypted data set.</u>

If (2) requires that a share contain a plurality non-consecutive bits from a single stripe (Swift), byte (Xu), or IDA (Krawczyk, where multiple IDAs are concatenated to create the original file p. 6 ¶ 1)(e.g. N.1), then such is not shown by the prior art. Conversely, if (2) merely requires that from the splitting process any two non-

consecutive data from the original file be present in a share, then such would be shown by all RAID(Swift) or array-coding (Xu) systems.

This action is provided to clarify Applicant's and Examiner's position so that the record may be clear with regard to how the claimed "splitting" is distinct from the prior art RAID (Swift) and array-coding (Xu) systems.

Claims 1, 2, 6-11, 15-20, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); Xu (Highly Available Distributed Storage Systems); or Swift (Long et al.—Swift/RAID: A Distributed RAID System).

Goodson et al. (Efficient consistency for erasure-coded data via versioning servers) discloses terminology in the art of erasure coding, specifically "With erasure coding, a data-item is encoded into a set of fragments such that any sufficient subset allows reconstruction. (A primitive version of this is the RAID mechanism [45] of striping plus parity computed across the stripe units.) With these data distribution schemes, reads require fragments from multiple servers. Moreover, the set of fragments must correspond to the same write operation or else the reconstituted "data" will be incoherent. Examples of distributed storage systems that use erasure coding include

Zebra [21], SwiftRAID [35], Intermemory [10], Cheops [4], Myriad [9], and PASIS [59, 60]." (Goodson p. 3 ¶ 1).

In summary, RAID was considered analogous to erasure coding, and SwiftRAID uses erasure coding. Swift would therefore have been an obvious implementation of the IDA scheme of Krawczyk, as suggested by Krawczyk (§ 3 ¶ 2).

See prior action (11/26/2014) and/or prosecution history for detailed mapping.

Claims 3, 5, 12, 14, 21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID in view of either {Wiencko et al. (US 6,557,123); Buckhard et al. (Disk Array Storage System Reliability); Xu (Highly Available Distributed Storage Systems); or Swift (Long et al.—Swift/RAID: A Distributed RAID System)} in view of either {Fitzpatrick (US 2003/30167408) or Tewari et al. (High Availability in Clustered Multimedia Servers)}.

Claims 1, 2, 6-11, 15-20, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells (The OceanStore Archive: Goals, Structures, and Self-Repair) in view of either {Wiencko et al. (US 6,557,123); or Xu (Highly Available Distributed Storage Systems)}.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Chao/
Primary Examiner, Art Unit 2492

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	O'HARE ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 67/108	4/25/2014	mc
G06F 11/1092	4/25/2014	mc

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/17/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	4/25/2014	mc
google searched "array coding" and "erasure OR error coding raid"	4/25/2014	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	10/3/2014	mc

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
google searched "RAID 0+1" "RAID storage randomize"	10/3/2014	mc
google searched "erasure-coding RAID"	6/11/2015	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	6/12/2015	mc

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	26 (with claim terms)	10/3/2014	mc

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

1473 7590 10/20/2015

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
10/20/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com
pair_rg@firsttofile.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	O'HARE ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*.

(2) *Christopher Han (Reg. No. 70,069)*.

(3) *George Ligler*.

(4) _____.

Date of Interview: *15 October 2015*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☐ applicant ☒ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *All cited in OA 7/01/2015*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner agreed that changing the non contiguous subset limitation to different amounts of the encrypted data set would distinguish over the art of record and place the claims in condition for allowance.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Michael Chao/ Primary Examiner, Art Unit 2492	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application.

Listing of Claims

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting, using a hardware processor, the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share ~~is based on~~ contains one or more, but not all, of the units of data of the encrypted data set, and wherein at least ~~some~~ two of the plurality of shares contain ~~a non-contiguous subset~~ different amounts of the encrypted data set;

including in the plurality of shares ~~(a)~~ data indicative of the encryption key and ~~(b)~~ the hash information; and

causing the plurality of shares to be stored in ~~respective~~ separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. (Original) The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. (Original) The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. (Previously Presented) The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

7. (Original) The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. (Original) The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. (Currently Amended) The method of claim 1, wherein ~~the step of storing~~ the ~~shares in respective~~ separate storage locations ~~comprises storing the shares~~ are located on at least two separate storage devices.

10. (Currently Amended) A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share ~~is based on~~ contains one or more, but not all, of the units of data of the encrypted data set, and wherein at least ~~some~~ two of the plurality of shares contain ~~a non-contiguous subset~~ different amounts of the encrypted data set;

including in the plurality of shares ~~(a)~~ data indicative of the encryption key and ~~(b)~~ the hash information; and

causing the plurality of shares to be stored in ~~respective~~ separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. (Original) The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. (Previously Presented) The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

16. (Original) The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. (Original) The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. (Currently Amended) The non-transitory computer readable medium of claim 10, wherein ~~the step of storing~~ the ~~shares in respective~~ separate storage locations ~~comprises storing the shares~~ are located on at least two separate storage devices.

19. (Currently Amended) A computer system for securing a data set, the system comprising:

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information, wherein each share ~~is based on~~ contains one or more, but not all, of the units of data of the encrypted data set, and wherein at least ~~some~~ two of the plurality of shares contain ~~a non-contiguous subset~~ different amounts of the encrypted data set;

including in the plurality of shares ~~(a)~~ data indicative of the encryption key and ~~(b)~~ the hash information; and

causing the plurality of shares to be stored in ~~respective~~ separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. (Original) The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. (Original) The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. (Previously Presented) The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir secret sharing algorithm.

25. (Original) The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. (Original) The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. (Original) The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

28. (New) The method of claim 1, wherein the separate storage locations are located on one storage device.

29. (New) The method of claim 1, wherein the separate storage locations are geographically separated.

30. (New) The method of claim 1, wherein causing the plurality of shares to be stored in separate storage locations comprises causing the plurality of shares to be stored in respective separate storage locations.

31. (New) The non-transitory computer readable medium of claim 10, wherein the separate storage locations are located on one storage device.

32. (New) The non-transitory computer readable medium of claim 10, wherein the separate storage locations are geographically separated.

33. (New) The non-transitory computer readable medium of claim 10, wherein causing the plurality of shares to be stored in separate storage locations comprises causing the plurality of shares to be stored in respective separate storage locations.

34. (New) The computer system of claim 19, wherein the separate storage locations are located on one storage device.

35. (New) The computer system of claim 19, wherein the separate storage locations are geographically separated.

36. (New) The computer system of claim 19, wherein causing the plurality of shares to be stored in separate storage locations comprises causing the plurality of shares to be stored in respective separate storage locations.

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,959,199	09/24/2009	Peleg et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 2 309 700	04/13/2011	Alcatel Lucent		
		JP 2005/244379	09/08/2005	NEC Communication Syst		√
		WO 2001/054370	07/26/2001	The University of Manitoba		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Goodson et al., "Efficient consistency for erasure-coded data via versioning servers," Retrieved from the Internet<URL:oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461126> 25 pages, March 2003.	
		Long et al., "Swift/RAID: A Distributed RAID System," Retrieved from the Internet<URL:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7183>pgs. 1-20 (1994).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

53811906_1

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
O'Hare et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

RESPONSE TO NON-FINAL OFFICE ACTION

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action dated July 1, 2015, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 309 700 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.02.2013 Bulletin 2013/09

(51) Int Cl.:
H04L 29/08 *(2006.01)* ***H04L 29/06*** *(2006.01)*
G06F 21/00 *(2013.01)*

(21) Application number: **09305958.2**

(22) Date of filing: **08.10.2009**

(54) **A method and a system for transferring data in a telecommunication network, a server, a storage, a computer program and a computer program product**

Verfahren und System zur Übertragung von Daten in einem Telekommunikationsnetzwerk, Server, Speicher, Computerprogramm und Computerprogrammprodukt

Système et procédé pour le transfert de données dans un réseau de télécommunication, serveur, stockage, programme informatique et produit de programme informatique

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(43) Date of publication of application:
13.04.2011 Bulletin 2011/15

(73) Proprietor: **Alcatel Lucent**
75007 Paris (FR)

(72) Inventors:
- **Wahl, Stefan**
  71707, Schwieberdingen (DE)
- **Drewniok, Marc**
  73728, Esslingen a. N. (DE)
- **Kessler, Marcus**
  73728, Esslingen a. N. (DE)

(74) Representative: **Wetzel, Emmanuelle et al**
Alcatel-Lucent Deutschland AG
Intellectual Property & Corporate Standards
Lorenzstrasse 10
70435 Stuttgart (DE)

(56) References cited:
US-A1- 2003 188 153 **US-A1- 2003 204 602**
US-A1- 2004 015 724 **US-A1- 2007 067 332**
US-A1- 2008 126 357

- **BATTEN C ET AL: "pStore: A Secure Peer-to-Peer Backup System (MIT-LCS-TM-632)" INTERNET CITATION 8 December 2001 (2001-12-08), XP002233336 Retrieved from the Internet: URL: http://kbarr.net/static/pstore/pStore. pdf> [retrieved on 2003-03-04]**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 2 309 700 B1

Description

Field of the invention

[0001] The invention relates to a method for transferring data in a computerized network.

Background

[0002] In an example for the implementation of a distributed storage an entire set of data is encrypted and then transferred entirely to a single storage unit of at distributed storage system.

[0003] However transferring entire sets of data, even encrypted, to a single storage unit, makes an attempt to breach the encryption and obtain the entire set of data easy. Data security in this case depends on the strength of the encryption only.

[0004] In another example a single set of data is split up into parts and individual parts of the single set of data are transferred to different storage units of a distributed storage.

[0005] This means that for multiple sets of data a header is needed for each part of each set of data. Furthermore this way of splitting up the set of data may easily allow not authorized access to the data transferred to the distributed storage, because the inherent structure of the parts and the headers is well known.

[0006] US2004/015724A1 discloses a transparent secure file storage in which network data files are secure through the operation of an infrastructure gateway based network file access appliance. Network file data corresponding to network pocket payload data are further reduced to a sequence of data blocks that are secured through any combination of block encryption, impression and digital signatures.

[0007] Thus, storing multiple sets of data, e.g. files from a company server, on a distributed storage, e.g. in cloud computing, with the aforementioned methods either is susceptible to breaching the encryption or requires a large overhead and a clear structure within the stored parts, that makes unauthorized access less difficult.

Summary

[0008] The object of the invention is thus to improve the transfer of data to a distributed storage.

[0009] The main idea of the invention is to transfer data in a computerized network, wherein a first data block is transferred between a first server and a second server, said first data block containing a first data segment determined depending on a first file, and a second data segment determined depending on a second file. This means that files, are split up in data segments and individual data segments of different files are combined to data blocks that are stored on a distributed storage. This way each data block contains data segments of different sets of data. This means that, because the data blocks don't contain information about start and end of a certain data segment, said data segments, and therefore said files, can't be accessed without further information about the structure of the data block that is not sent to said distributed storage.

[0010] Advantageously said first server determines said first data segment depending on a first fragment of said first set of data or of a first encrypted set of data, or said second data segment depending on a second fragment of said second set of data or of a second encrypted set of data. This means that the sets of data, e.g. files, are split up in fragments and data blocks containing only fragments of the sets of data. Thus no single storage device of said distributed storage stores all data segments required to re-assemble a certain set of data, i.e. file. This makes unauthorized access to the sets of data more difficult.

[0011] Advantageously said first server determines said first data segment depending on a first encryption key or said second data segment depending on a second encryption key. This means that the segments are stored encrypted which adds to the data security.

[0012] Advantageously said first encrypted set of data or said second encrypted set of data contains error correction code, and said first set of data or said second set of data is recreated from less than all of said data blocks.

[0013] Further developments of the invention can be gathered from the dependent claims and the following description.

Brief description of the figures

[0014] In the following the invention will be explained further making reference to the attached drawings.

Fig. 1 schematically shows part of a computerized network according to an embodiment of the invention.

Fig. 2 schematically shows some typical data structures according to said embodiment of the invention.

Fig. 3 schematically shows a table according to said embodiment of the invention.

Fig. 4 schematically shows a flow chart according to said embodiment of the invention.

Detailed description of the embodiments

[0015] A first example of an embodiment of the invention is described below making reference to figures 1, 2, 3 and 4.

[0016] Goal of said fist example is to store two sets of data, e.g. two files, on a distributed storage.

[0017] Fig. 1 shows part of a computerized network 100 according to said first example.

[0018] Said computerized network 100 comprises sev-

EX1009, Page 1216

en servers 101, ..., 107. Said servers 101, ..., 107 are identified by consecutively numbered storage identifiers A1, ..., A7.

[0019] Said storage identifiers A1, ..., A7 are for example internet protocol addresses of said corresponding servers 101, ..., 107. Said storage identifiers A1, ..., A7 may be any other identifier of said servers 101, ..., 107, like a name according to the domain name system (well known as DNS).

[0020] Said internet protocol addresses are for example read by said first server 101 from a mapping stored on said first server 101 in a first non-volatile storage.

[0021] Said servers 101, ..., 107 are connected to each other via one data link or multiple a data links.

[0022] According to said first example said distributed storage comprises said server 101, ..., 107. Alternatively said distributed storage may include more or less servers. Alternatively said distributed storage may not include said first server 101.

[0023] Said data link is for example an internet protocol connection (well known as IP connection) or any other type of data connection.

[0024] Said servers 101 ..., 107 may be connected to each other via multiple network nodes or directly.

[0025] Said figure 2 schematically shows a first set of data 201 and a second set of data 202.

[0026] Said first server 101 may be adapted to store said sets of data 201, 202 in a first volatile memory of said first server 101. Alternatively said sets of data 201, 202 may be stored at least temporarily on said first non-volatile storage.

[0027] Furthermore said figure 2 schematically shows a first encrypted set of data 203 and a second encrypted set of data 204. Said first server 101 may be adapted to encrypt said sets of data 201, 202 to determine said encrypted sets of data 203, 204 using a first encryption key k1 and a second encryption key k2 respectively.

[0028] Methods for encrypting sets of data, e.g. using Twofish encryption or the symmetric advanced encryption standard (well known as AES), are well know to a person skilled in the art and not further explained here.

[0029] Additionally said first server 101 is adapted to fragment said encrypted sets of data 203, 204 into data fragments. Said first server 101 is for example adapted to randomly fragment each of said encrypted sets of data 203, 204 into the same amount of fragments. Said fragments may be of same size, e.g. 128bit or different, arbitrarily, e.g. randomly, chosen size,

[0030] Alternatively said first server 101 may be adapted to fragment said encrypted sets of data 203, 204 into different amounts of fragments. This is particularly useful in case more than two encrypted sets of data are to be stored.

[0031] Any of the sets of data or encrypted sets of data may be padded, i.e. filled, with additional, e.g. randomly selected, bits.

[0032] Furthermore said first server 101 is adapted to determine data blocks from said data fragments.

[0033] Said figure 2 schematically shows a first data block 210 as an example for said data blocks. Said first data block 210 comprises a first header 211, a first data segment 212 and a second data segment 213.

[0034] Said first data block 210 is determined by said first server 101 depending on a first data fragment 205 and a second data fragment 206. Said first data fragment 205 and said second data fragment 206 are, e.g. randomly or consecutively, chosen by said first server 101 from said data fragments of said first encrypted set of data 203 and said second encrypted set of data 204 respectively.

[0035] Additionally the order of said first data segment 212 and said second data segment 213 in said first data block 210 is determined randomly by said first server 101.

[0036] In order to be able to reconstruct said sets of data 201, 202 from said data blocks, said first server 101 is adapted to gather and store information about said data blocks. According to said first example a first table 301, as depicted in figure 3, is stored in said first non-volatile storage.

[0037] Said table 301 consist of a first column containing in a first row a first data identifier I1 of said first set of data 201 and in a second row a second data identifier I2 of said second set of data 202.

[0038] Columns two to eight contain in each row 3-tuples each containing one of said storage identifiers A1, ..., A7, said block identifiers B1, ..., B7, and a segment identifier S(I1,B1), ..., S(I1,B7), S(I2,B1), ..., S(I2, B7) each.

[0039] Said segment identifiers S(I1,B1), ..., S(I1,B7), S(I2,B1), ...,S(I2,B7) are determined by said first server 101 for each of said data segments. Said segment identifiers S(I1,B1), ..., S(I1,B7), S(I2,B1), ...,S(I2,B7) references a position of each of said data segments in their respective data block. Said position is for example referenced via a Bit offset for the starting address of each of said data segments in each of said data blocks.

[0040] As an example the determination of a first segment identifier S(I1,B1) and a second segment identifier S(I2,B1) as shown in table 301 is explained below. All other segment identifiers are determined likewise.

[0041] Said first segment identifier S(I1,B1) is set to the starting address of said first data segment 212 in said first data block 210. Additionally said second segment identifier S(I2,B1) is set to the starting address of said second data segment 213 in said first data block 210.

[0042] Said first server 101 is adapted to places each randomly chosen data fragment into any randomly chosen data segment of any randomly chosen data block. Additionally said first server 101 may be adapted to place only a single data fragment of a specific set of data into a certain data block.

[0043] Said table 301 is further explained using said first data block 210 as example. Information about any other data block is stored in the same way.

[0044] Said table 301 indicates the storage location of said first data fragment 205 of said first encrypted set of

EX1009, Page 1217

data 203. According to said table 301, said first data fragment 205 is stored on said first server 101 in said first data block 210 as indicated by said 3-touple in line one, column two. Also from said first segment identifier S (I1,B1) contained in said 3-touple the starting position of said first data segment 212 containing said first data fragment 205 can be derived. The length of said first data fragment 205 can be derived from the starting address of said second data fragment 206 or the overall length of said first data block 210 in case said first data fragment 205 would be the last data fragment of said first data block 210.

[0045] Additionally to the storage information, said first encryption key k1 and said second encryption key k2 are stored in a last column, i.e. column 9, of said table 301 in said first row and said second row respectively.

[0046] According to said first example seven data blocks including two data segments each are determined this way.

[0047] Said data blocks according to said first example are identified by consecutive data block identifiers B1, ..., B7 respectively. Said data block identifiers are for example a consecutive numbering of said data blocks starting at One, e.g. B1=1, ..., D7=7.

[0048] Said first header 211 contains said first data block identifier B1, identifying said first data block 210.

[0049] Said first data block identifier B1 is set for example to One by said first server 101, stored in said first table 301 and said first header 211. Said first data block identifier B1 may be any other identifier, like a random number or a literal.

[0050] Additionally said first server 101 is adapted to transfer, i.e. to send or receive, said data blocks.

[0051] Said first server 101 is adapted to determine, e.g. randomly, said storage identifiers as a destination for each of said data blocks. Additionally said server 101 is adapted to send each of said data blocks in a first message to the server corresponding to the determined storage identifier. Said first message contains a first indicator, e.g. a bit, indicating the request to store said first data block 210.

[0052] Additionally said first server 101 is adapted to store said storage identifier in the appropriate 3-tuple in said first table 301.

[0053] Said first storage identifier is for example said internet protocol address of said first data storage 111.

[0054] Additionally said first server 101 is adapted to request said data blocks from their respective storage.

[0055] To that end said first server 101 is adapted to read said information about said storage location from said first table 301 stored on said non-volatile storage.

[0056] According to said first example all servers, data blocks and data segments are selected by said first server 101 randomly. Alternatively the order of said distributed storages said data blocks or said data segments may be selected consecutively.

[0057] In order to retrieve a certain set of data from said distributed storage, said first server 101 is adapted to send a second message, e.g. as burst message to all servers, requesting all data blocks a set of data is comprised of. Said second message is determined by said first server 101 depending on said information about said storage location stored in said first table 301.

[0058] According to said first example said first server 101 is adapted to look up said information about said storage location in said table 301 upon a trigger. Such trigger is for example a user input received by said first server 101 via user interface. Said user input identifies said first set of data 201 by means of said first data identifier I1 or said second set of data 202 by means of said second data identifier I2.

[0059] Said first server 101 is adapted to determine said second message to request said data blocks by looking up said storage identifiers, i.e. said first internet protocol addresses of said servers, in said table 301. Said second message is sent to said internet protocol addresses of said servers via said internet protocol.

[0060] Furthermore said second message contains a second indicator that said data blocks are requested from said servers. Said indicator may be a bit indicating said request. Additionally said second message contains said data block, identifiers B1, ..., B7.

[0061] Said first server 101 is adapted to wait for a third message in response to sending said second message. According to said first example said first server 101 is adapted monitor all incoming messages to detect said third message containing any of said data blocks.

[0062] The assembling of said sets of data is explained by example of said first set of data 201. Any other set of data is assembled by said first server 101 likewise.

[0063] Said first server 101 is adapted to assemble said first set of data 201 depending on said data blocks received from said distributed storage in said third messages.

[0064] According to said first example, said first server 101 is adapted to assemble said first encrypted set of data 204 by consecutively looking up said data segments in all data blocks according to the information stored in the row of said table 301 that is indicated by said data identifier I1.

[0065] Said first server 101 is adapted to decipher said first encrypted set of data 204 using said first encryption key k1, stored in said table 301,

[0066] As example for all servers of said distributed data storage capable of storing data blocks, a second server 107 is described below. All other servers are adapted likewise.

[0067] According to said first example said second server 107 is adapted to store said first data block 210 upon receipt of said first message. To that end said second server 107 is adapted to monitor all incoming messages and to determine if an incoming message contains said first indicator or said first data block 210. Furthermore said second server 107 is adapted to store said first data block 210 if it was determined that said first data block 210 was received.

EX1009, Page 1218

[0068] Furthermore according to said first example said second server 107 is adapted to determine said first data block identifier B1 from said first message and store said first data identifier B1 in a look-up table together with a reference to the storage location of said first data block 210 on said second server 107.

[0069] Additionally said second server 107 is adapted to transfer said first data block 210 upon receipt of said second message. To that end said second server 107 is adapted to monitor all incoming messages to determine if said second message is received, e.g. by monitoring said bit in said messages.

[0070] Additionally said second server 107 is adapted to send a third message containing said first data block 210 to said server 101 upon receipt of said second message.

[0071] Furthermore said second server 107 is adapted to determine said first data block identifier B1 from said second message and determine said third message containing said first data block 210 by looking up said storage sector in said look-up table.

[0072] According to said first example, said third message is sent to said server 101 using a second internet protocol address of said server 101. Said second internet protocol address is received as return address in said second message.

[0073] The goal of a first method according to the invention is to transfer said sets of data to said distributed storage, According to said first example said first method starts as soon as two sets of data need to be stored.

[0074] Below said first method is described referencing figure 4 and using said first set of data 201 and said second set of data 202 as example. Said first method applies likewise to any other amount of sets of data.

[0075] After the start of said first method a step 1 is executed.

[0076] In said step 1 all sets of data that need to be stored on said distributed storage are determined by means of their data identifier. A set of data may be a file or a folder as defined by an operating system that is used to run said first server 101. According to said first example only said first set of data 201 and said second set of data 202 need to be transferred. Afterwards a step 2 is executed.

[0077] In said step 2 each set of data is encrypted. According to said first example said first set of data 201 is encrypted using said first encryption key k1 and said second set of data 202 is encrypted using said second encryption key k2. Said encrypted sets of data are stored in a volatile storage on said first server 101. Said first encrypted set of data 203 or said second encrypted set of data 204 may additionally contain error correction code, e.g. a forward error correction code like a Reed-Solomon-Code, or manipulation detection code, e.g. a hash value or a cyclic redundancy check checksum. Afterwards a step 3 is executed.

[0078] In said step 3 each encrypted set of data is fragmented. According to said first example said first encrypted set of data 203 and said second encrypted set of data 204 are fragmented into 7 randomly sized fragments each. Afterwards a step 4 is executed.

[0079] In said step 4 each header of each data block is determined. According to said first example said first data block 210 contains said first header 211. Said first header 211 comprises said first data block identifier B1. Said first. data block identifier B1 is set to B1=1. All other headers are determined likewise using corresponding storage identifiers and data identifiers. Afterwards a step 5 is executed.

[0080] In said step 5 each data block is assembled by combining its header with data segments resulting from fragmenting said encrypted sets of data. According to said first example each data block contains at least one data fragment of each encrypted set of data. According to said first example said first data block 210 is assembled to comprise said first header 211, said first data segment 212, containing said first data fragment 205, and said second data segment 213, containing said second data fragment 206. To indicate the position of said first data segment 212 in said first data block 210, said first segment identifier S(I1,B1) is set to the starting address of said first data segment 212. Likewise said second data segment identifier S(I2,B1) is set to the starting address of said second data segment 213. Afterwards a step 6 is executed.

[0081] In said step 6 said information about said storage location is stored. According to said first example said table 301 is generated and stored. Afterwards a step 7 is executed.

[0082] In said steep 7 each data block is sent to a random server of the distributed storage. Said first table 301 is amended to include the storage identifier for each data block. According to said first example said first message is determined and sent. Afterwards said first method ends.

[0083] The goal of a second method according to the invention is to retrieve data blocks stored on said distributed storage.

[0084] Said second method is described using said first set of data 201 as an example but applies to any set of data as well.

[0085] Said second method starts, whenever said first set of data 201 needs to be retrieved from said distributed storage. According to said first example said second method starts, whenever said user inputs said first data identifier I1 using said user interface.

[0086] After said second method started a step 20 is executed.

[0087] In said step 20 said second message is determined. According to said first example said second message is determined to include all data block identifier B1, ..., B7 depending on said table 301. Said second message is determined to contain said first storage identifier A1 and said first block identifier B1. Afterwards a step 21 is executed.

[0088] In step 21 said second message is sent. Ac-

EX1009, Page 1219

cording to said first example, said second message is sent to all servers that according to said first table 301 contain data blocks of said first set of data 201. Afterwards a step 22 is executed.

[0089] In said step 22 a timer is started to wait for said third messages. According to said second method, said timer is a clock initialized with Zero. Afterwards a step 23 is executed.

[0090] In said step 23 a test is performed to determine if said timer exceeds a first threshold. According to said second example a test is performed to determine, whether said timer exceeds 500 milliseconds. In case said timer exceeds said first threshold said second method ends, for example with an error message. Otherwise a step 24 is executed.

[0091] In said step 24, a test is performed to check whether all or all except one of the requested data blocks were received. To that end the block identifiers of the data blocks received are compared to the entries in said first table 301. In case all of the requested data blocks or all but one of the requested data block were received a step 25 is executed. Otherwise said timer is increased, e.g. by 5 milliseconds, and said step 23 is executed.

[0092] In said step 25 said first encrypted set of data 203 is assembled using all available data fragments of all data blocks received with said third messages. In case one data block is missing, an additional step is executed to recreate said first encrypted set of data 203 or said second encrypted set of data 204 from less than all of said data blocks by means of decoding said error correction code. Afterwards a step 26 is eye-cuted.

[0093] In said step 26 said first encrypted set of data 203 is deciphered using said first encryption key k1 to determine said first set of data 201. Afterwards said second method ends.

[0094] The goal of a third method according to the invention is to store said data blocks on said servers 101, ..., 107.

[0095] Said third method is described using said first data block 210 as an example. Said third method starts whenever said first message is received. Afterwards a step 30 is executed.

[0096] In said step 30 said first data block 210 received in said first message is stored. Additionally said first data block identifier B1 is determined and stored separately in said look-up table. Afterwards said third method ends.

[0097] The goal of a fourth method according to the invention is to send said data blocks from said data storages 111, 112, ..., 119 to said first server 101.

[0098] Said fourth method is described using said first data block 210 was an example. Said fourth method starts whenever said second message is received. Afterwards a step 40 is executed.

[0099] In said step 40 said first data block identifier B1, is determined from said second message and used to look up said storage location of said first data block 210 in said look-up Lable. Afterwards said first data block 210 is read and sent in said third message. According to said first example, said third message is addressed using said internet protocol address received in said second message. Afterwards said fourth method ends.

[0100] The invention is neither limited to determining seven data blocks nor to using seven servers or fragments. Any other number or order of data blocks and servers may be used. Furthermore the number of data blocks and the number of servers may differ from each other.

[0101] All of the aforementioned methods may be implemented as a computer program that, when executed on a computer performs all of the steps described in the method. Said computer program may be stored on a computer program product, like a compact disk or a hard disk.

[0102] The description and drawings merely illustrate the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the invention and are included within its spirit and scope. Furthermore, all examples, recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the invention and the concepts contributed by the inventor(s) to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0103] The functions of the various elements shown in the figures, including any functional blocks labeled as 'processors', may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software, When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term 'processor' or 'controller' should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, network processor, application specific, integrated circuit (ASIC), field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), and non volatile storage, Other hardware, conventional and/or custom, may also be included. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the implementer as more specifically understood from the context.

[0104] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative circuitry embodying the principles of the invention, Similarly, it will be appreciated that any

EX1009, Page 1220

flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0105] A person of skill in the art would readily recognize that steps of various above-described methods can be performed by programmed computers. Herein, some embodiments are also intended to cover program storage devices, e.g., digital data storage media, which are machine or computer readable and encode machine-executable or computer-executable programs of instructions, wherein said instructions perform some or all of the steps of said above-described methods. The program storage devices may be, e.g., digital memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media. The embodiments are also intended to cover computers programmed to perform said steps of the above-described methods.

Claims

1. A method for transferring data in a computerized network, wherein a first data block (210) is transferred between a first server (101) and a second server (107), **characterized in that** said first data block (210) contains a first data segment (212) determined depending on a first fragment (205) of a first file (201), and a second data segment (213) determined depending on a second fragment (206) of a second file (202).

2. The method according to claim 1, **characterized in that** said first server (101) determines said first data segment (212) depending on a first fragment (205) of a first encrypted set of data (203), or said second data segment (213) depending on a second fragment (206) of a second encrypted set of data (204).

3. The method according to claim 1, **characterized in that** said first server (101) determines said first data segment (212) depending on a first encryption key (k1) or said second data segment (213) depending on a second encryption key (k2).

4. The method according to claim 1, **characterized in that** said first server (101) stores information (301) about said second server (107).

5. The method according to claim 1, **characterized in that** said first file or said second file are recreated from said data blocks.

6. The method according to claim 1, **characterized in that** a first encrypted set of data (203) or a second encrypted set of data (204) contain error correction code, and that said first file or said second file is recreated from less than all of said data blocks.

7. A system for transferring data in a computerized network, wherein said system comprises a first server (101) and a second server (107) for transferring a first data block (210), said first data block (210) containing a first data segment (212) determined depending on a first fragment (205) of a first file (201) and a second data segment (213) determined depending on a second fragment (206) of a second file (202).

8. A first server (101) for transferring data in a computerized network, adapted to determine a first data block (210) containing a first data segment (212) determined depending on a first fragment (205) of a first file (201) and a second data segment (213) determined depending on asecond fragment (206) of a second file (202), and to transfer said first data block (210).

9. A computer program for transferring data in a computerized network, wherein said computer program, when executed on a computer, causes the computer to transfer a first data block (210), said first data block (210) containing a first data segment (212) determined depending on a first fragment (205) of a first file (201) and a second data segment (213) determined depending on a second fragment (206) of a second file (202).

10. A computer program product for transferring data in a computerized network, comprising a computer usable medium having a computer readable program, wherein said computer readable program, when executed on a computer, causes the computer to transfer a first data block (210), said first data block (210) containing a first data segment (212) determined depending on a first fragment (205) of a first file (201) and a second data segment (213) determined depending on a second fragment (206) of a second file (202).

Patentansprüche

1. Verfahren zur Übertragung von Daten in einem computergesteuerten Netzwerk, wobei ein erster Datenblock (210) zwischen einem ersten Server (101) und einem zweiten Server (107) übertragen wird, **dadurch gekennzeichnet, dass** der besagte erste Datenblock (210) ein erstes Datensegment (212), welches in Abhängigkeit von einem ersten Fragment (205) einer ersten Datei (201) bestimmt wird, und ein zweites Datensegment (213), welches in Abhängigkeit von einem zweiten Fragment (206) einer

EX1009, Page 1221

zweiten Datei (202) bestimmt wird, enthält.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der besagte erste Server (101) das besagte erste Datensegment (212) in Abhängigkeit von einem ersten Fragment (205) eines ersten verschlüsselten Datensatzes (203) oder das besagte zweite Datensegment (213) in Abhängigkeit von einem zweiten Fragment (206) eines zweiten verschlüsselten Datensatzes (204) bestimmt.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der besagte erste Server (101) das besagte erste Datensegment (212) in Abhängigkeit von einem ersten Verschlüsselungsschlüssel (k1) oder das besagte zweite Datensegment (213) in Abhängigkeit von einem zweiten Verschlüsselungsschlüssel (k2) bestimmt.

4. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der besagte erste Server (101) Informationen (301) über den besagten zweiten Server (107) speichert.

5. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die besagte erste Datei oder die besagte zweite Datei aus den besagten Datenblöcken zurückgewonnen wird.

6. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** ein erster verschlüsselter Datensatz (203) oder ein zweiter verschlüsselter Datensatz (204) einen Fehlerkorrekturcode enthält, und dass die besagte erste Datei oder die besagte zweite Datei aus weniger als allen der besagten Datenblöcke zurückgewonnen wird.

7. System zur Übertragung von Daten in einem computergesteuerten Netzwerk, wobei das besagte System einen ersten Server (101) und einen zweiten Server (107) für die Übertragung eines ersten Datenblocks (210) umfasst, wobei der besagte erste Datenblock (210) ein erstes Datensegment (212), welches in Abhängigkeit von einem ersten Fragment (205) einer ersten Datei (201) bestimmt wird, und ein zweites Datensegment (213), welches in Abhängigkeit von einem zweiten Fragment (206) einer zweiten Datei (202) bestimmt wird, enthält.

8. Erster Server (101) zur Übertragung von Daten in einem computergesteuerten Netzwerk, dazu ausgelegt, einen ersten Datenblock (210), der ein erstes Datensegment (212), welches in Abhängigkeit von einem ersten Fragment (205) einer ersten Datei (201) bestimmt wird, und ein zweites Datensegment (213), welches in Abhängigkeit von einem zweiten Fragment (206) einer zweiten Datei (202) bestimmt wird, enthält, zu bestimmen und den besagten ersten Datenblock (210) zu übertragen.

9. Computerprogramm zur Übertragung von Daten in einem computergesteuerten Netzwerk, wobei das besagte Computerprogramm bei dessen Ausführung auf einem Computer den Computer veranlasst, einen ersten Datenblock (210) zu übertragen, wobei der besagte erste Datenblock (210) ein erstes Datensegment (212), welches in Abhängigkeit von einem ersten Fragment (205) einer ersten Datei (201) bestimmt wird, und ein zweites Datensegment (213), welches in Abhängigkeit von einem zweiten Fragment (206) einer zweiten Datei (202) bestimmt wird, enthält.

10. Computerprogramm-Produkt zur Übertragung von Daten in einem computergesteuerten Netzwerk, umfassend ein computerlesbares Medium mit einem computerlesbaren Programm, wobei das besagte computerlesbare Programm bei dessen Ausführung auf einem Computer den Computer veranlasst, einen ersten Datenblock (210) zu übertragen, wobei der besagte erste Datenblock (210) ein erstes Datensegment (212), welches in Abhängigkeit von einem ersten Fragment (205) einer ersten Datei (201) bestimmt wird, und ein zweites Datensegment (213), welches in Abhängigkeit von einem zweiten Fragment (206) einer zweiten Datei (202) bestimmt wird, enthält.

Revendications

1. Procédé de transfert de données dans un réseau informatisé, selon lequel un premier bloc de données (210) est transféré entre un premier serveur (101) et un second serveur (107), **caractérisé en ce que** ledit premier bloc de données (210) contient un premier segment de données (212) déterminé en fonction d'un premier fragment (205) d'un premier fichier (201), et un second segment de données (213) déterminé en fonction d'un second fragment (206) d'un second fichier (202).

2. Procédé selon la revendication 1, **caractérisé en ce que** ledit premier serveur (101) détermine ledit premier segment de données (212) en fonction d'un premier fragment (205) d'un premier ensemble crypté de données (203) ou ledit second segment de données (213) en fonction d'un second fragment (206) d'un second ensemble crypté de données (204).

3. Procédé selon la revendication 1, **caractérisé en ce que** ledit premier serveur (101) détermine ledit premier segment de données (212) en fonction d'une première clé de cryptage (k1) ou ledit second segment de données (213) en fonction d'une seconde clé de cryptage (k2).

EX1009, Page 1222

4. Procédé selon la revendication 1, **caractérisé en ce que** ledit premier serveur (101) stocke des informations (301) à propos dudit second serveur (107).

5. Procédé selon la revendication 1, **caractérisé en ce que** ledit premier fichier ou ledit second fichier sont recréés à partir desdits blocs de données.

6. Procédé selon la revendication 1, **caractérisé en ce qu'**un premier ensemble crypté de données (203) ou un second ensemble crypté de données (204) contient un code de correction d'erreur et **en ce que** ledit premier fichier ou ledit second fichier est recréé à partir de moins que la totalité desdits blocs de données.

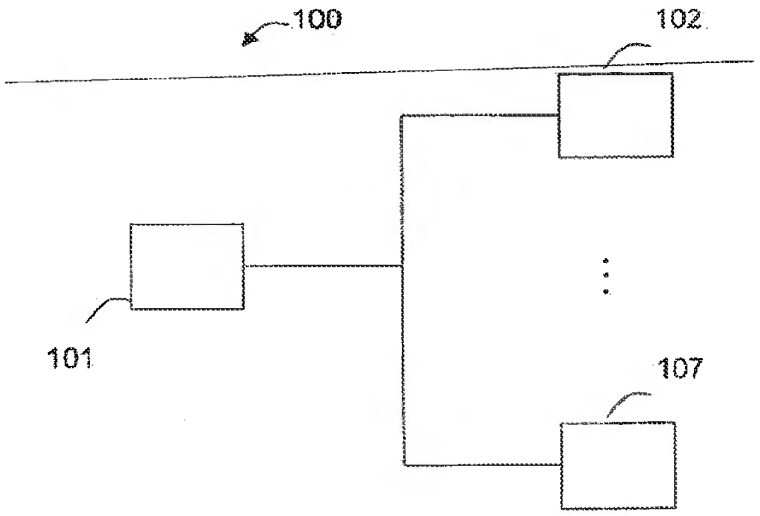
7. Système de transfert de données dans un réseau informatisé, ledit système comprenant un premier serveur (101) et un second serveur (107) pour transférer un premier bloc de données (210), ledit premier bloc de données (210) contenant un premier segment de données (212) déterminé en fonction d'un premier fragment (205) d'un premier fichier (201) et un second segment de données (213) déterminé en fonction d'un second fragment (206) d'un second fichier (202).

8. Premier serveur (101) pour transférer des données dans un réseau informatisé, adapté pour déterminer un premier bloc de données (210) contenant un premier segment de données (212) déterminé en fonction d'un premier fragment (205) d'un premier fichier (201), et un second segment de données (213) déterminé en fonction d'un second fragment (206) d'un second fichier (202), et pour transférer ledit premier bloc de données (210).

9. Programme informatique pour transférer des données dans un réseau informatisé, ledit programme informatique, lorsqu'il est exécuté sur un ordinateur, ayant pour effet que l'ordinateur transfère un premier bloc de données (210), ledit premier bloc de données (210) contenant un premier segment de données (212) déterminé en fonction d'un premier fragment (205) d'un premier fichier (201) et un second segment de données (213) déterminé en fonction d'un second fragment (206) d'un second fichier (202).

10. Produit de programme informatique pour transférer des données dans un réseau informatisé, comprenant un support utilisable par un ordinateur sur lequel se trouve un programme lisible par un ordinateur, ledit programme lisible par un ordinateur, lorsqu'il est exécuté sur un ordinateur, ayant pour effet que l'ordinateur transfère un premier bloc de données (210), ledit premier bloc de données (210) contenant un premier segment de données (212) déterminé en fonction d'un premier fragment (205) d'un premier fichier (201) et un second segment de données (213) déterminé en fonction d'un second fragment (206) d'un second fichier (202).

EX1009, Page 1223



1/4

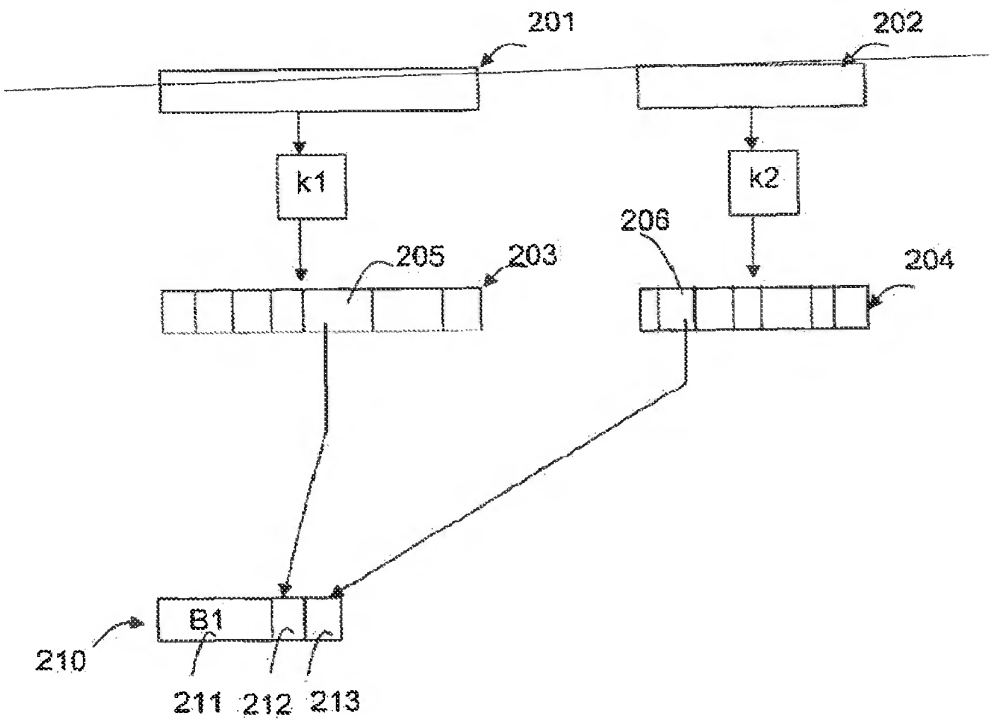


Fig.2

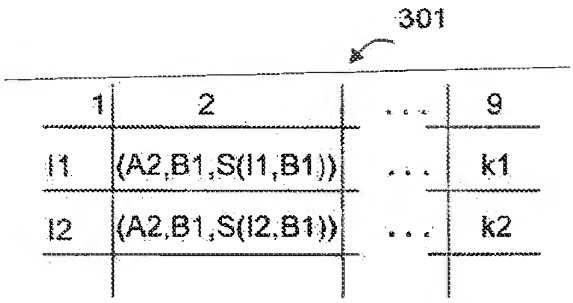


Fig.3

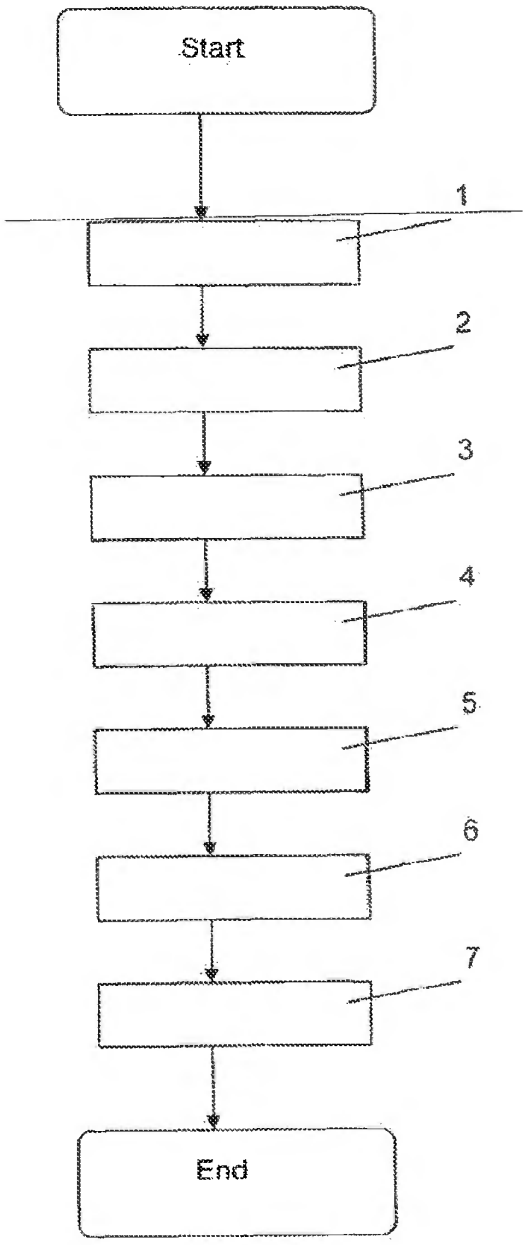


Fig.4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

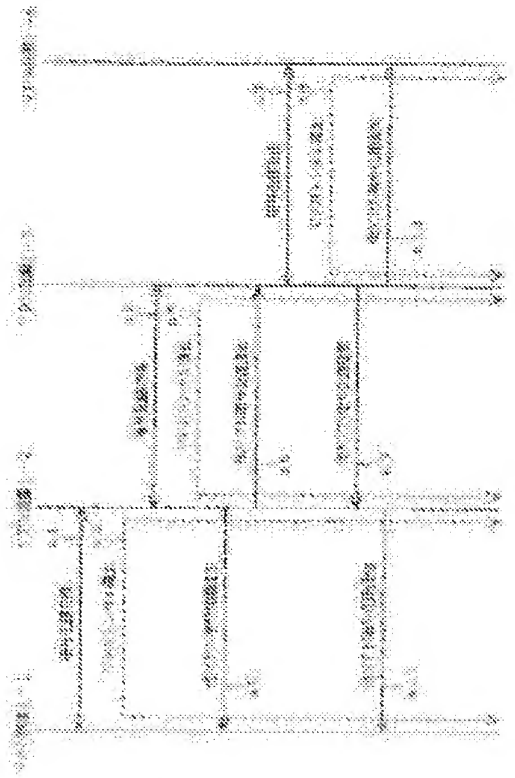
- US 2004015724 A1 **[0006]**

Bibliographic data: JP2005244379 (A) — 2005-09-08

VPN SYSTEM, VPN APPARATUS, AND ENCRYPTION KEY DISTRIBUTION METHOD USED FOR THEM

No documents available for this priority number.

Page bookmark	JP2005244379 (A) - VPN SYSTEM, VPN APPARATUS, AND ENCRYPTION KEY DISTRIBUTION METHOD USED FOR THEM
Inventor(s):	SAKAMOTO MINEYUKI ± (SAKAMOTO MINEYUKI)
Applicant(s):	NEC COMMUNICATION SYST ± (NEC COMMUN SYST LTD)
Classification:	- ***H04L12/70***; ***H04L9/08***; (IPC1-7): H04L12/56; **international:** H04L9/08 - **cooperative:**
Application number:	JP20040048865 20040225
Priority number(s):	JP20040048865 20040225



Abstract of JP2005244379 (A)

PROBLEM TO BE SOLVED: To provide a VPN system enhancing a communication speed in communications using a plurality of VPN tunnels. ;SOLUTION: A VPN tunnel is established between a VPN apparatus 1-1 and a VPN apparatus 1-2 (a2), and an encryption key is exchanged between the VPN apparatus 1-1 and the VPN apparatus 1-2 (a1). In the case of establishing a VPN tunnel between the VPN apparatus 1-2 and a VPN apparatus 1-3 (a4), the VPN apparatus 1-2 uses the VPN tunnel having already been established and encrypted to securely inform the VPN apparatus 1-1 about the encryption key (a3) received from the VPN apparatus 1-3 (a5). Upon the receipt of the encryption key of the VPN apparatus 1-3 from the VPN apparatus 1-2, the VPN apparatus 1-1 stores the encryption key to a communication partner dependent encryption key storage memory as the encryption key by each communication opposite party. ;COPYRIGHT: (C)2005,JPO&NCIPI

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP2005244379

[0001]

The present invention VPN system, a encryption key distribution method used in the VPN device and they, in particular VPN (Virtual Private Network) devices: relates to a method for improving the transmission speed of the communication that uses the (IPsec Internet Protocol security protocol).

[0002]

Conventionally, the VPN system, as shown in FIG. 1, IP (Internet Protocol) and VPN apparatus 1-1 to 1-5 disposed on the network 100, VPN user Communication terminal or LAN with VPN capabilities (Local and Area Network)] 2-1~2-5, and a VPN tunnel 101-105 Metropolitan.

[0003]

In such a configuration of the VPN system, if the VPN user 2-1 transmits the communication packet to the VPN user 2-3, it encrypts the data using first, an encryption key of the VPN apparatus 1-2, the VPN tunnel 103 and use it to send to the VPN apparatus 1-2 to.

[0004]

Is decrypted by using the encryption key of the VPN apparatus 1-2 the packet received in the VPN apparatus 1-2, a route is searched from the destination information, and then to the VPN apparatus 1-3 to send the packet, the was re-encrypts the decrypted data using an encryption key of the VPN apparatus 1-3, and transmits the packet by using a VPN tunnel 104.

The packet VPN device 1-3 which is received is decrypted by using the encryption key of the VPN apparatus 1-3, and transmits it to the VPN users 2-3 (for example, see Patent Document 1).

[0005]

Patent Publication No. 2002-111732

[0006]

However, in the conventional VPN systems described above, when the communication data is delivered to the VPN tunnel from the VPN tunnel, because the decryption of the encrypted data and the re-encryption and is carried out, if communication across multiple VPN tunnels, intermediate in it is not possible to speed up the transmission speed by the encryption and decryption capabilities of the VPN apparatus for performing communication.

[0007]

An object of the present invention to solve the above problems, VPN system that can improve the communication speed in a communication using multiple VPN tunnels, and provides an encryption key distribution method used in the VPN device and their It has to be.

[0008]

VPN system according to the invention, IPsec (Internet Protocol security protocol) between the VPN (Virtual Private Network) system using the protocol by setting the VPN tunnel to exchange mutual encryption key between the VPN device, the encrypted A VPN system for transmitting encrypted data by a key to the connection destination through the VPN tunnel,

and a means for notifying the connection destination by said other VPN tunnels through another VPN tunnel with the being established the encryption key established during and replaced with its destination VPN tunnels already in the VPN device.

[0009]

VPN device according to the invention, using IPsec (Internet Protocol security protocol) protocol to exchange mutual encryption key with the other devices by setting the VPN (Virtual Private Network) tunnel between the other devices, the encrypted data in the encrypted key to a VPN device to be transmitted to the destination via the VPN tunnel,

and a means for notifying the connection destination by said other VPN tunnels through another VPN tunnel with the being established the encryption key established during and replaced with its destination VPN tunnels already.

[0010]

Encryption key distribution method according to the invention, to exchange mutual encryption keys between IPsec (Internet Protocol security protocol) wherein between the VPN (Virtual Private Network) system using the protocol by setting the VPN tunnel VPN devices, An encryption key distribution method for distributing the encryption key in a VPN system for transmitting the encrypted data in the encrypted key to the destination via the VPN tunnel to the VPN device side, the VPN tunnel through the other of the VPN tunnels that are established during the encryption key that was exchanged with the connection destination already established and a step of notifying the connection destination by said other VPN tunnel.

[0011]

That, VPN system of the present invention, the VPN (Virtual Private Network) system using IPsec (Internet Protocol security protocol) protocol provides a method for improving the transmission rate in communication using multiple VPN tunnels (connect) it is intended to.

[0012]

More specifically, the VPN system of the invention, communication between the terminal may span multiple VPN tunnels, the encryption / decryption key data to be used in the closest VPN devices on one terminal and the other it notifies the nearest VPN device to the terminal, or by performing an inverse of the notification, so as not to perform processing for further encrypting and decrypting the encryption when relaying the VPN tunnel to another VPN tunnel.

[0013]

In this way, the VPN system of the present invention is to reduce the load related to the encryption processing of the communication between the VPN tunnel, thereby enabling the improvement in transmission rate.

In other words, the VPN system of the present invention, since it becomes possible to omit the process of re-encrypted by decrypting the encrypted data when transmitting the packet received from the VPN tunnel to another VPN tunnels, multiple VPN tunnels it is possible to improve the communication speed in a communication using.

[0014]

The present invention, by adopting the configuration and operation as described below, the effect is obtained that it is possible to improve the communication speed in a communication using a plurality of VPN tunnels.

[0015]

It will now be described with reference to the accompanying drawings embodiments of the present invention.

Figure 1 is a block diagram showing the configuration of a VPN (Virtual Private Network) system according to an embodiment of the present invention.

In Figure 1, VPN system according to an embodiment of the present invention, VPN device having a communication interface connected to the IP network 100 (the program running in the communication terminal with a communication interface is also included) 1-1 to 1-5 and , with the respective VPN users that are connected to the VPN apparatus 1-1 to 1-5 [communication terminal or LAN (Local Area Network)] 2-1~2-5, and a VPN tunnel 101-105 Metropolitan.

[0016]

VPN tunnel 101 is created between the VPN apparatus 1-1 and the VPN device 1-2, VPN tunnel 102 is created between the VPN apparatus 1-2 and the VPN device 1-3, VPN tunnel 103 VPN equipment is created between the 1-3 and the VPN device 1-4,

VPN tunnel 104 is created between the VPN apparatus 1-3 and the VPN device 1-5, VPN tunnel 105 VPN devices 1-4 and VPN equipment it has been created between 1-5.

[0017]

Figure 2 is a block diagram showing the configuration of a VPN according to an embodiment of the present invention.

In Figure 2, VPN device 1 and the encryption key exchange means 11 at the VPN tunnel establishment, the encryption key updating unit 12, the VPN packet transmitting means 13, the VPN packets through means 15 or VPN packet receiver 14, a communication and a partner by the encryption key storage memory 16..

The configuration of the VPN device 1-1 through 1-5 shown in Figure 1 have the same configuration as the above-described VPN device 1.

[0018]

3 and 4 is a sequence chart showing a method for exchanging cryptographic keys according to an embodiment of the present invention. FIG. 5 is a flowchart showing a transmission process of the VPN packets according to an embodiment of the present invention, Fig. 6 it is a flowchart showing a through and reception processing of the VPN packets according to an embodiment of the present invention. FIG. 7 is a diagram showing a configuration of a communication partner by the encryption key storage memory 16 of Figure 2, Figure 8 of the present invention is a diagram showing a VPN through display on the header of the received data according to one embodiment.

Referring to these FIGS. 1 to 8 for the processing of one embodiment of the present invention will be described.

[0019]

First, VPN tunnel 101 is established between the VPN apparatus 1-1 and the VPN device 1-2 (a2 in FIG. 3).

In this case, between the VPN device 1-1 and the VPN apparatus 1-2, mutual encryption key is exchanged in order to perform encrypted communication (a1 in FIG. 3).

[0020]

Then, when you establish a VPN tunnel 102 between the VPN apparatus 1-2 and the VPN apparatus 1-3 (FIG. 3 a4), the encryption key VPN apparatus 1-2 is received from the VPN apparatus 1-3 (a3 in FIG. 3), to securely notify the VPN apparatus 1-1 using the VPN tunnel 101 is encrypted already been established (a5 in FIG. 3).

[0021]

VPN apparatus 1-1 receives the encryption key for the VPN device 1-3 from the VPN apparatus 1-2, the communication partner by the encryption key stored as the communication partner by the encryption key memory 16 as shown in FIG. 7 We want to save to.

in this case, the communication partner by the encryption key storage memory 16, the communication partner by the encryption key, TCP the VPN user 2-3 VPN device 1-3 can be taken (Transmission Control Protocol) / IP network address It is stored along with the.

[0022]

Also, VPN apparatus 1-2 is already communicating party by encryption key information that is stored, VPN equipment in this case is a connection destination of the VPN tunnel 102 that established a new encryption key information of the VPN apparatus 1-1 to notify the 1-3 (a6 in FIG. 3).

VPN apparatus 1-3 is the encryption key information of the VPN apparatus 1-1 which has been notified from the VPN apparatus 1-2, similar to the VPN apparatus 1-1, and stores it in the communication partner by the encryption key storage memory 16.

[0023]

Then, when the VPN tunnel 103 is established between the VPN apparatus 1-3 and the VPN device 1-4 (a8 in FIG. 3), between the VPN apparatus 1-3 and VPN devices 1-4, encryption mutual encryption key is exchanged for communication (a7 in FIG. 3).

VPN apparatus 1-3, similarly to the above processing, the safety of the encryption key received from the VPN device 1-4, the VPN apparatus 1-2 using the VPN tunnel 102 is already encrypted is established to notify the (a9 in FIG. 3).

[0024]

When VPN apparatus 1-2 receives the encryption key information of the VPN device 1-4 from the VPN apparatus 1-3, because there are already established in the VPN tunnel 101 opponent, the VPN device 1-1 is its opponent, the encryption key information of the VPN device 1-4 received from the VPN apparatus 1-3 to safely notification using the VPN tunnel 101 (a11 in FIG. 3).

[0025]

Meanwhile, VPN devices 1-3 to the encryption key information of the VPN apparatus 1-2 and the VPN apparatus 1-1 that had ever, and notifies the secure VPN device 1-4 using a VPN tunnel 103 is established.

[0026]

When the VPN tunnel 104 is established between the VPN device and the VPN device 1-3 1-5, and also when the VPN tunnel 105 is established between the VPN device and the VPN device 1-4 1-5 in the same manner as described above, so that the encryption key is securely notified using the VPN tunnel 101 through 105 that are encrypted already been established to the VPN devices 1-1 to 1-5.

Thus, in this embodiment, can all VPN devices 1-1 through 1-5 that are connected by the VPN tunnel 101 to 105 has the encryption keys of all the VPN devices 1-1 to 1-5 become.

[0027]

Because of the encryption key is safety to be used in the VPN tunnel 101 to 105, a certain period of time has elapsed, is updated to the new key.

As shown in Figure 4, if the exchange of the encryption key for updating in the VPN tunnel 101 is generated that is established between the VPN apparatus 1-1 and the VPN apparatus 1-2, the encryption that is newly received it notifies the other party in the case where there the key is other VPN tunnel.

[0028]

In the case shown in Figure 4, VPN device 1-2 notifies the encryption key received from the VPN apparatus 1-1 to the VPN apparatus 1-3.

And along with the VPN apparatus 1-3 which received the new encryption key from the VPN apparatus 1-2 VPN apparatus 1-1 to update the data that I have, VPN equipment, which has received the partner of other VPN tunnel 103, 104 1 Notice one of the encryption key.

In this case, it is notified to the VPN devices 1-4 and 1-5.

[0029]

The new encryption key for the VPN apparatus 1-2, similarly to the case of the VPN apparatus 1-1 is notified to all of the VPN device 1-1~1-5 (b1~b6 in Figure 4).

Consequently, in the present embodiment, it is possible to have the latest encryption key information in all of the VPN devices 1-1 to 1-5.

[0030]

Next, a communication method using the VPN tunnel 101 through 105, will be described using the VPN packet through and receiving process shown in VPN packet transmission process and 5 shown in FIG.

[0031]

When transmitting a packet using a VPN tunnel 101~105, VPN devices 1-1 to 1-5 is initially obtains the network address from the destination IP address, a specific communication partner is shown in FIG. 7 by using it Search for encryption key of the VPN devices 1-1 to 1-5 to 2-1 to 2-5 VPN users of the destination from the encryption key is connected (Figure 6 step S11).

[0032]

If the encryption key # 1 to # 3 is registered (Figure 6 step S12), VPN devices 1-1 to 1-5 to encrypt the data to be transmitted using the encryption key (Fig. 6 Step S13), and transmitted by setting "1" to the VPN through flag of the communication data header portion shown in FIG. 8 (6 steps S14, S15).

[0033]

If the encryption key is not registered (Figure 6 step S12), VPN devices 1-1 to 1-5 to encrypt the data to be transmitted in encrypted key of the other VPN device of the VPN

tunnel 101 through 105 to be used for transmission (Figure 6 step S16), and transmitted by setting "0" to the VPN through flag of the communication data header section (6 steps S17, S15).

[0034]

If VPN devices 1-1 to 1-5 which received the packet with the VPN tunnel 101 to 105 that do not under the destination VPN users (Fig. 5 step S1), a VPN through flag in the header portion of the communication data If referring to "1" (Fig. 5 step S4), and as it transmits the packet received using the following VPN tunnel toward the destination VPN users (Fig. 5 step S7).

[0035]

For a "0" VPN through flag of the communication header section (Fig. 5 step S4), VPN devices 1-1 to 1-5 is decrypted using an encryption key that has been notified of the received data from its own device to the other VPN device After (Fig step S5), and performs the above-described VPN packet transmitting process (Fig. 5 step S6).

[0036]

If there are under the destination VPN users (Fig. 5 step S1), VPN devices 1-1 to 1-5 is decoded by the encryption key is notified to the other VPN device (Fig. 5 step S2), and that the decoded data and it sends to the VPN user 2-1 to 2-5 (Fig. 5 step S3).

[0037]

Thus, in this embodiment, it is possible to omit the process of re-encrypted by decrypting the encrypted data when transmitting the packet received from the VPN tunnel 101 through 105 to another VPN tunnels, multiple VPN It is possible to increase the communication speed in a communication using the tunnel 101-105.

[0038]

Is a block diagram showing the configuration of a VPN system according to an embodiment of the present invention.

Is a block diagram showing the configuration of a VPN according to an embodiment of the present invention.

Is a sequence chart illustrating a method for exchanging cryptographic keys according to an embodiment of the present invention.

Is a sequence chart illustrating a method for exchanging cryptographic keys according to an embodiment of the present invention.

It is a flowchart showing a transmission process of the VPN packets according to an embodiment of the present invention.

It is a flowchart showing a through and reception processing of the VPN packets according to an embodiment of the present invention.

It is a diagram showing a configuration of a communication partner by the encryption key storage memory in FIG.

Is a diagram showing a VPN through display on the header of the received data according to an embodiment of the present invention.

[0039]

1-1~1-5 VPN equipment

2-1~2-5 VPN user

11 cryptographic key exchange means

12 encryption key update means

13 VPN packet transmission means

14 VPN packet receiving means

15 VPN packet through means

16 communication partner another encryption key storage memory

100 IP network

101~105 VPN tunnel

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS JP2005244379

[0001]

IP (Internet Protocol) is located on a network a VPN (Virtual Private Network) by setting the VPN tunnel to exchange mutual encryption key between the VPN device between devices, and is encrypted by the encrypted key data The A VPN system for transmitting to a destination via the VPN tunnel,

and characterized in that it comprises a means for notifying the connection destination by said other VPN tunnels through another VPN tunnel with the being established the encryption key established during and replaced with its destination VPN tunnels already in the VPN device VPN system to be.

[0002]

VPN system according to claim 1, characterized in that it comprises holding means for holding together the information of the communication counterpart encryption key received as a communications partner by the encryption key to the VPN device via the VPN tunnel.

[0003]

The VPN device, VPN system of claim 2, wherein the encryption is performed by using the communication partner by the encryption key held in the holding means in response to the destination of the data.

[0004]

The VPN apparatus claims 1 to 3, characterized in that it informs the encryption key is updated to the destination due to the VPN tunnel through the VPN tunnel that is already established when updating the encryption key VPN system according to any one of.

[0005]

The VPN device, IPsec (Internet Protocol security protocol) VPN system according to any one of claims 1 to 4, characterized in that is used.

[0006]

IP is placed (Internet Protocol) network, and to exchange each other's encryption key with the other devices by setting the VPN (Virtual Private Network) tunnel between the other devices, and encryption by the encrypted key A VPN device that transmits and turned into data to the destination via the VPN tunnel,

VPN device characterized in that it has a means for notifying the connection destination by said other VPN tunnels through another VPN tunnel with the being established the encryption key established during and replaced with its destination VPN tunnels already.

[0007]

The VPN tunnel VPN device according to claim 6, characterized in that it comprises holding means for holding together the information of the communication counterpart encryption key received as a communications partner by the encryption key through.

[0008]

VPN apparatus of claim 7, wherein the encryption is performed by using said another communication party encryption key held in the holding means in response to the destination of the data.

[0009]

According to any one of claims 8 from claim 6, characterized in that it informs the encryption key is updated to the destination due to the VPN tunnel through the VPN tunnel that is already established when updating the encryption key VPN equipment.

[0010]

IPsec (Internet Protocol security protocol) VPN apparatus according to any one of claims 9 from claim 6, characterized by using the.

[0011]

IP (Internet Protocol) is located on a network a VPN (Virtual Private Network) by setting the VPN tunnel to exchange mutual encryption key between the VPN device between devices, and is encrypted by the encrypted key data The above is an encryption key distribution method for distributing the encryption key in a VPN system for transmitting to a destination via a VPN tunnel, the VPN apparatus and replaced in its destination when establishing the VPN tunnel and encrypting encryption key distribution method characterized by comprising the step of notifying the destination by said other VPN tunnels through another VPN tunnel is already established the key.

[0012]

The VPN device, the encrypted key distribution according to claim 11, characterized in that held in the holding means together with information of the communication partner an encryption key received as a communications partner by the encryption key through the VPN tunnel way.

[0013]

The VPN device, encryption key distribution method according to claim 12, characterized in that for encryption by using the communication partner by the encryption key held in the holding means in response to the destination of the data.

[0014]

The VPN device, the encrypted claim 11 claim 13, wherein the notifying the encryption key is updated to the destination due to the VPN tunnel through the VPN tunnel when the key is updated is already established encryption key distribution method according to any one of.

[0015]

The VPN device, IPsec (Internet Protocol security protocol) encryption key distribution method according to any one of claims 14 to claim 11, wherein the use of.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-244379
(P2005-244379A)
(43)公開日　平成17年9月8日(2005.9.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	5J104
H04L 12/56	H04L	12/56	H	5K030
	H04L	9/00	601E	

審査請求 未請求　請求項の数 15　OL　（全 10 頁）

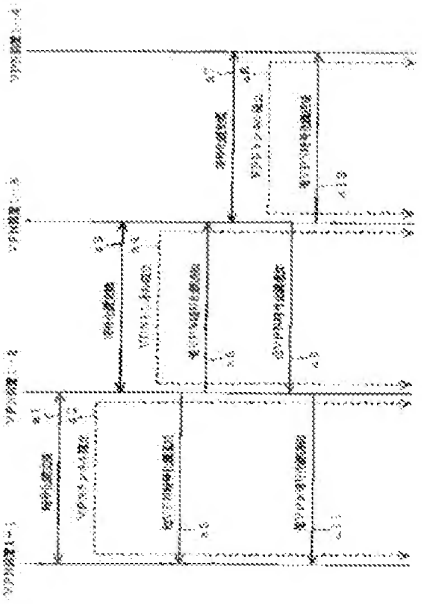
(21)出願番号　特願2004-48865(P2004-48865)
(22)出願日　平成16年2月25日(2004.2.25)

(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番２８号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　坂本　義彦
東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内

Ｆターム(参考)　5J104 AA16 EA04 EA16 EA18 JA03
NA02 NA37 PA07
5K030 GA15 HA08 HC01 HC13 LD19

(54)【発明の名称】ＶＰＮシステム、ＶＰＮ装置及びそれらに用いる暗号化鍵配布方法

(57)【要約】
【課題】　複数のＶＰＮトンネルを用いた通信において通信速度の向上を図ることが可能なＶＰＮシステムを提供する。
【解決手段】　ＶＰＮ装置１－１とＶＰＮ装置１－２との間にはＶＰＮトンネルが確立され（ａ２）、ＶＰＮ装置１－１とＶＰＮ装置１－２との間で暗号化鍵が交換される（ａ１）。ＶＰＮ装置１－２とＶＰＮ装置１－３との間にＶＰＮトンネルを確立する時（ａ４）、ＶＰＮ装置１－２はＶＰＮ装置１－３から受け取った暗号化鍵を（ａ３）、既に確立されて暗号化されているＶＰＮトンネルを使ってＶＰＮ装置１－１に安全に通知する（ａ５）。ＶＰＮ装置１－１は、ＶＰＮ装置１－３の暗号化鍵をＶＰＮ装置１－２から受け取ると、通信相手別の暗号化鍵として通信相手別暗号化鍵保存用メモリに保存する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワーク上に配置されたＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）装置間にＶＰＮトンネルを設定して前記ＶＰＮ装置間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記ＶＰＮトンネルを介して接続先に伝送するＶＰＮシステムであって、
前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知する手段を前記ＶＰＮ装置に有することを特徴とするＶＰＮシステム。
【請求項２】
前記ＶＰＮトンネルを介して受信した暗号化鍵を通信相手別の暗号化鍵としてその通信相手の情報とともに保持する保持手段を前記ＶＰＮ装置に含むことを特徴とする請求項１記載のＶＰＮシステム。
【請求項３】
前記ＶＰＮ装置は、データの送信先に応じて前記保持手段に保持された前記通信相手別の暗号化鍵を用いて暗号化を行うことを特徴とする請求項２記載のＶＰＮシステム。
【請求項４】
前記ＶＰＮ装置は、前記暗号化鍵の更新時に既に確立されているＶＰＮトンネルを介してそのＶＰＮトンネルによる接続先に更新された暗号化鍵を通知することを特徴とする請求項１から請求項３のいずれか記載のＶＰＮシステム。
【請求項５】
前記ＶＰＮ装置は、ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を用いることを特徴とする請求項１から請求項４のいずれか記載のＶＰＮシステム。
【請求項６】
ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワーク上に配置され、他装置との間にＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）トンネルを設定してその他装置との間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記ＶＰＮトンネルを介して接続先に伝送するＶＰＮ装置であって、
前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知する手段を有することを特徴とするＶＰＮ装置。
【請求項７】
前記ＶＰＮトンネルを介して受信した暗号化鍵を通信相手別の暗号化鍵としてその通信相手の情報とともに保持する保持手段を含むことを特徴とする請求項６記載のＶＰＮ装置。
【請求項８】
データの送信先に応じて前記保持手段に保持された前記通信相手別の暗号化鍵を用いて暗号化を行うことを特徴とする請求項７記載のＶＰＮ装置。
【請求項９】
前記暗号化鍵の更新時に既に確立されているＶＰＮトンネルを介してそのＶＰＮトンネルによる接続先に更新された暗号化鍵を通知することを特徴とする請求項６から請求項８のいずれか記載のＶＰＮ装置。
【請求項１０】
ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を用いることを特徴とする請求項６から請求項９のいずれか記載のＶＰＮ装置。
【請求項１１】
ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワーク上に配置されたＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）装置間にＶＰＮトンネルを設定して前記ＶＰＮ装置間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記Ｖ

ＰＮトンネルを介して接続先に伝送するＶＰＮシステムにおいて前記暗号化鍵を配布する暗号化鍵配布方法であって、前記ＶＰＮ装置側に、前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知するステップを有することを特徴とする暗号化鍵配布方法。

【請求項１２】

前記ＶＰＮ装置が、前記ＶＰＮトンネルを介して受信した暗号化鍵を通信相手別の暗号化鍵としてその通信相手の情報とともに保持手段に保持することを特徴とする請求項１１記載の暗号化鍵配布方法。

【請求項１３】

前記ＶＰＮ装置が、データの送信先に応じて前記保持手段に保持された前記通信相手別の暗号化鍵を用いて暗号化を行うことを特徴とする請求項１２記載の暗号化鍵配布方法。

【請求項１４】

前記ＶＰＮ装置が、前記暗号化鍵の更新時に既に確立されているＶＰＮトンネルを介してそのＶＰＮトンネルによる接続先に更新された暗号化鍵を通知することを特徴とする請求項１１から請求項１３のいずれか記載の暗号化鍵配布方法。

【請求項１５】

前記ＶＰＮ装置は、ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）を用いることを特徴とする請求項１１から請求項１４のいずれか記載の暗号化鍵配布方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はＶＰＮシステム、ＶＰＮ装置及びそれらに用いる暗号化鍵配布方法に関し、特にＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）装置（ＩＰｓｅｃ：Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）を使用する通信における伝送速度を向上させる方法に関する。

【背景技術】

【０００２】

従来、ＶＰＮシステムにおいては、図１に示すように、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ネットワーク１００上に配置されたＶＰＮ装置１－１～１－５と、ＶＰＮ機能を持つＶＰＮユーザ｜通信端末またはＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）｜２－１～２－５と、ＶＰＮトンネル１０１～１０５とから構成されている。

【０００３】

このような構成のＶＰＮシステムでは、ＶＰＮユーザ２－１がＶＰＮユーザ２－３に通信パケットを送信する場合、まずＶＰＮ装置１－２の暗号化鍵を用いてデータを暗号化し、ＶＰＮトンネル１０３を使ってＶＰＮ装置１－２に送信する。

【０００４】

ＶＰＮ装置１－２では受信したパケットをＶＰＮ装置１－２の暗号化鍵を用いて復号化し、送信先情報から経路を探索し、次にパケットを送信するＶＰＮ装置１－３に対して、このＶＰＮ装置１－３の暗号化鍵を用いて復号化したデータを再度暗号化し、そのパケットをＶＰＮトンネル１０４を使って送信する。ＶＰＮ装置１－３は受信したパケットをＶＰＮ装置１－３の暗号化鍵を用いて復号化し、ＶＰＮユーザ２－３に送信する（例えば、特許文献１参照）。

【０００５】

【特許文献１】特開２００２－１１１７３２号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、上述した従来のＶＰＮシステムでは、ＶＰＮトンネルからＶＰＮトンネ

ルに通信データが引き渡される際に、暗号データの復号化と再暗号化とが行われるため、複数のＶＰＮトンネルにまたがる通信の場合、中間で通信を行うＶＰＮ装置の暗号化及び復号化の能力によって伝送速度を高速化することができないという問題がある。

【０００７】

そこで、本発明の目的は上記の問題点を解消し、複数のＶＰＮトンネルを用いた通信において通信速度の向上を図ることができるＶＰＮシステム、ＶＰＮ装置及びそれらに用いる暗号化鍵配布方法を提供することにある。

【課題を解決するための手段】

【０００８】

本発明によるＶＰＮシステムは、ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）プロトコルを用いたＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）装置間にＶＰＮトンネルを設定して前記ＶＰＮ装置間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記ＶＰＮトンネルを介して接続先に伝送するＶＰＮシステムであって、

前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知する手段を前記ＶＰＮ装置に備えている。

【０００９】

本発明によるＶＰＮ装置は、ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）プロトコルを用い、他装置との間にＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）トンネルを設定してその他装置との間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記ＶＰＮトンネルを介して接続先に伝送するＶＰＮ装置であって、

前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知する手段を備えている。

【００１０】

本発明による暗号化鍵配布方法は、ＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）プロトコルを用いたＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）装置間にＶＰＮトンネルを設定して前記ＶＰＮ装置間で相互の暗号化鍵を交換し、その暗号化鍵にて暗号化したデータを前記ＶＰＮトンネルを介して接続先に伝送するＶＰＮシステムにおいて前記暗号化鍵を配布する暗号化鍵配布方法であって、前記ＶＰＮ装置側に、前記ＶＰＮトンネルの確立時にその接続先と交換した暗号化鍵を既に確立されている他のＶＰＮトンネルを介して前記他のＶＰＮトンネルによる接続先に通知するステップを備えている。

【００１１】

すなわち、本発明のＶＰＮシステムは、ＩＰｓｅｃ（ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）プロトコルを用いたＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）システムにおいて、複数のＶＰＮトンネル（接続）を使用する通信にて伝送速度を向上させる方法を提供するものである。

【００１２】

より具体的に説明すると、本発明のＶＰＮシステムでは、端末間での通信が複数のＶＰＮトンネルにまたがる場合、一方の端末に一番近いＶＰＮ装置で使用する暗号／復号用鍵データを、他方の端末に一番近いＶＰＮ装置に通知し、または逆の通知を行うことによって、ＶＰＮトンネルから別のＶＰＮトンネルへ中継する際に暗号を復号して更に暗号化する処理を行わないようにする。

【００１３】

このようにして、本発明のＶＰＮシステムでは、ＶＰＮトンネル間での通信の暗号処理に係わる負荷を軽減し、伝送速度の向上を可能としている。つまり、本発明のＶＰＮシステムでは、ＶＰＮトンネルから受信したパケットを他のＶＰＮトンネルへ送信する際に暗

号データを復号して再度暗号化する処理を省略することが可能となるため、複数のＶＰＮトンネルを用いた通信において通信速度の向上を図ることが可能となる。

【発明の効果】

【００１４】

本発明は、以下に述べるような構成及び動作とすることで、複数のＶＰＮトンネルを用いた通信において通信速度の向上を図ることができるという効果が得られる。

【発明を実施するための最良の形態】

【００１５】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）システムの構成を示すブロック図である。図１において、本発明の一実施例によるＶＰＮシステムは、ＩＰネットワーク１００に接続された通信インタフェースを持つＶＰＮ装置（通信インタフェースを持つ通信端末で稼働するプログラムも含める）１－１～１－５と、それぞれのＶＰＮ装置１－１～１－５に接続されるＶＰＮユーザ［通信端末またはＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）］２－１～２－５と、ＶＰＮトンネル１０１～１０５とから構成されている。

【００１６】

ＶＰＮトンネル１０１はＶＰＮ装置１－１とＶＰＮ装置１－２との間に作成され、ＶＰＮトンネル１０２はＶＰＮ装置１－２とＶＰＮ装置１－３との間に作成され、ＶＰＮトンネル１０３はＶＰＮ装置１－３とＶＰＮ装置１－４との間に作成され、ＶＰＮトンネル１０４はＶＰＮ装置１－３とＶＰＮ装置１－５との間に作成され、ＶＰＮトンネル１０５はＶＰＮ装置１－４とＶＰＮ装置１－５との間に作成されている。

【００１７】

図２は本発明の一実施例によるＶＰＮ装置の構成を示すブロック図である。図２において、ＶＰＮ装置１はＶＰＮトンネル確立時の暗号化鍵交換手段１１と、暗号化鍵更新手段１２と、ＶＰＮパケット送信手段１３と、ＶＰＮパケットスルー手段１５またはＶＰＮパケット受信手段１４と、通信相手別暗号化鍵保存用メモリ１６とから構成されている。尚、図１に示すＶＰＮ装置１－１～１－５の構成は上記のＶＰＮ装置１と同様の構成となっている。

【００１８】

図３及び図４は本発明の一実施例による暗号化鍵の交換方法を示すシーケンスチャートであり、図５は本発明の一実施例によるＶＰＮパケットの送信処理を示すフローチャートであり、図６は本発明の一実施例によるＶＰＮパケットのスルー及び受信処理を示すフローチャートであり、図７は図２の通信相手別暗号化鍵保存用メモリ１６の構成を示す図であり、図８は本発明の一実施例による送受信データのヘッダ上のＶＰＮスルー表示を示す図である。これら図１～図８を参照して本発明の一実施例の処理について説明する。

【００１９】

まず、ＶＰＮ装置１－１とＶＰＮ装置１－２との間にはＶＰＮトンネル１０１が確立される（図３のａ２）。この時、ＶＰＮ装置１－１とＶＰＮ装置１－２との間では、暗号通信を行うために互いの暗号化鍵が交換される（図３のａ１）。

【００２０】

次に、ＶＰＮ装置１－２とＶＰＮ装置１－３との間にＶＰＮトンネル１０２を確立する時（図３のａ４）、ＶＰＮ装置１－２はＶＰＮ装置１－３から受け取った暗号化鍵を（図３のａ３）、既に確立されて暗号化されているＶＰＮトンネル１０１を使ってＶＰＮ装置１－１に安全に通知する（図３のａ５）。

【００２１】

ＶＰＮ装置１－１は、ＶＰＮ装置１－３の暗号化鍵をＶＰＮ装置１－２から受け取ると、図７に示すような通信相手別の暗号化鍵として通信相手別暗号化鍵保存用メモリ１６に保存する。この場合、通信相手別暗号化鍵保存用メモリ１６には、通信相手別の暗号化鍵が、ＶＰＮ装置１－３のＶＰＮユーザ２－３が取り得るＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏ

ｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）／ＩＰのネットワークアドレスと一緒に格納される。

【００２２】

また、ＶＰＮ装置１－２は既に保存している通信相手別暗号化鍵情報、この場合にはＶＰＮ装置１－１の暗号化鍵情報を新たに確立したＶＰＮトンネル１０２の接続先であるＶＰＮ装置１－３に通知する（図３のａ６）。ＶＰＮ装置１－３はＶＰＮ装置１－２から通知されたＶＰＮ装置１－１の暗号化鍵情報を、ＶＰＮ装置１－１と同様に、通信相手別暗号化鍵保存用メモリ１６に格納する。

【００２３】

続いて、ＶＰＮ装置１－３とＶＰＮ装置１－４との間にＶＰＮトンネル１０３が確立された時（図３のａ８）、ＶＰＮ装置１－３とＶＰＮ装置１－４との間では、暗号通信を行うために互いの暗号化鍵が交換される（図３のａ７）。ＶＰＮ装置１－３は、上記の処理と同様にして、ＶＰＮ装置１－４から受け取った暗号化鍵を、既に確立されて暗号化されているＶＰＮトンネル１０２を使ってＶＰＮ装置１－２に安全に通知する（図３のａ９）。

【００２４】

ＶＰＮ装置１－２はＶＰＮ装置１－３からＶＰＮ装置１－４の暗号化鍵情報を受け取ると、既に確立されたＶＰＮトンネル１０１の相手があるので、その相手であるＶＰＮ装置１－１に、ＶＰＮ装置１－３から受け取ったＶＰＮ装置１－４の暗号化鍵情報をＶＰＮトンネル１０１を使って安全に通知する（図３のａ１１）。

【００２５】

一方、ＶＰＮ装置１－３は今まで持っていたＶＰＮ装置１－２及びＶＰＮ装置１－１の暗号化鍵情報を、確立したＶＰＮトンネル１０３を使って安全にＶＰＮ装置１－４に通知する。

【００２６】

ＶＰＮ装置１－３とＶＰＮ装置１－５との間にＶＰＮトンネル１０４が確立された時、及びＶＰＮ装置１－４とＶＰＮ装置１－５との間にＶＰＮトンネル１０５が確立された時にも、上記と同様にして、ＶＰＮ装置１－１～１－５には既に確立されて暗号化されているＶＰＮトンネル１０１～１０５を使って暗号化鍵が安全に通知されることとなる。よって、本実施例では、ＶＰＮトンネル１０１～１０５で接続されている全てのＶＰＮ装置１－１～１－５が全てのＶＰＮ装置１－１～１－５の暗号化鍵を持つことが可能となる。

【００２７】

ＶＰＮトンネル１０１～１０５で使用する暗号化鍵は安全のため、一定時間が過ぎると、新しい鍵に更新される。図４に示すように、ＶＰＮ装置１－１とＶＰＮ装置１－２との間に確立されているＶＰＮトンネル１０１にて更新のための暗号化鍵の交換が発生した場合、新たに受け取った暗号化鍵を他のＶＰＮトンネルがある場合にはその相手に通知する。

【００２８】

図４に示す場合には、ＶＰＮ装置１－２はＶＰＮ装置１－１から受け取った暗号化鍵をＶＰＮ装置１－３に通知する。ＶＰＮ装置１－２からＶＰＮ装置１－１の新しい暗号化鍵を受け取ったＶＰＮ装置１－３は自分が持つデータを更新するとともに、他のＶＰＮトンネル１０３，１０４の相手に受け取ったＶＰＮ装置１－１の暗号化鍵を通知する。この場合には、ＶＰＮ装置１－４，１－５に通知される。

【００２９】

ＶＰＮ装置１－２の新しい暗号化鍵も、上記のＶＰＮ装置１－１の場合と同様に、全てのＶＰＮ装置１－１～１－５に通知される（図４のｂ１～ｂ６）。これによって、本実施例では、全てのＶＰＮ装置１－１～１－５で最新の暗号化鍵情報を持つことが可能となる。

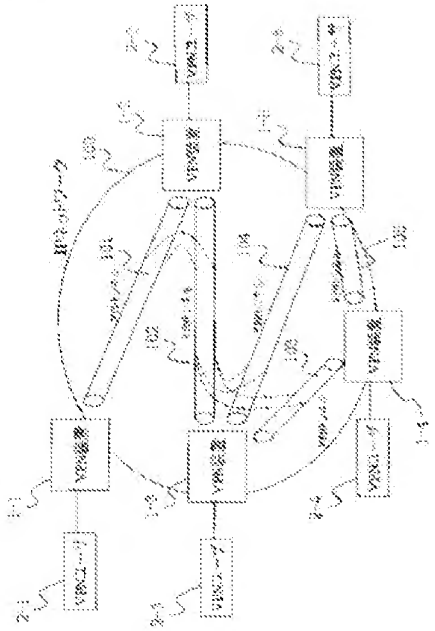
【００３０】

次に、ＶＰＮトンネル１０１～１０５を使った通信方法について、図６に示すＶＰＮパ

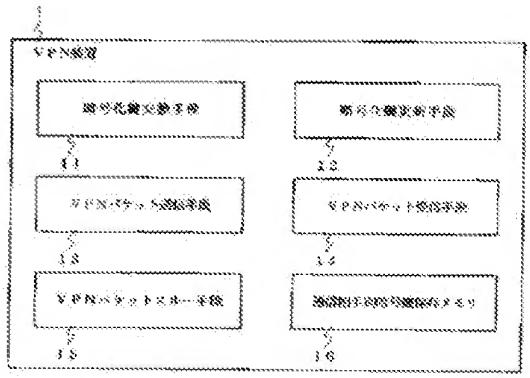
ケット送信処理と図５に示すＶＰＮパケットスルー及び受信処理とを用いて説明する。
【００３１】
ＶＰＮトンネル１０１～１０５を使ってパケットを送信する場合、ＶＰＮ装置１－１～１－５は最初に送信先のＩＰアドレスからネットワークアドレスを求め、それを使用して図７に示す通信相手別の暗号化鍵から送信先のＶＰＮユーザ２－１～２－５が接続されているＶＰＮ装置１－１～１－５の暗号化鍵を検索する（図６ステップＳ１１）。
【００３２】
暗号化鍵＃１～＃３が登録されていた場合（図６ステップＳ１２）、ＶＰＮ装置１－１～１－５はその暗号化鍵を使用して送信するデータを暗号化し（図６ステップＳ１３）、図８に示す通信データヘッダ部のＶＰＮスルーフラグに“１”を設定して送信する（図６ステップＳ１４，Ｓ１５）。
【００３３】
暗号化鍵が登録されてない場合（図６ステップＳ１２）、ＶＰＮ装置１－１～１－５は送信に使用するＶＰＮトンネル１０１～１０５の相手ＶＰＮ装置の暗号化鍵で送信するデータを暗号化し（図６ステップＳ１６）、通信データヘッダ部のＶＰＮスルーフラグに“０”を設定して送信する（図６ステップＳ１７，Ｓ１５）。
【００３４】
ＶＰＮトンネル１０１～１０５を使ってパケットを受信したＶＰＮ装置１－１～１－５は送信先のＶＰＮユーザが配下にいない場合（図５ステップＳ１）、通信データのヘッダ部にあるＶＰＮスルーフラグを参照して“１”であれば（図５ステップＳ４）、送信先ＶＰＮユーザに向かう次のＶＰＮトンネルを使って受信したパケットをそのまま送信する（図５ステップＳ７）。
【００３５】
通信ヘッダ部のＶＰＮスルーフラグが“０”の場合（図５ステップＳ４）、ＶＰＮ装置１－１～１－５は受信したデータを自装置から相手ＶＰＮ装置に通知した暗号化鍵を用いて復号した後（図５ステップＳ５）、上述したＶＰＮパケット送信処理を実行する（図５ステップＳ６）。
【００３６】
送信先ＶＰＮユーザが配下にいる場合（図５ステップＳ１）、ＶＰＮ装置１－１～１－５は相手ＶＰＮ装置に通知した暗号化鍵で復号し（図５ステップＳ２）、その復号したデータをＶＰＮユーザ２－１～２－５に送信する（図５ステップＳ３）。
【００３７】
このように、本実施例では、ＶＰＮトンネル１０１～１０５から受信したパケットを他のＶＰＮトンネルへ送信する際に暗号データを復号して再度暗号化する処理を省略することができるため、複数のＶＰＮトンネル１０１～１０５を用いた通信において通信速度を向上させることができる。
【図面の簡単な説明】
【００３８】
【図１】本発明の一実施例によるＶＰＮシステムの構成を示すブロック図である。
【図２】本発明の一実施例によるＶＰＮ装置の構成を示すブロック図である。
【図３】本発明の一実施例による暗号化鍵の交換方法を示すシーケンスチャートである。
【図４】本発明の一実施例による暗号化鍵の交換方法を示すシーケンスチャートである。
【図５】本発明の一実施例によるＶＰＮパケットの送信処理を示すフローチャートである。
【図６】本発明の一実施例によるＶＰＮパケットのスルー及び受信処理を示すフローチャートである。
【図７】図２の通信相手別暗号化鍵保存用メモリの構成を示す図である。
【図８】本発明の一実施例による送受信データのヘッダ上のＶＰＮスルー表示を示す図である。
【符号の説明】

【００３９】
１－１～１－５　ＶＰＮ装置
２－１～２－５　ＶＰＮユーザ
１１　暗号化鍵交換手段
１２　暗号化鍵更新手段
１３　ＶＰＮパケット送信手段
１４　ＶＰＮパケット受信手段
１５　ＶＰＮパケットスルー手段
１６　通信相手別暗号化鍵保存用メモリ
１００　ＩＰネットワーク
１０１～１０５　ＶＰＮトンネル

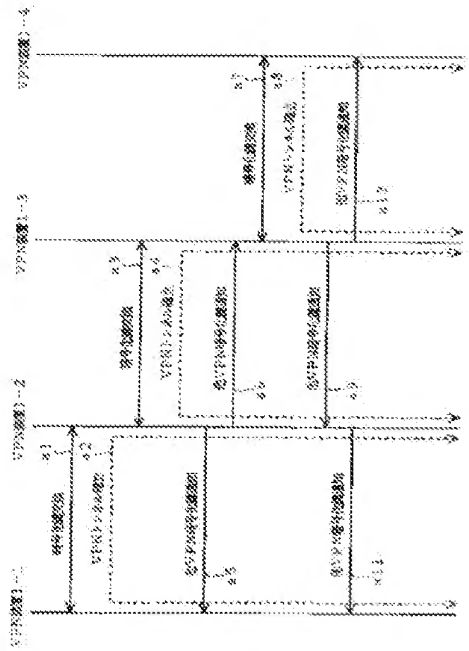
【図１】



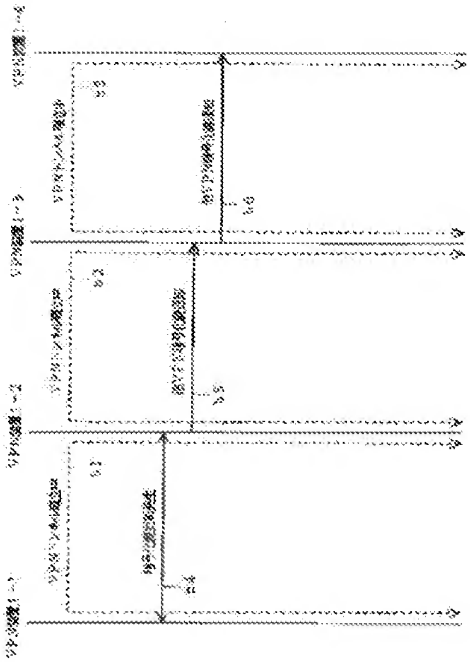
【図２】



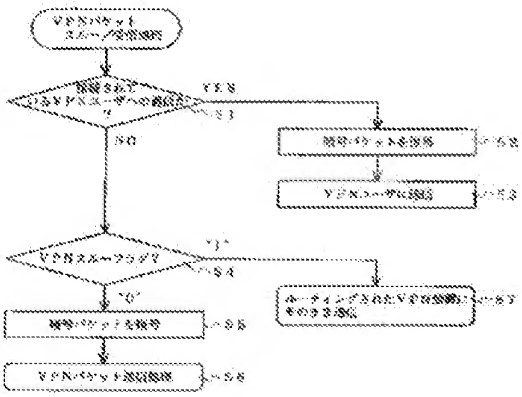
【図３】



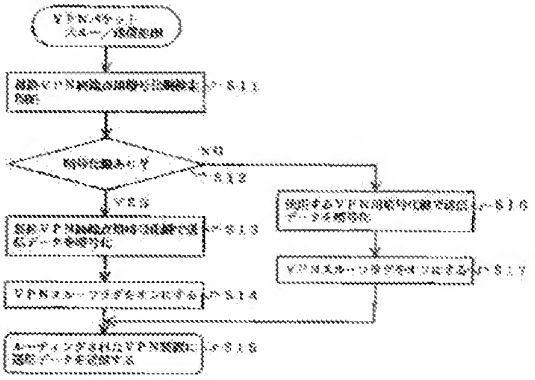
【図４】



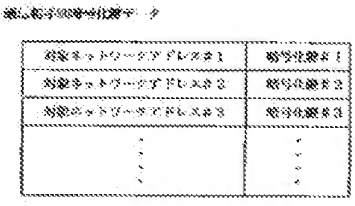
【図５】



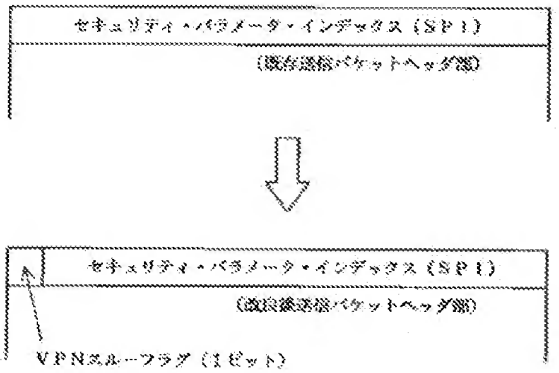
【図６】



【図７】



【図８】


セキュリティ・パラメータ・インデックス（ＳＰＩ）
セキュリティ・パラメータ・インデックス（ＳＰＩ）
ＶＰＮルーフラグ（１ビット）

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
O'Hare et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed more than three months after the U.S. filing date, AND after the mailing date of the first Office Action on the merits, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted a copy of the U.S. patent. Applicant submits herewith copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 18-1945 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 18-1945, under Order No. 104093-0002-105.

Dated: October 27, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 July 2001 (26.07.2001)

PCT

(10) International Publication Number
WO 01/54370 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/CA01/00056

(22) International Filing Date: 24 January 2001 (24.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/177,361 24 January 2000 (24.01.2000) US

(71) Applicant *(for all designated States except US)*: **THE UNIVERSITY OF MANITOBA** [CA/CA]; 202 Administration Building, Winnipeg, Manitoba R3L 1X3 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MCLEOD, Robert, D.** [CA/CA]; 37 Fifth Avenue, Winnipeg, Manitoba R2M 0A9 (CA). **BLIGHT, David, C.** [CA/CA]; 179 Edgewater Drive, Winnipeg, Manitoba R2J 2V4 (CA). **KRETSCHMANN, Steven, R.** [CA/CA]; 20-117 Bryce Street, Winnipeg, Manitoba R3L 1X3 (CA).

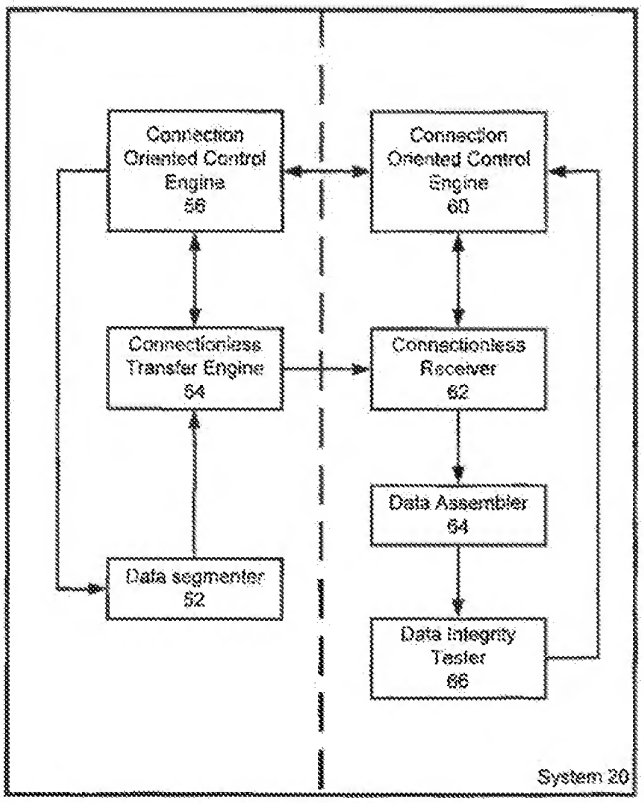
(74) Agents: **KINSMAN, L., Anne** et al.; Borden Ladner Gervais LLP, 1000-60 Queen Street, Ottawa, Ontario K1P 5Y7 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR SEGMENTED FILE TRANSFER



(57) Abstract: An architecture for improving the waiting time to download documents from the Internet and a set of methods are disclosed. A methodology is disclosed to improve download time from a number of sites containing component data denoted component based downloading (CBD). The components are downloaded autonomously and reassembled at the client site. A methodology is disclosed for downloading large files using an application denoted file segment transfer protocol (FSTP). FSTP is an application which sends data over UDP and provides its own error control and retransmission. Transfer rates and parameters such as packet size which effect file transfer latency can either be pre-selected or determined dynamically. A second architecture is disclosed which is denoted Distributed File Transfer (DFT). DFT illustrates a more automated approach to file size and server load determination procedures.

WO 01/54370 A2

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR SEGMENTED FILE TRANSFER

FIELD OF THE INVENTION

The present invention relates generally to data transfer via a telecommunication system. More particularly, the present invention relates to a method and system for segmented file transfer over a communications network, such as the Internet.

BACKGROUND OF THE INVENTION

The Internet has seen tremendous growth within the last few years. One of the main reasons for its popularity is quick and easy access to a wide variety of data from remote locations. The size of the data varies extensively. It might be a small web page, a relatively large multimedia file, a large video file or an extremely large archive (e.g., a new version of Netscape). In spite of these capabilities, Internet users tend to complain about the time that they waste sitting behind their computers, waiting for data. In other words, for a typical Internet user, latency is a big concern. Latency comes from different sources. For instance, if a server is overloaded or has a slow disk, it imposes a considerable delay before processing a request. Or, if a user's computer does not quickly parse the packets being received and process them, further delay is added.

The latency caused by a server or client can be largely eliminated by using a more powerful computer, more memory, or a faster disk. The main portion of the latency perceived by an Internet user is caused by the network itself. Some sources of this delay are intrinsic to the network infrastructure, namely, propagation and transmission delays. Fortunately, many Internet users presently have access to a reasonably high-bandwidth Internet connection. Other sources of delay are due to network congestion and router delays (the buffering & processing time involved for routing each packet). Yet another source of latency is due to the design/implementation of the Internet protocols themselves; for instance, the delay incurred for retransmission of a lost packet, while using a sliding-window flow control mechanism. These protocols are designed to best match particular network characteristics with the type or size of the data to be transmitted. Therefore, with

the evolving nature of the Internet, the protocols are modified occasionally in order to optimize performance.

Many modifications to the existing protocols, mostly of HyperText Transfer Protocol (HTTP), have been proposed in the literature to reduce latency. Some of them have been already implemented on the Internet. These include pre-fetching web pages the user is likely to access next, while browsing the current displayed page; using multiple Transmission Control Protocol (TCP) connections to the server, currently used by web browsers that comply with HTTP1.1; and using mirror servers (i.e.; spreading the workload among a cluster of servers rather than a single machine handling the HTTP requests).

Current file transfer protocols on the Internet are primarily based on using TCP running on the Internet Protocol (IP). TCP was designed for operation over IP, and thus it does not assume that the underlying network service is reliable. TCP provides a connection oriented service, which requires that the two parties communicating with each other progress through the phases of establishing a connection, transferring data, and releasing the connection. To achieve error free connections, TCP implements a selective Automatic Repeat reQuest (ARQ) technique, whereby repeated packets are requested when needed, through the use of a positive acknowledgement system. Additionally TCP implements congestion control by identifying congestion through packet loss monitoring. TCP then minimizes congestion by controlling the rate at which information enters the network through a congestion window.

TCP was defined in the early eighties when the transmission medium was a communication bottleneck. (There have been numerous modifications to enhance the performance of TCP, such as "selective acknowledgement", "window scale option", "round-trip time measurement", and "protection against wrapped sequence numbers".) Today, the emerging use of high-speed networks, fiber optic links, and powerful routers, has dramatically reduced the number of corrupted or lost packets in the Internet. This has made the existing transfer protocol redundant and slow in some cases, due to their assumption of a very unreliable network layer. TCP is the most widely used transport protocol on the Internet, although somewhat mismatched with the speed and reliability of gigabit class networks. This mismatch is mainly due to TCP's use of a sliding-window mechanism and a slow start procedure to ensure a reliable virtual connection. Slowness of TCP has the motivation for designing faster application protocols. This has been achieved

EX1009, Page 1257

as a trade off between speed and loss of data integrity -i.e., no guarantee that the user receives all the packets. For example, TFTP (Trivial File Transfer Protocol) uses User Datagram Protocol (UDP) as its transport-level service to move files around with no reliability guarantee. Though TFTP is acceptable on a small LAN, or subnet, where data can be reliably delivered it is not feasible in the internet as a whole, where there is substantial reliability on a per packet basis but there is still no guarantee that the data will arrive in order.

File transfer across a network that utilizes TCP as the transport layer protocol is carried out after a bi-directional connection is made between the two parties. The TCP connection is considered reliable because TCP guarantees that the data is provided to the application layer in order and without error. TCP gives each connection a randomly assigned long (32 bit) sequence of numbers as an identifier to allow a terminal to distinguish between multiple TCP sessions. In essence each TCP connection, when it is created, is assigned one number that it is identified by. Because there are a large number of possible identifiers the probability that two sessions on a single system will have the same identifier is small. To transfer data, TCP provides a sliding window mechanism to track packets, and to assist in reassembling them in correct order for the application layer. To transmit data, TCP requires the sender to fragment the data into segments, which are then encapsulated in a Transport Protocol Data Unit (TPDU). The TPDU has a header containing information about the source, the destination, the session ID, and several other factors. The TPDU is transmitted either upon receipt of a push command from the application layer, or when a counter expires. A window, the sliding window, is defined and a number of TPDUs are transmitted. The receiver sends an acknowledgement (ACK) for each TPDU that is received without error. When the earliest TPDU in the window is acknowledged then the window slides to allow another TPDU to be transmitted. If an ACK is not received for a TPDU within a set time, or before a TPDU near the end of the window is transmitted, then the TPDU is resent. Though this does provide for the arrival of all the TPDUs, it also introduces the unnecessary retransmission of TPDUs. When a TPDU is received, but the ACK is lost in transmission a new copy of the TPDU is sent to the receiver, which them discards the TPDU and sends another ACK, which results in unnecessary traffic. Upon receiving all the TPDUs that constitute the data being transmitted, TCP provides the completed data to the application layer. This allows TCP to ensure that the data has arrived, and is presented in order without error. TCP was

designed to be robust in an unreliable environment, and as a result has a high overhead in simple file transfers. One of the most widely used file transfer application programs on the Internet is File Transfer Protocol (FTP). However, because FTP relies on TCP transport layer protocols, it is inefficient in moving large data sets in a timely manner due to the overhead required to implement and process acknowledgements and error correction.

Different approaches have been taken to overcome the inefficiencies of FTP for file transfer. For example, Sun Microsystems, Inc. has designed a web network file system (WebNFS™) for sharing files over the Internet. WebNFS™ is an update of Sun's open standard NFS ™ protocol, which allows client systems to mount partitions located on a server. Transfer of files can then be accomplished through the use of standard copy commands. Additionally both WebNFS ™ and NFS ™ allow transparent access to the data on the shared partition, whereby a user can execute applications from the shared partition, and otherwise act as if that partition was a part of their physical machine. NFS™ is typically only used on local networks, due to the requirement of reliability and high overhead introduced on larger networks. WebNFS™ still uses TCP because of the generally unreliable nature of the Internet, compared to local networks.

In addition there are several proprietary protocols for file transfer that are based on the UDP where the file transfer application is responsible for the reliable transfer of data. UDP itself is a connectionless unreliable transport protocol. UDP relies upon the either network, or the application layer to ensure that messages are transmitted correctly. UDP does have a header, but it is minimal in nature to reduce overhead. UDP was originally designed for short communications where the overhead of establishing a TCP connection would be considered prohibitive. One common use for UDP is in requests to Domain Name Servers (DNS). A DNS query typically provides an alphanumeric string, and the response is a numeric address associated with the alphanumeric string. These requests are short and bursty in nature and thus establishing a connection-oriented session is not needed. If the user does not receive a response to the DNS query the query can be re-issued. UDP relies upon a reliable network infrastructure, whereas TCP assumes an unreliable network. Because traditionally UDP requests were only sent over a short topological distance the network was considered reliable.

Several proprietary transfer techniques have been developed using UDP, the most prominent of them being developed for use in RealAudio™ and RealVideo™ applications.

EX1009, Page 1259

In these applications a server segments the data into TPDUs based on UDP, and transmits them to the user. The packets arrive out of order due to the unreliable nature of the Internet. To accommodate the out of order nature of the data, a buffer is employed by the client to allow the data be reconstructed in order. Occasionally packets do not arrive, or do not arrive before they are needed, and the missing packet is skipped in the presentation of data. The listener, or viewer, does not notice the missing data, and thus to the end user the system has low overhead, and through the use of a buffer it ensures that the data is presented in order. Unfortunately, these applications do not have a method of ensuring that a packet is delivered, making them as unacceptable in applications where data integrity is important.

It is also well known that file transfer mechanisms can be distributed over a number of servers. Typically this is done through the use of mirrored servers. To ensure data availability, in the face of either network outage, high demand, or other such problem, many servers on the Internet contain copies of the same data set. Because the standard FTP application has the ability to resume a transfer that had been previously terminated it is possible, if a group of mirror servers are known, to have an FTP client concurrently download different segments of the same file from different servers, to reduce the bandwidth limitations incurred on a busy server. This segmenting technique is purely dependent upon the client, and the client performs the re-assembly of the transferred file. Effective architectures for efficiently transferring large data sets however require network and server load performance metrics to be effective.

Typically, a number of servers can be joined together in a load balancing arrangement, so that in the event of heavy demand the demand is spread among a number of servers. In common load balancing arrangements all client requests are routed to a load-balancing server which determines which server the client request should be routed to. There are a number of techniques that can be applied, but the most efficient is a load monitoring technique, where the load balancing server directs the client request to the server with the least load. U.S. Patent No. 6,078,960 to Ballard, entitled "Client-Side Load-Balancing in Client Server Network", discloses a method of retrieving a file from a plurality of servers without interacting with a load balancing server. The problem of a load-balancing server is that since all requests are routed through a central server there is a single point of failure at the load-balancing server. Ballard discloses a method where the client itself determines the server with the lowest load and directs its transfer to that

EX1009, Page 1260

server. This method requires the use of a local load-balancing list that contains information on servers, including the share of the load that the server should carry, and optionally contains information about the load carried by each server. This information is obtained from one of the servers. The client then uses the list to select a server with the most excess capacity, and begins the transfer with that server. There are protocols available for events such as the unavailability of a selected server that are also disclosed.

U.S. Patent No. 6,085,251 to Fabozzi III, entitled "Implementing a Parallel File Transfer Protocol", discloses a method of transferring a file to a client from a server. The method disclosed by Fabozzi requires segmenting the file, creating a log to aid in the reconstruction of the segmented file, transferring the log to the client, and then having the client request each of the segments in different file transfer sessions and reconstruct the file upon receipt of all the segments. This method seeks to overcome the problems that may arise with a sliding window, by creating multiple sliding windows, and letting a few sliding windows do the transfer. This method of multiply accessing a file does introduce efficiencies, and is often limited either by bandwidth restrictions at a single server or by restrictions that servers impose on multiple logins from a single client. Additionally there is a point of diminishing returns, where the overhead of the different TCP sessions becomes more of a burden on the transfer than the additional session provides in throughput.

It is, therefore, desirable to provide a method and system for transferring files, particularly large files, over the Internet that provide reliability and speed without high overhead.

SUMMARY OF THE INVENTION

It is an object of the present invention to obviate or mitigate at least one disadvantage of previous systems and methods for file transfer. It is a particular object of the present invention to improve the performance of Internet-based applications that require moving data from one or more servers over the Internet, moving data between clients and servers, moving data between peers in a peer-to-peer network, and moving data between cache appliances, in a single or multiple server environment.

In a first aspect, the present invention provides a method for transmitting data to a client in a distributed network environment. This transmission method begins by

EX1009, Page 1261

establishing a control channel to a client. This control channel optionally employs a connection-oriented protocol, such as TCP. The data to be transmitted to the client is then segmented into data segments, and the data segments are transmitted to the client using a connectionless protocol, such as UDP. In a presently preferred embodiment, a sequence number is attached to each data segment prior to transmission. Repeat requests, requesting retransmission of any erred data segments are received over the control channel. To improve performance, an inter-packet transmission delay can also be included.

In a further aspect, there is provided a method for receiving a data file in a distributed network environment. The reception method begins by establishing a control channel to a server. This control channel optionally employs a connection-oriented protocol, such as TCP. Data file segments, transmitted from the server, are received using a connectionless protocol, such as UDP. A data file is assembled from the received data file segments, typically by ordering the segments by their sequence numbers, or through supplemental control information. If the assembled data file contains erred segments, a request for transmission of the erred segments is made over the control channel.

In yet a further aspect there is provided a method for transmitting a data file to a client in a distributed network environment. The method begins by establishing control channels from a plurality of servers to a client. These control channels optionally employ a connection-oriented protocol, such as TCP. The data file is divided into components on the plurality of servers, and at each of the plurality of servers, the components are segmented into data segments to be transmitted to the client. The data segments are then transmitted to the client, in parallel, using a connectionless protocol, such as UDP. A repeat request, requesting retransmission of erred data segments, can be received over any of the control channels. Load balancing can be implemented to improve performance.

In yet another aspect, there is provided a file transfer system for transmitting a data file to a client in a distributed network environment. The file transfer system includes a data segmenter for dividing a data file into components on a plurality of servers and for segmenting the components into data segments to be transmitted to a client. A connectionless transfer engine, in communication with the data segmenter, transmits, in parallel, the data segments to the client using a connectionless protocol. Finally, control engine, in communication with the connectionless transfer engine, can establish control channels from the plurality of servers to the client, and can receive, over at least one of the control channels, a repeat request requesting retransmission of erred data segments. The

control engine optionally includes a connection oriented control engine, which optionally employs a connection-oriented protocol to establish a control channel.

At the reception side, there is also provided a file transfer system for receiving a data file in a distributed network environment. This receiving system includes a control engine that establishes a control channel to a server. The control engine optionally includes a connection oriented control engine, which optionally employs a connection-oriented protocol to establish a control channel. A connectionless receiver, in communication with the connection-oriented control engine, receives data file segments transmitted from the server using a connectionless protocol. While a data assembler, in communication with the connectionless receiver, assembles a data file from the received data file segments. A data integrity tester, in communication with the data assembler, can then determine if the assembled data file includes erred segments, and can relay to the connection-oriented control engine a request for transmission of the erred segments.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described, by way of example only, with reference to the attached figures, wherein:

Fig. 1 is a block diagram of a communications system according to the present invention;

Fig. 2 is a block diagram of the logical components of a file transfer system according to the present invention;

Fig. 3 is a flow chart of the component-based download method of the present invention;

Fig. 4 is a flow chart of the file segment transfer protocol method of the present invention;

Fig. 5 is a flow chart of the combined component-based download and file segment transfer protocol method of the present invention; and

Fig. 6 is a flow chart of the distributed file transfer method of the present invention.

EX1009, Page 1263

DETAILED DESCRIPTION

Generally, the present invention provides a method and system for transferring data files over the Internet, or other distributed communications network. Ideally, the present invention results in improved data transmission performance as viewed from an individual user's perspective. First, a distributed approach for downloading files, referred to herein as Component-Based Download (CBD), is introduced. Second, an application protocol for more efficient and reliable transfer of large data sets, referred to herein as File Segment Transfer Protocol (FSTP), is described. Third, the combination of CBD and FSTP, referred to herein as CBD-FSTP, is described. Fourth, a file transfer architecture, referred to herein as Distributed File Transfer (DFT) architecture, is described. DFT uses standard file transfer protocols to adaptively download segments of replicated files stored on distributed servers. Finally, the results of several simulations and tests are presented to demonstrate the advantages of the proposed method and system.

The following description will focus on the presently preferred embodiment of the present invention, which is operative in an Internet-connected environment, including, for example, machines operating under a Microsoft® Windows or UNIX® environment and connected to an open network, such as the Internet. The present invention is not, however, limited to any particular one environment. Instead, as will be understood by those of skill in the art, the system and methods described herein can be advantageously applied to a variety of system and application software, operating on a variety of platforms, including the Macintosh® operating system, and the like, and can apply to systems implemented on any wide area network (WAN), or local area network (LAN).

Referring to **Fig. 1**, a block diagram of the system of the present invention is shown, and generally referenced at **20**. System **20** generally consists of client(s) **24**, servers **28**, **32**, and **34**, interconnected via the Internet **36**. Clients **24** are typically embodied on a general purpose computer, such as an IBM PC-compatible personal computer, operating as stand-alone machines or interconnected on a LAN. For example, in a LAN based environment, client can consist of a central processor, a main memory, such as conventional random access memory (RAM), an input/output controller, a keyboard, a pointing device, such as a mouse, track ball, track pad, pen device or the like, a display or screen device, a mass storage device, such as a hard drive, floppy drive, optical disk, flash memory or the like, a network interface card or controller, such as an Ethernet card, and a

EX1009, Page 1264

modem. Client 24 communicates with other systems via the network interface card and/or modem. A variety of optional input/output devices (not illustrated) can also be attached to client 24, including printers, slide output devices, plotters, etc. Typically, a computer software system is provided for directing the operation of client 24. The software system is stored in memory, and on the mass storage device, and generally includes a kernel, or operating system (OS), and a windows shell. The OS and windows shell can, for example, be provided by Microsoft® Windows 98, Microsoft® Windows NT, IBM OS/2®, Macintosh® OS, Linux, or other similar application. One or more application programs, such as client application software, can be loaded for execution by client 24. In a presently preferred embodiment, client application software includes a web browser, such as Microsoft Internet Explorer™ or Netscape Navigator™ browser software that communicates with the Internet through a communication layer or driver, such as a Winsock driver. The software system typically further includes a user interface, preferably a graphical user interface (GUI), for receiving and displaying user inputs, commands, and data and outputs resulting from operation of the operating system and the application programs.

Servers 28, 32 and 34 can each consist of one or more conventional computers having a Pentium™ class, or better, central processing unit, such as manufactured by Intel™ Corporation, Santa Clara, CA, or other similar processing unit. Each of the servers can be provided with peripheral components and software components as described above with respect to client 24. Servers 28, 32 and 34 can be attached to large mass storage devices, such as a RAID storage device. Those of skill in the art will understand that servers 28, 32 and 34 can be distributed in various locales and can communicate with each other over dedicated lines, or over Internet 36.

The logical components of the file transfer system 20 are shown in Fig. 2. The logical components are embodied in appropriate application software, as is well known to those of skill in the art. On the transmitting side, file transfer system 20 consists of a data segmenter 52 for segmenting a data file into data segments to be transmitted to a client. A connectionless transfer engine 54 is in communication with the data segmenter 52. The connectionless transfer engine 54 transmits the data segments to the client using a connectionless protocol, such as UDP. A connection-oriented control engine 56, in communication with the connectionless transfer engine 54, establishes control channel(s) to the client using a connection-oriented protocol, such as TCP, and can receive repeat

EX1009, Page 1265

transmission requests for erred data segments. As used herein, an erred data segment means missing/lost or corrupt data segments.

On the receiver side, system **20** consists of a further connection-oriented control engine **60** that communicates with the connection-oriented control engine **56** to establish a control channel to the server(s) using a connection-oriented protocol. A connectionless receiver **62**, in communication with the connection-oriented control engine **60** and the connectionless transfer engine **54**, receives data file segments transmitted from the server using a connectionless protocol. A data assembler **64**, in communication with the connectionless receiver **62**, assembles a data file from the received data file segments. A data integrity tester **66**, in communication with the data assembler **64**, determines if the assembled data file includes erred segments, and relays a request for retransmission to the connection-oriented control engine **60** which can send the request to the connection-oriented control engine **56**.

As described below, the control engine of the system **20** need not be connection oriented. It is possible to implement a system, within the scope of the present invention, that uses a connectionless protocol to establish a control channel. This control channel need only be bi-directional to facilitate communication. Connection oriented channels introduce benefits, such as guaranteed arrival of control information, that though beneficial are not essential to the operation of the present invention.

The operation of system **20** and the method of the present invention will now be described with reference to **Figs. 1 - 6**. The following description assumes that the client **24** is connected to Internet **36** and has access to the servers **28, 32** and **34** for the purposes of file download.

Referring to **Fig. 3**, using CBD, a file to be downloaded is split into components, or clusters, at step **200**. The number of components is determined by the number of available servers **28, 32** and **34**, while the size of the components can be determined by the relative connection speeds, server speeds, or other suitable factors. Ideally, the component sizes are chosen such that each component can be downloaded to the client **24** in approximately the same time. Each component is then placed on a different server at step **202**. When a user, situated at client **24**, attempts to download the file, parallel, or concurrent, connections are established, at step **204**, between the client **24** and the servers **28, 32** and **34** maintaining the file components. All the components are then downloaded simultaneously at step **206**. At the client side, after the download is complete, the

EX1009, Page 1266

components on the client machine are appended to each other at step 208, thereby reconstituting the original file.

In other words, with CBD, a file is first divided into several components or clusters and put on different servers. To initiate the download of the file cluster, parallel FTP sessions are established between the user and the respective servers and files are downloaded to the user's side in a parallel fashion. On the user's side, each FTP session is terminated after the respective component is completely downloaded. This leads to a faster transmission rate, and thus a considerably shorter latency perceived by the user.

CBD is inherently fault tolerant. There are occasions in which a server may go down, or a router starts discarding the packets when buffers are full. This means file components may no longer be accessible if they reside on that part of the sub-network. This problem can be addressed by resorting to a replication scheme. Depending on the nature of the file cluster, and the network's environment, several simple replication schemes can be implemented. One is to put the whole file cluster on a backup server. The other is to divide the file into replicated components and spread them among the servers.

In order to substantiate the assumption that CBD is faster than the conventional approach, a series of preliminary experimental measurements were carried out. In these experiments the CBD paradigm used FTP as the file transfer protocol (FTP was chosen, because it is the de facto protocol for downloading files through the Internet), the respective latencies were measured, and compared to the latencies while using the conventional method. To do that, several files, located on different FTP servers, were downloaded by establishing simultaneous FTP sessions (i.e.: concurrently). Then, the same files were downloaded, by opening FTP sessions with those servers one after another (i.e.: sequentially). Measurements were performed and the results are discussed in detail below. Extensive experimental results were collected over campus type LANs, modems, and wireless LANs supporting the wireless protocol 802.11. Three different FTP servers at remote locations were chosen: ftp.microsoft.com in USA, ftp.unix.hensa.ac.uk in England, and ftp.dti.ad.jp at Japan. On each server, relatively large files were selected for download (2, 2 & 4.7 Mbytes, respectively). A UNIX/SUN workstation connected to a 100BaseT LAN was used as the client machine, housed at the University of Manitoba. The time it takes to download the files to the local machine was measured in two ways: (1) The three files were consecutively downloaded, and the latencies incurred in downloading each file was measured. The latencies were added, which gave us the total latency. (2) The same

EX1009, Page 1267

three files were downloaded, this time by establishing three simultaneous FTP sessions with those servers. We measured the time interval between initiation of the first FTP session and termination of the last session. We ran the FTP sessions simultaneously by spawning parallel threads for each one. Intuitively, this time is the latency perceived by the user while using the CBD approach. In order to be able to repeat the experiment for a reasonable number of times, a Java application was created to automate the process of opening the FTP sessions, measuring and collecting the latencies. In the experiments, several contingencies that might occur in a real-life situation were covered. To compensate for the effect of variations of the traffic load on the network, experiments were repeated at various hours of the day on different days of the week. We repeated our experiments 70 times to get a reliable result. According to our measurements, the average time for downloading files through the component-based approach was 13.5 seconds, as opposed to conventional approach delay with an average of 25.8 seconds. These results clearly illustrated the potential to improve the performance of a network by using CBD for large files.

In a second test, the total latencies for each scenario were calculated as follows: In concurrent download, the perceived latency is equal to the greatest value of latencies measured for each download. In sequential download, the perceived latency is equal to the sum of latencies measured for each download. The experiments were performed on 4 different environments: 100BaseT LAN, 10BaseT LAN, 802.11 wireless LAN, and with a dialup modem. First, three files with total size of 4.5 megabytes; second, three larger files with total size of 26 megabytes; and third, five files with total size of 9 megabytes were downloaded.

The results clearly illustrate the potential to improve the performance of a network by using CBD for large files. Latency can be reduced to less than 50% compared to when downloading in conventional way. These results are summarized in **Table 1**.

Table 1: Relative Latencies for CBD compared to traditional FTP

Size/No. of Files	Environment			
	100BaseT	10BaseT	802.11	Dial up modem
3 Files (4.5 Meg)	0.48	0.47	0.46	1.06
3 Files (26 Meg)	0.45	0.39	0.74	-
5 Files (9 Meg)	0.34	-	0.32	-

EX1009, Page 1268

In this table relative latencies (the latency for CBD method divided by the latency for sequential download) are presented. This method can be extended using various numbers of TCP connections, larger files, and various access methods to determine an optimal range of TCP connections, which gives us the best latency. Opening more TCP sockets enhances the latency, but this would also introduce more network and processing overhead.

Referring to **Fig. 4**, to further improve the latency, a novel application-level protocol, FSTP, is shown. In this protocol a TCP socket connection is established at step **300**. The TCP socket connection forms the control channel and is used for sending commands. Concurrently with step **300**, or separately, one or more UDP socket connections are established at step **302** to enable data transmission. By contrast, in FTP, which is the current dominant protocol for transferring data, TCP sockets are used for both the control and data channels. At step **304**, the desired data file is transmitted as data units, such as datagrams or packets of predetermined size, as is well known to those of skill in the art. Since UDP does not provide a reliable connection, the integrity of the data transfer is checked in the application level at step **306**. FSTP takes advantage of the more reliable network infrastructure currently available in the Internet, as compared to when TCP was first introduced. Preliminary tests show that FSTP transmits data much faster than FTP. Experimental results have been obtained for campus LANs, wireless LANs, and traditional telephone modems and cable modems. In the worst case, FSTP performs no worse that FTP, and in the best cases to date with experiments over broadband networks typical file transfer speed-up improvements are on the order of 500-800%.

To better understand the FSTP, the network connections used for an FTP session are explained and compared to the transport layer connections used in the FSTP protocol. FTP uses two TCP connections, one for exchanging command/control packets, and the other one for the data itself. Basically, FTP protocol is not concerned about retrieving the missing/corrupted packets. The job of providing a reliable network connection is delegated to the transfer layer protocol, i.e., TCP. TCP ensures the integrity of the data by checking the incoming packets, and asking the other side for retransmission of the erroneous/missing packets.

FSTP operates significantly differently from FTP. Although there is still a TCP network connection to send command/requests to the server, all of the data is transferred

EX1009, Page 1269

via UDP packets. UDP here affords simple access to the Internet Protocol (IP) layer. Sending data over UDP does not bind us to restrained performance of a TCP connection's sliding window flow control. Another benefit in using UDP packets is that there is less processing overhead compared to a TCP connection. However, since UDP only provides a datagram service, the necessary functionality for data consistency is provided in another level. This task is performed in the application level (i.e., by FSTP itself). In a presently preferred embodiment, FSTP attaches a unique sequence or tag number to each packet. On the client side, after FSTP receives all of the data packets in a stream, it looks for missing/corrupted packets. The missing packets may be logged during the transfer or determined after the transfer is completed. If found, the FSTP client sends a request for retransmission of the missing packets back to the FSTP server. The server retrieves the missing parts of the file from its local disk or memory, and sends them again to the client. This loop continues until the data is completely transferred to the user.

Clearly, transmitting packets at the maximum possible speed can result in many of the packets getting lost in transit due to a smaller maintainable bandwidth over certain portions of the Internet and/or an inability of the client to process the incoming datagrams. To maintain a reasonably small percentage of packet loss, an inter-packet transmission delay can be added. Adding this delay results in a greater packet reception success rate (with respect to the number of packets transmitted), and results in fewer required retransmissions. Because the examination of received packets, generation of a retransmission requests, and processing of these request by the server takes of time, the perceived latency to the user will actually be less with the use of the appropriate inter-packet transmission delay for a pre- chosen packet size. Adaptive inter-packet transmission timing scheme will also work to minimize excessive network traffic.

To optimize throughput between the client and the server, FSTP can, for example, conduct a brief test where the server attempts to flood its connection with UDP packets destined for the client for a short time interval (under 1 second). The client counts the number of packets it received out of the total and, with the noted transmission time from the server, calculates an appropriate delay. For example, if the server sends 1000 packets in one second and the clients receives 100, we can speculate that if we transmit a packet every 10mS, we should be able to maintain a high packet reception success.

The presently preferred initialization steps a FSTP file transmission are: FSTP client opens up a TCP connection with the server for exchanging commands. The client

EX1009, Page 1270

receives a list of files and their respective sizes. The packet size is chosen by the user and this selection is forwarded to the server. The server begins the transmission timing test by sending UDP packets of the specified size to the client. After the test has completed, the server sends the client a message indicating the total transmission time for the test and the number of packets transmitted during the test. The client calculates an appropriate inter-packet transmission time and sets this transmission delay on the server. The client sends a "SEND" command by specifying the name of the file to be retrieved, taking note of the file's size from the previously acquired file listing.

Both the client and the server can calculate the number of bytes necessary for the packets' sequence numbers, or tags. It is necessary for the client to calculate this as well, so it will properly handle the format of the received packets without the server having to explicitly send a description of the format. This is possible because the client and server use the same program library to handle tag numbers. The server sends the file as a steam of UDP packets whose headers contain the file name and tag made of bytes to indicate the position of the data in the file. Other methods with less overhead can be used, such as after the stream of UDP packets has ended, the client generates a list of missing/corrupted packets and sends them in a retransmission request to the server; the server retransmits the requested packets in the same format as the original transmission; and this retransmission continues until all of the packets are received. To pinpoint the corrupted packets, the checksum capability of UDP protocol can be used. The current, experimental system attempts to establish an average maintainable data rate in packets per second (for a chosen packet size) and transmits the data from a single server to the client.

An alternative method would be for the server to adapt its rate and packet size in response to the client. The packet size is easily adjusted and is often optimal if near the maximum segment size of any of the intervening networks a packet would traverse from source to destination. For example, based on all experiments to date a packet size of 1500 bytes has been found to be near optimal. In addition the inter-packet transmission delay can be adapted using a simple feedback control increasing or decreasing the rate depending on the rate of packets received. If for example, if only 80% of the packets were being delivered the server can throttle back its transmission of packets into the network until a desirable reception rate is achieved.

To test the performance of FSTP and compare it with that of FTP, some preliminary measurements were performed. Three types of machines and network

EX1009, Page 1271

connections were chosen. The same file was downloaded, using FTP and then by FSTP. The time taken for each download was recorded and compared. From the results of the tests, when a 1500-byte IP packet size is used with FSTP transfers (as the optimum packet size), the transfer time range from approximately the same as FTP times to nine times faster. This is most likely because the FSTP transfers do not depend on acknowledgement for each packet, and are therefore not bound by round trip propagation delay over the network. The other fact derived from the test is that FSTP does not improve the latency when used in a low-bandwidth network connection (e.g., dialup modem). This is not surprising, because FSTP is basically designed based on the assumption of exploiting the large available bandwidth (which is exactly the shortcoming of FTP that uses TCP for transferring data). So, FSTP performs best, compared to FTP, when the two machines (client and server) are connected via a fast Internet connection, with a relatively high RTT (round trip time). **Table 2** shows the average transfer times for FTP and FSTP measured in seconds.

Table 2: Latencies for FTP and FSTP (seconds)

File Size	Environment(packet size)			
	FTP	FSTP(500)	FSTP(1000)	FSTP(1500)
(15 Meg)	192	38	21	19

A file was transferred from a remote machine (located at the University of Victoria) to a local machine (located at the University of Manitoba). The two machines were Sun Sparc™ workstations, running Solaris™ 5.6 and 5.7. They were connected via a high-speed connection. The measurements were repeated 5 times during a weekday afternoon, when the machines were busy running other processes and the Internet was being used by business and academic users. Three different packet sizes were used, 500, 1000, and 1500 bytes.

The method disclosed in the previous example used a TCP connection for the control channel, due to the inherent reliability of the TCP channel. Though this is advantageous in many circumstances it should be noted that the control channel need only be a bi-directional channel and does not absolutely require the benefits of a TCP channel. One embodiment of the present invention uses a connectionless protocol for the control channel and the transfer channel. This embodiment takes advantage of the lack of

EX1009, Page 1272

overhead to minimize traffic in the control channel. As segments arrive at the receiver they are reassembled as in the previous example. Upon receipt of the final segments a list of erred segments is prepared and sent out over a connectionless control channel, preferably using UDP. Upon receipt of the retransmission list the server(s) transfer the erred segments. If the transmitter does not receive one part of the retransmission list, then it will not be sent to the receiver. The receiver does not remove segments from the erred segment list until they have arrived intact. If segments do not arrive correctly, or do not arrive at all, in the second transmission, then they will be re-requested and the process will continue until all the segments have arrived.

Although good results have been achieved using FSTP (up to 900%), still more enhancements can be done on FSTP protocol, without affecting the basic concepts embodied within FSTP.

Referring to **Fig. 5**, to integrate the two concepts and achieve even a higher speed of data transmission, a distributed version of FSTP, namely CBD-FSTP, is shown. Under this distributed version, file components are stored on distributed servers and downloaded to the client **24** seamlessly over multiple FSTP connections. A file to be downloaded is split into components, or clusters, at step **200**, as described above. Each component is then placed on a different server at step **202**. When a user attempts to download the file, parallel, or concurrent, FSTP connections are established, at step **404**. As described above, a TCP socket connection is established with each server, and UDP socket connections are established for the data transmission. At step **410**, the segmented data file is transmitted as datagrams in parallel from each server to the client. At the client side, after this download is complete, the components on the client machine are re-sequenced at step **412** to reconstitute the original file. A check is made for missing and corrupt packets at step **414**, and transmission of any erred packets is requested at step **416**.

In this instance FSTP is used within the CBD architecture. This is a simple extension and illustrates the use of FSTP with a concurrent download environment. As expected, since file transfer delay is improved with either method, when combined further improvements are multiplicative.

To incorporate FSTP into the CBD paradigm, some modifications are applied to FSTP. The following features/changes are added to FSTP. An additional field is added to the FSTP header. This field represents the file component to which that packet is belonged.

Since in the CBD approach the client establishes parallel/concurrent connections to multiple servers. The client is implemented using threads. Each thread is responsible for maintaining connection (a TCP and UDP connection) with a participating server.

After the client sorts each component, it appends these components sequentially together to create the original file.

Initial tests with CBD-FSTP shows an even faster download time compared to using FSTP. Preliminary test results for CBD-FSTP connections to Victoria BC Canada, Regina SK Canada, and Edmonton AB Canada, from Winnipeg MB Canada, demonstrate the multiplicative speedup of both techniques. These results are illustrated in **Table 3**. These results illustrate the additional benefit that can be achieved using the FSTP protocol within a distributed file transfer application.

Table 3: Latency CBD-FSTP (seconds)

		Average Latency (sec)		
File Size	Num. of Servers	CBD-FSTP	FSTP	FTP
(20 Meg)	3	59	85	434
(40 Meg)	4	122	198	872

A novel load balancing method, namely DFT, can also be implemented in the system of the present invention. DFT utilizes a intermediate tier process to coordinate the selection of file servers and to maintain server status information. In the implementation of DFT each server has completely replicated data or files. The degree to which a server provides content is based on measurements made by the client. The client actively probes the connection to the server and monitors the file transfer process balancing the load as required during the download. DFT illustrates the role of active monitoring and the decision process involved in concurrently downloading files over the network. DFT is responsible for partitioning the file in terms of server performance and reassembling the file on the client side. DFT can be deployed with using either traditional FTP or the FSTP protocol disclosed here.

The Distributed File Transfer (DFT) architecture can further automate the process of downloading files from a number of servers. A current instance of DFT can allocate server resources according to their availability and utilization. Therefore, we obtain reliability, scalability and efficiency by making better use of all file servers in the Internet.

This approach makes all FTP servers that contain the same files a cluster of servers and distributes load among them.

The design concept of DFT is as follows: In order to switch among servers, a client connects to multiple file servers to download file components simultaneously. This approach like CBD improves the performance of file transfer in general. The client monitors all connections to file servers to detect failure and congestion problems. If some connection is broken, the DFT client has sufficient intelligence or means to decide which server it should switch to and switch to that server immediately and transparently. This is an improvement over CBD in terms of fault tolerance. Within the DFT architecture there is a Load Distributing Server (LDS). The LDS knows all file servers or can search for them so that it can provide a server list to a client. Thus, the LDS coordinates the load distribution among all servers allowing the client to focus on file transfer among a small set of servers. In the current implementation traditional FTP is used although FSTP can be used if the servers are replaced with FSTP servers.

Referring to **Fig. 6**, the working procedure for DFT is as follows: The DFT client sends a request to the LDS at step **500**. The LDS looks for servers that contains the target file. LDS provides the DFT client with a list of servers at step **502**. The DFT client tests the speed and availability of the servers at step **504**, and calculates the segment sizes for each server at step **506**. The DFT client then establishes multiple data links with those servers and downloads different segments from them at step **508**.

DFT achieves performance improvements by more intelligently selecting and monitoring the file transfer process. DFT initially estimates the server speed and network by issuing ping and/or FTP size commands. This establishes the size of the component to be downloaded from each participating server. Once the file transfer is in progress DFT monitors each concurrent connection and reallocates load as required. The present instance and example of DFT disclosed here utilizes FTP for downloading a 47 Mbyte file from 1 to 5 servers. File transfer speedup for this series of experiments resulted in throughput improvements which increased linearly from 600 Kbps to 1400 Kbps as the number of servers ranged from 1 to 5.

Using the method and system of the present invention a higher throughput is achieve simply by modifying the implementation of the existing application protocols to account for the inherent unreliable data transfer that would otherwise be seen transferring files directly over UDP. Higher throughput means faster data transfer, which leads to a

EX1009, Page 1275

shorter perceived latency by the user. This enhancement is achieved with more processing overhead and network cost. Fortunately, this is not a significant burden on new computers with ever-increasing processing power, cheaper memory, and fiber optic Gigabit links.

The above-described aspects of the invention are suited for transferring all types of files, and have been shown to reduce transfer times. These techniques have been shown to work on files of all sizes, though the improvements are most noticeable with larger files.

The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those of skill in the art without departing from the scope of the invention, which is defined solely by the claims appended hereto.

What is claimed is:

1. A method for transmitting data to a client in a distributed network environment, comprising:

(i) establishing a control channel;

(ii) segmenting the data into data segments to be transmitted to the client;

(iii) transmitting the data segments to the client using a connectionless protocol; and

(iv) receiving, over the control channel, a repeat request requesting retransmission of erred data segments.

2. The method according to claim 1, wherein the control channel is established using a connection-oriented protocol.

3. The method according to claim 2, wherein the control channel is established using Transmission Control Protocol.

4. The method according to claim 1, wherein the connectionless protocol is User Datagram Protocol.

5. The method according to claim 1, further including attaching a sequence number to each data segment prior to transmission.

6. The method according to claim 1, further including retransmitting the erred data segments using a connectionless protocol.

7. The method according to claim 1, wherein transmitting the data segments includes determining an inter-packet transmission delay.

8. A method for receiving a data file in a distributed network environment, comprising:

(i) establishing a control channel to a server;

(ii) receiving data file segments transmitted from the server using a connectionless protocol;

EX1009, Page 1277

(iii) assembling a data file from the received data file segments;

(iv) determining if the assembled data file contains erred segments; and

(v) requesting, over the control channel, transmission of the erred segments.

9. The method according to claim 8, wherein the control channel is established using a connection-oriented protocol.

10. The method according to claim 8, wherein assembling the data file includes assembling the data file segments in order of respective associated sequence numbers.

11. The method according to claim 8, wherein the determining if the assembled data file contains erred segments includes performing a checksum.

12. The method according to claim 8, wherein the determining if the assembled data file contains erred segments includes determining a sequence number for one of the expected data file segments is missing.

13. A method for transmitting a data file to a client in a distributed network environment, comprising:

(i) establishing control channels from a plurality of servers to a client using a connection-oriented protocol;

(ii) dividing a data file into components on the plurality of servers;

(iii) at each of the plurality of servers, segmenting the components into data segments to be transmitted to the client;

(iii) transmitting, in parallel, the data segments to the client using a connectionless protocol; and

(iv) receiving, over at least one of the control channels, a repeat request requesting retransmission of erred data segments.

14. The method according to claim 13, wherein the control channels are established using Transmission Control Protocol.

15. The method according to claim 13, wherein the connectionless protocol is User Datagram Protocol.

16. The method according to claim 13, further including attaching a sequence number to each data segment prior to transmission.

17. The method according to claim 13, further including retransmitting the erred data segments using a connectionless protocol.

18. The method according to claim 13, wherein transmitting the data segments includes determining an inter-packet transmission delay.

19. The method according to claim 13, further including balancing a transmission load between the plurality of servers in accordance with their respective performance metrics.

20. A file transfer system for transmitting a data file to a client in a distributed network environment, comprising:

a data segmenter for dividing a data file into components on a plurality of servers, and, at each of the plurality of servers, segmenting the components into data segments to be transmitted to a client;

a connectionless transfer engine, in communication with the data segmenter, for transmitting, in parallel, the data segments to the client using a connectionless protocol.; and

a control engine, in communication with the connectionless transfer engine, for establishing control channels from the plurality of servers to the client, and for receiving, over at least one of the control channels, a repeat request requesting retransmission of erred data segments.

21. A file transfer system according to claim 20, wherein the control engine includes a connection-oriented control engine.

22. A file transfer system for receiving a data file in a distributed network environment, comprising:

a control engine for establishing a control channel to a server;

a connectionless receiver, in communication with the connection-oriented control engine, for receiving data file segments transmitted from the server using a connectionless protocol;

a data assembler, in communication with the connectionless receiver, for assembling a data file from the received data file segments;

a data integrity tester, in communication with the data assembler, for determining if the assembled data file includes erred segments, for relaying to the connection-oriented control engine a request for transmission of the erred segments.

23. A file transfer system according to claim 22, wherein the control engine includes a connection-oriented control engine.

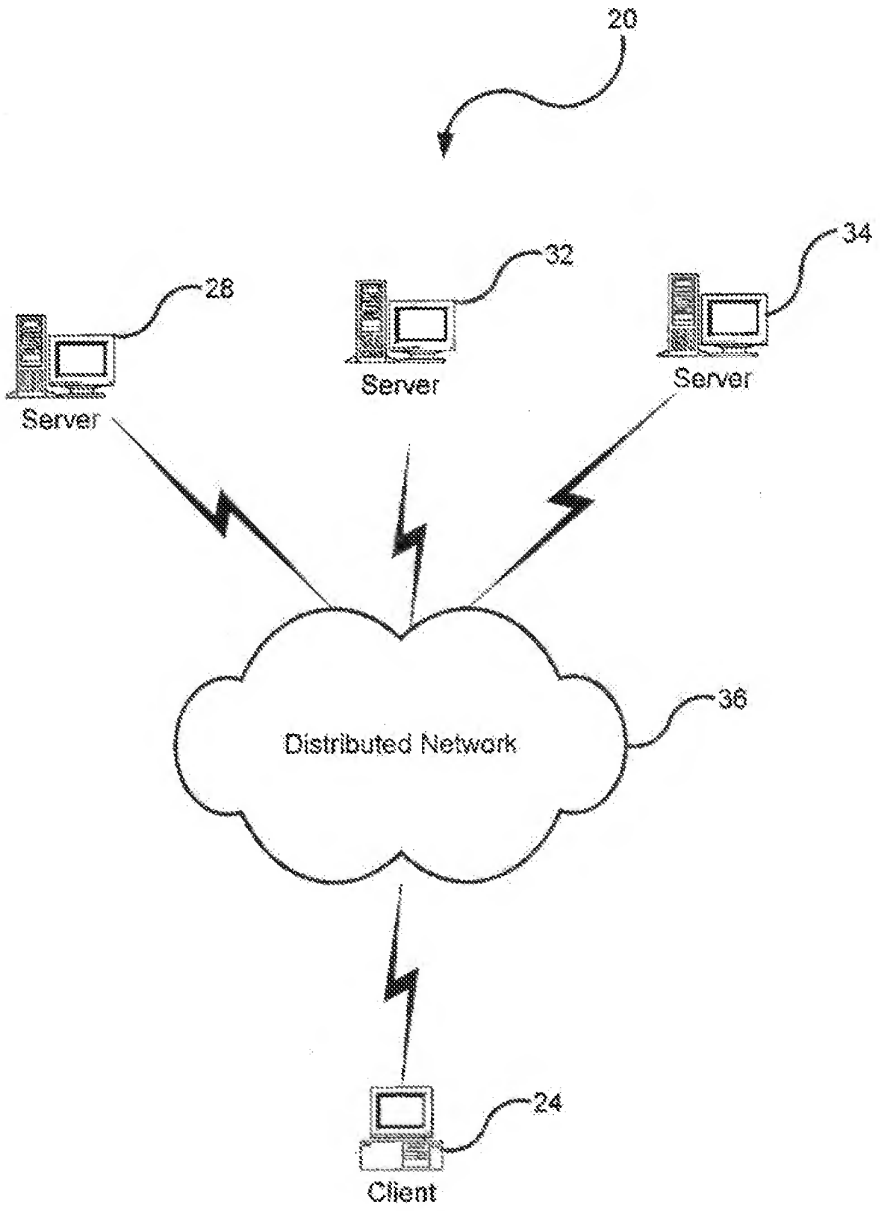

20
28
Server
32
Server
34
Server
Distributed Network
36
24
Client

Figure 1

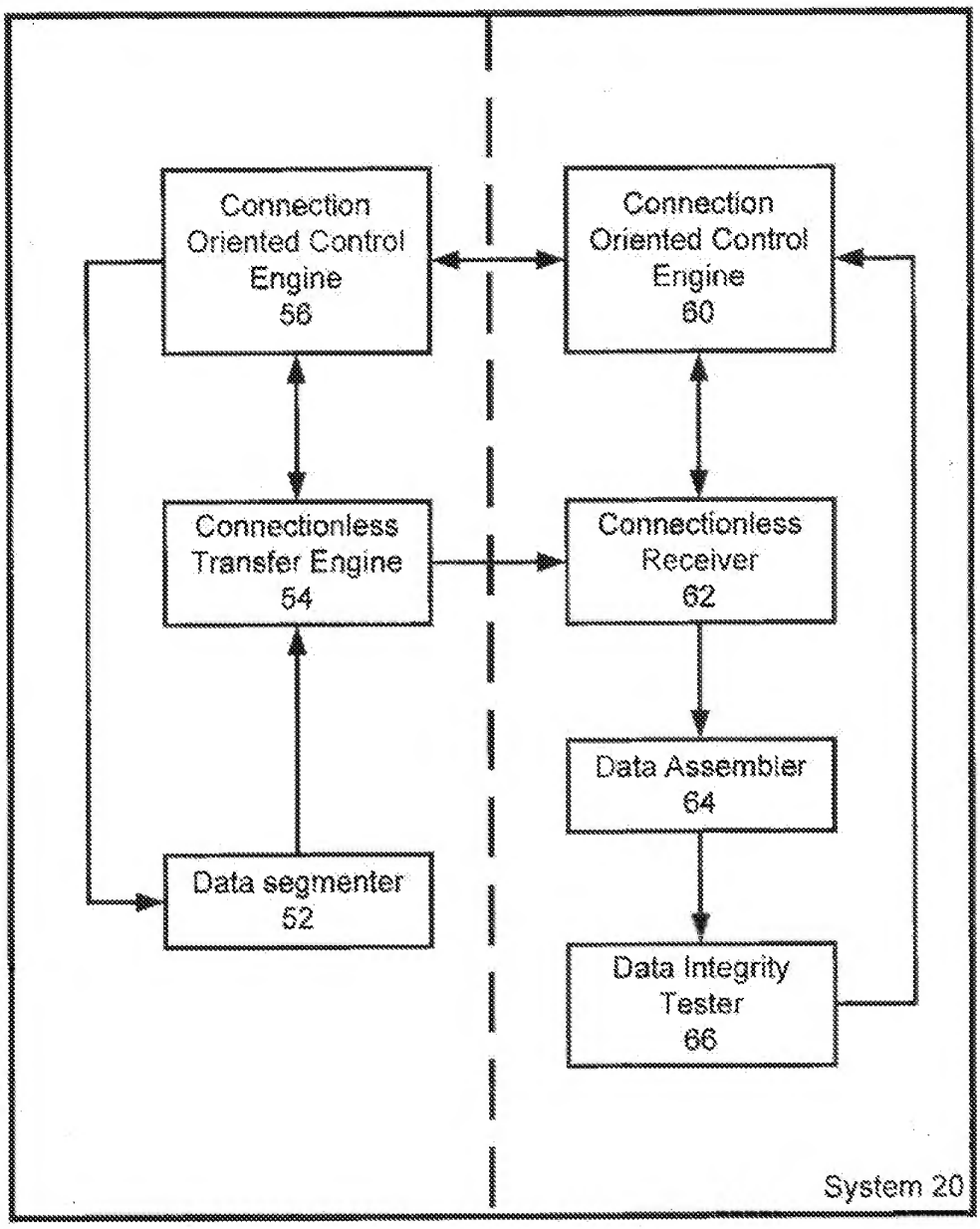

Connection Oriented Control Engine 56
Connection Oriented Control Engine 60
Connectionless Transfer Engine 54
Connectionless Receiver 62
Data Assembler 64
Data segmenter 52
Data Integrity Tester 66
System 20

Figure 2

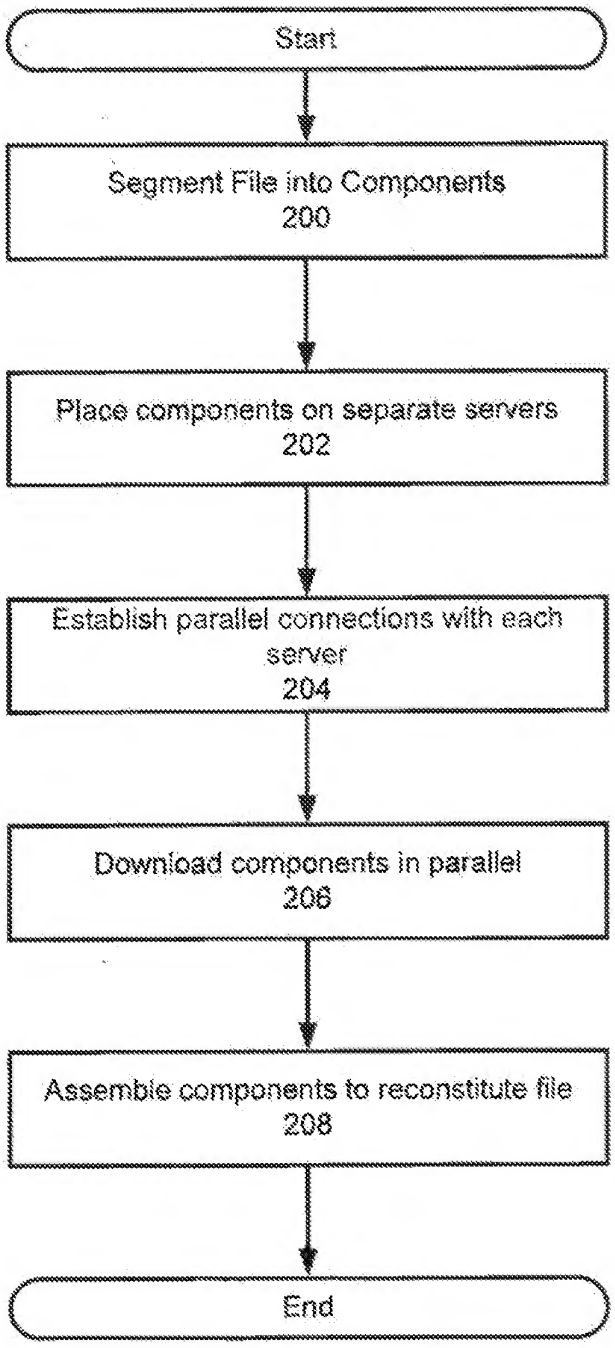

Start
Segment File into Components
200
Place components on separate servers
202
Establish parallel connections with each server
204
Download components in parallel
206
Assemble components to reconstitute file
208
End

Figure 3

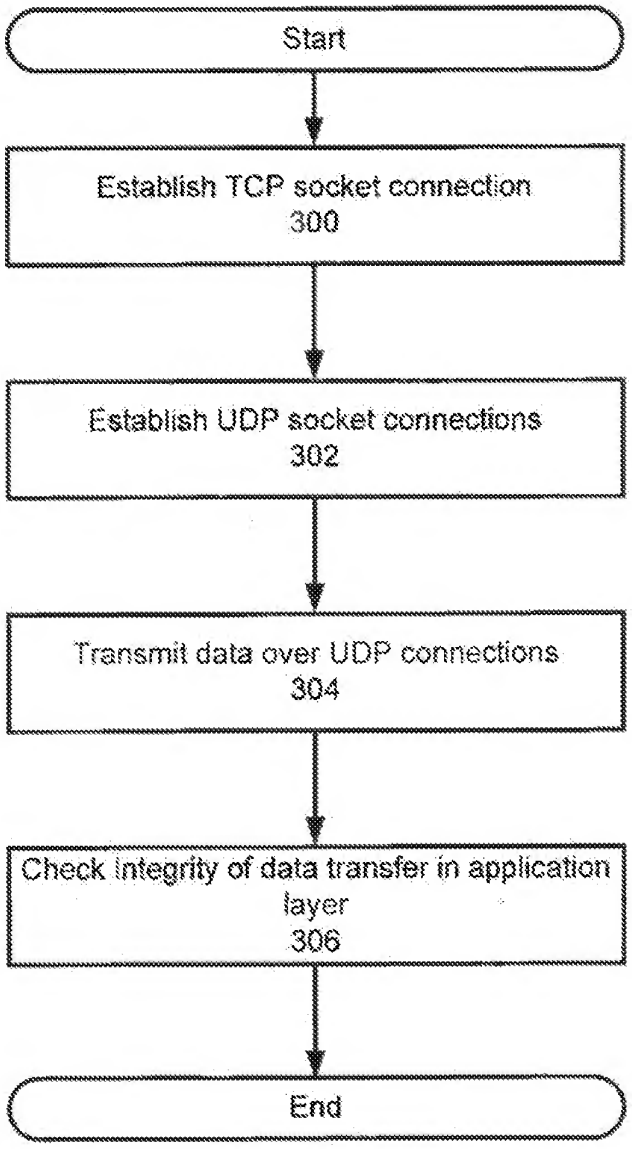

Start
Establish TCP socket connection
300
Establish UDP socket connections
302
Transmit data over UDP connections
304
Check integrity of data transfer in application layer
306
End

Figure 4

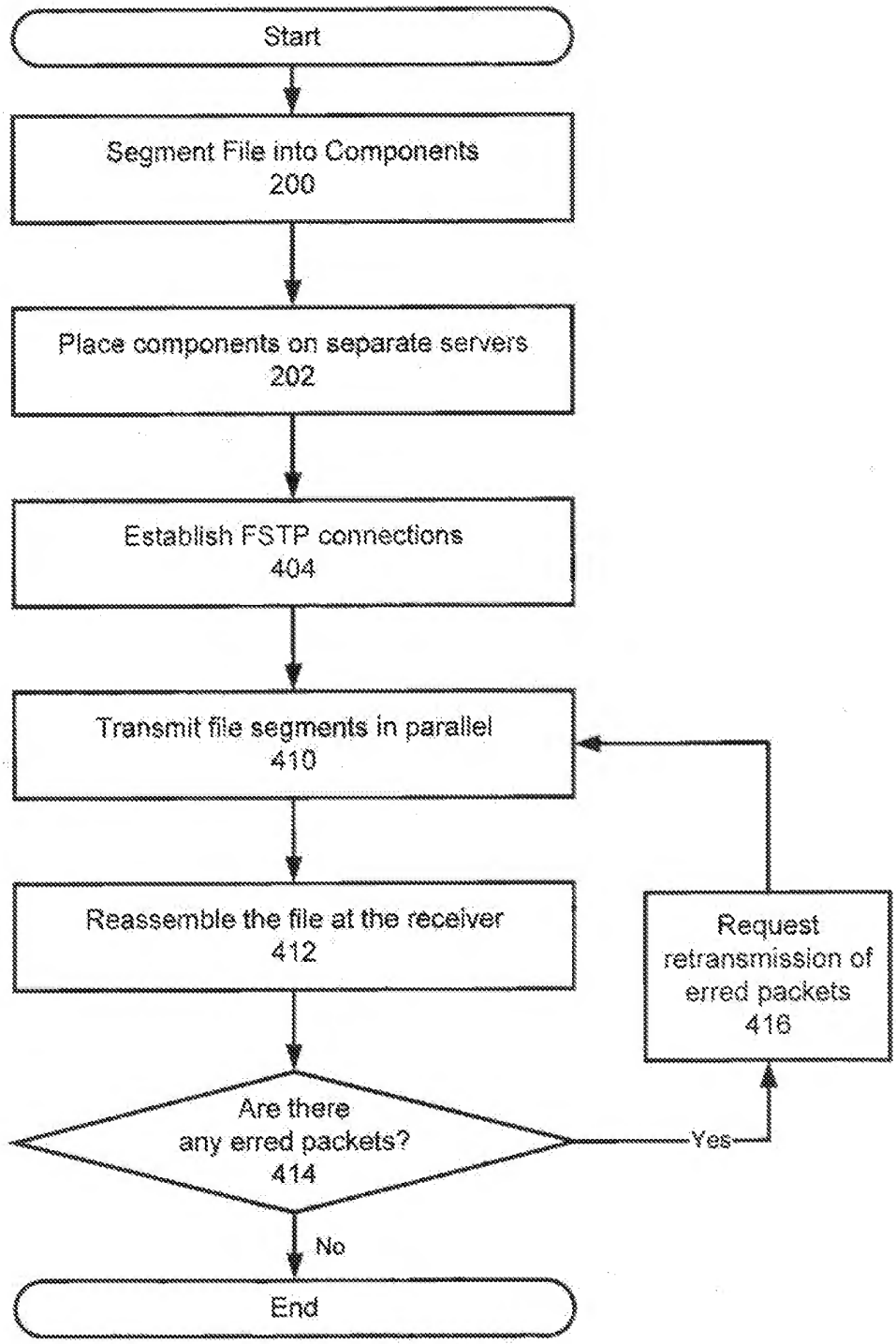

Start
Segment File into Components
200
Place components on separate servers
202
Establish FSTP connections
404
Transmit file segments in parallel
410
Reassemble the file at the receiver
412
Are there
any erred packets?
414
Yes
Request
retransmission of
erred packets
416
No
End

Figure 5

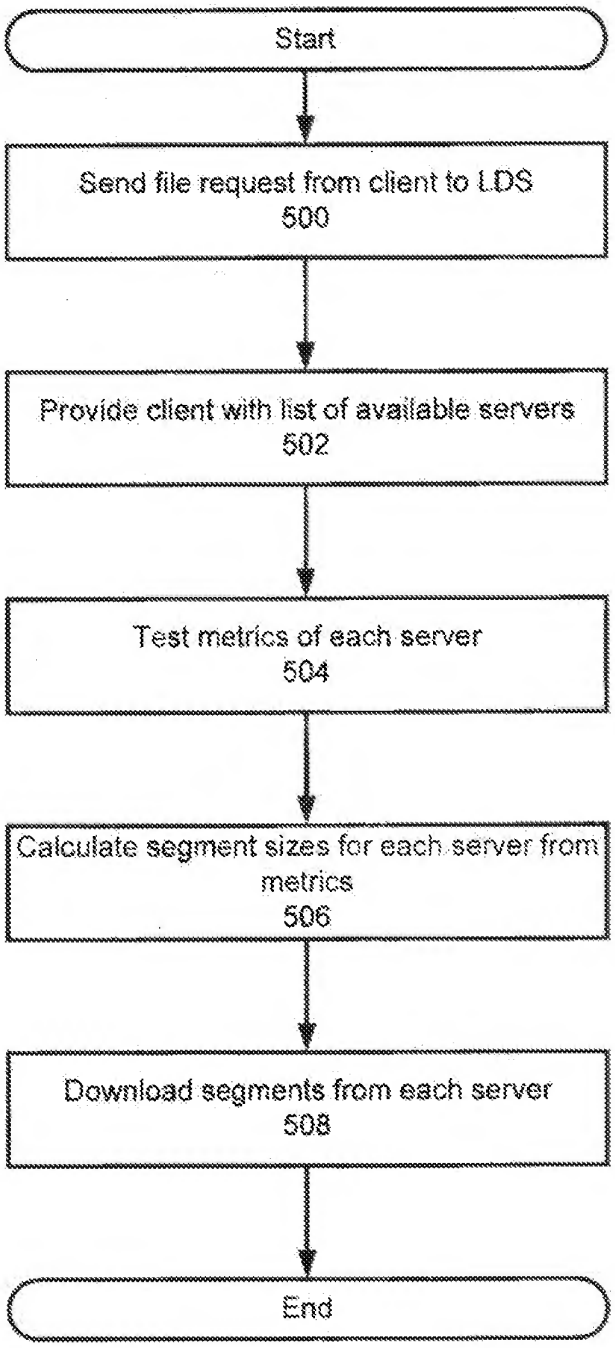

Start
Send file request from client to LDS
500
Provide client with list of available servers
502
Test metrics of each server
504
Calculate segment sizes for each server from metrics
506
Download segments from each server
508
End

Figure 6

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-105
Application Number 13/371,363	Filed February 10, 2012
For SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	
Art Unit 2492	Examiner M. W. Chao

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
[X] One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 200.00
[ ] Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
[ ] Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
[ ] Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
[ ] Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

[ ] Applicant asserts small entity status. See 37 CFR 1.27.

[ ] Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

[ ] A check in the amount of the fee is enclosed.

[ ] Payment by credit card. Form PTO-2038 is attached.

[X] The Director has already been authorized to charge fees in this application to a Deposit Account.

[X] The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 18-1945 .

[X] Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

[ ] applicant/inventor.

[ ] assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

[X] attorney or agent of record. Registration number 70,069 .

[ ] attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Christopher J. Han/	October 27, 2015
Signature	Date
Christopher J. Han	(617) 951-7000
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

[X] * Total of 1 forms are submitted.

53813918_1

Electronic Acknowledgement Receipt

EFS ID:	23900115
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	27-OCT-2015
Filing Date:	10-FEB-2012
Time Stamp:	14:44:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1100
RAM confirmation Number	944
Deposit Account	181945
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	EP2309700.pdf	15846871 c635d7bf2444cefb17d3eb341d94cb920b0902e1	no	14
Warnings:					
Information:					
2	Foreign Reference	JP2005244379_with_Eng_Abstract_and_machine_translation.pdf	4239700 aa15b8077ef153212dd78f855a5884ef03f569dc	no	23
Warnings:					
Information:					
3	Foreign Reference	WO200154370.pdf	9398333 d9f6b5642d28e6906be475efb46c82113a6f2a30	no	33
Warnings:					
Information:					
4	Non Patent Literature	Goodson_Efficient_consistency_for_erasure_coded_data.pdf	10454415 a858bc8ba7a676a11c0cb6126f0d13e09f59a1d5	no	25
Warnings:					
Information:					
5	Non Patent Literature	Long_Swift-RAID_A_Distributed_RAID_System.pdf	22433782 ddcfa3a3477f491c679a3a272d7e707df0c7bbf0	no	20
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_SB08.pdf	160106 1f5df1693a4e652956644c2ef3d5a1c930cb1627	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Transmittal Letter	104093_0002_105_IDS_Transmittal.pdf	83344 80e7ca2ea279517e00312959947a5d64fa94a1421	no	2
Warnings:					
Information:					

8		104093_0002_105_Amendment.pdf	135081 c79ebbb2bfb8d4bd185b2b2c1566c12ec783d45c	yes	10

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	8
Applicant Arguments/Remarks Made in an Amendment	9	10

Warnings:

Information:

9	Extension of Time	104093_0002_105_EOT.pdf	75047 0f38ace2020878596891b51f92705477960db076c	no	1

Warnings:

Information:

10	Fee Worksheet (SB06)	fee-info.pdf	34094 483f1ae4333e62d17277076c31cee7c3d179e451	no	2

Warnings:

Information:

Total Files Size (in bytes):	62860773

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in Excess of 20	1202	9	80	720
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**1100**

REMARKS

Claims 1-27 are pending in this application. Independent claims 1, 10, and 19 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Krawczyk, *Secret Sharing Made Short* ("SSMS"), Krawczyk *Distributed Fingerprints and Secure Information Dispersal* ("DFSID"), and in combination with one of the following: U.S. Patent No. 6,557,123 ("Wiencko"), Buckhard *Disk Array Storage System Reliability* ('Buckhard"), Xu *Highly Available Distributed Storage Systems* ("Xu"), or Swift *RAID: A Distributed RAID System* ("Swift"). In the alternative, independent claims 1, 10, and 19 stand rejected under 35 U.S.C. § 103 as being allegedly obvious in view of Wells *The OceanStore Archive: Goals, Structures, and Self-Repair* in combination with one of Wiencko or Xu.

In order to expedite prosecution, and without concurring in the rejections, Applicants have amended independent claims 1, 10, and 19 to clarify the claimed subject matter. Dependent claims 9 and 18 are amended to conform to amended independent claims 1, 10, and 19. New claims 28-36 are added. The amendments and new claims do not add new matter and are fully supported by the original application. Applicants traverse the rejections and request reconsideration and withdrawal of the same in light of the following remarks.

Summary of Examiner Interview

The undersigned wishes to thank Examiner Chao for the courtesies extended during the in-person interview conducted on October 15, 2015. During the interview, the Examiner and the undersigned discussed the rejections under § 103 and the amendments made herein in this reply. The Examiner agreed that the amended claims are patentable over the art of record (for example, the art of record does not teach or suggest shares that have different amounts of data from an encrypted data set, as claimed). Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejections under § 103 of the independent claims 1, 10, and 19 and all claims that depend thereon.

Conclusion

In view of the foregoing, Applicants believe the pending application is in condition for allowance.

Applicants believe no fee is due with this response other than as indicated on the Fee Transmittal submitted concurrently herewith. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: October 27, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/371,363	Filing Date 02/10/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	10/27/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 36	Minus	** 27	= 9	X $80 =	720
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**720**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/VENESSA JONES/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
O'Hare et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: T. K. Kim

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed more than three months after the U.S. filing date, AND after the mailing date of the first Office Action on the merits, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 18-1945 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 18-1945, under Order No. 104093-0002-105.

Dated: December 4, 2015

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Electronic Acknowledgement Receipt

EFS ID:	24261924
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	04-DEC-2015
Filing Date:	10-FEB-2012
Time Stamp:	11:37:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	8906
Deposit Account	181945
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_SB08.pdf	99634 f02d6ad4951ceeb2192db07b3e1a512c142a838f	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Transmittal Letter	104093_0002_105_IDS_Transmittal.pdf	83083 7ecbc41d374f42d998524e01b5a8c613fdc01078	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30788 3e9f7354c089caa0ce0a41bbaffe6fca10228f0b8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	213505		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2003/0110188-A1	06-12-2003	Howard et al.	
		US-20040193878-A1	09-30-2004	Dillinger et al.	
		US-20050210243-A1	09-22-2005	Archard et al.	
		US-2006/0090200-A1	04-27-2006	Oie	
		US-20060075225-A1	04-06-2006	Flynn et al.	
		US-2010/0191958-A1	07-29-2010	Chen	
		US-4,802,220	01-31-1989	Marker, Jr.	
		US-6,078,888	06-20-2000	Johnson, Jr.	
		US-6,898,285	05-24-2005	Hutchings et al.	
		US-6,981,141	12-27-2005	Mahne et al.	
		US-7,039,189	05-02-2006	Kienzle et al.	
		US-7,076,651	07-11-2006	Droge	
		US-7,346,773	03-18-2008	Cam-Winget et al.	
		US-7,464,152	12-09-2008	Ishizaki et al.	
		US-7,548,556	06-16-2009	Wittenschlaeger	
		US-7,584,285	09-01-2009	Hudson et al.	
		US-7,609,687	10-27-2009	Kobayashi et al.	
		US-7,940,932	05-10-2011	Paksoy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

54258316_1

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,983,994	07-19-2011	Hurry	
		US-8,112,622	02-07-2012	Qi	
		US-8,135,980	03-13-2012	Dodgson et al.	
		US-8,190,905	05-29-2012	Chang et al.	
		US-8,213,387	07-03-2012	Xia et al.	
		US-8,397,083	03-12-2013	Sussland et al.	
		US-8,473,757	06-25-2013	Gladstone et al.	
		US-8,635,456	01-21-2014	Fascenda	
		US-8,755,322	06-17-2014	Miettinen et al.	
		US-8,761,401	06-24-2014	Sprunk et al.	
		US-8,959,199	02-17-2015	Peleg et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

54258316_1
54258316_1

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	O'HARE ET AL.
	Examiner	**Art Unit**
	TAE KIM	2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/02/2012	07/16/2012	03/12/2013	09/06/2013	10/03/2014	12/14/2015			
	1	✓	✓	✓	✓	✓	=			
	2	✓	✓	✓	✓	✓	=			
	3	✓	✓	✓	✓	✓	=			
	4	✓	✓	✓	✓	✓	=			
	5	✓	✓	✓	✓	✓	=			
	6	✓	✓	✓	✓	✓	=			
	7	✓	✓	✓	✓	✓	=			
	8	✓	✓	✓	✓	✓	=			
	9	✓	✓	✓	✓	✓	=			
	10	✓	✓	✓	✓	✓	=			
	11	✓	✓	✓	✓	✓	=			
	12	✓	✓	✓	✓	✓	=			
	13	✓	✓	✓	✓	✓	=			
	14	✓	✓	✓	✓	✓	=			
	15	✓	✓	✓	✓	✓	=			
	16	✓	✓	✓	✓	✓	=			
	17	✓	✓	✓	✓	✓	=			
	18	✓	✓	✓	✓	✓	=			
	19	✓	✓	✓	✓	✓	=			
	20	✓	✓	✓	✓	✓	=			
	21	✓	✓	✓	✓	✓	=			
	22	✓	✓	✓	✓	✓	=			
	23	✓	✓	✓	✓	✓	=			
	24	✓	✓	✓	✓	✓	=			
	25	✓	✓	✓	✓	✓	=			
	26	✓	✓	✓	✓	✓	=			
	27	✓	✓	✓	✓	✓	=			
	28						=			
	29						=			
	30						=			
	31						=			
	32						=			
	33						=			
	34						=			
	35						=			
	36						=			

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

1473 7590 01/14/2016

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
KIM, TAE K	
ART UNIT	PAPER NUMBER
2492	

DATE MAILED: 01/14/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

TITLE OF INVENTION: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	04/14/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

1473 7590 01/14/2016
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

TITLE OF INVENTION: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	04/14/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
KIM, TAE K	2492	726-030000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

1473 7590 01/14/2016

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
KIM, TAE K	

ART UNIT	PAPER NUMBER
2492	

DATE MAILED: 01/14/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/371,363	Applicant(s) O'HARE ET AL.	
	Examiner TAE KIM	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *October 27, 2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-36*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE** "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 10/27/15; 12/04/15
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/TAE KIM/
Primary Examiner, Art Unit 2492

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This is in response to the Applicant's response filed on October 27, 2015. Claims 1, 10, and 19 are amended by the Applicant. Claims 28 – 26 are added. Claims 1 – 36, where Claims 1, 10, and 19 are in independent form, are presented for examination.

Information Disclosure Statement

The information disclosure statements (IDSs) submitted on October 27, 2015 and December 4, 2015 were filed before the mailing date of the current action. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Allowable Subject Matter

Claims 1 – 36 allowed.

The following is an examiner's statement of reasons for allowance: see Remarks, Pg. 9; shares that have different amounts of data from an encrypted data set.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tae K. Kim, whose telephone number is (571) 270-1979. The examiner can normally be reached on Monday - Friday (10:00 AM - 6:30 PM EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar, can be reached on (571) 272-4006. The fax phone number for submitting all Official communications is (703) 872-9306. The fax phone number for submitting informal communications such as drafts, proposed amendments, etc., may be faxed directly to the examiner at (571) 270-2979.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

/Tae K. Kim/

Tae K. Kim
Primary Examiner, Art Unit 2492

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	O'HARE ET AL.
	Examiner	**Art Unit**
	Tae Kim	2492

CPC- SEARCHED		
Symbol	**Date**	**Examiner**
H04L 67/108	4/25/2014	mc
G06F 11/1092	4/25/2014	mc
G06F21/ 6218, /606, /62, /602	12/14/2015	Tae Kim
H04L9/08, /3226, /3263	12/14/2015	Tae Kim
H04L63/04, /08, /0876, /0428	12/14/2015	Tae Kim

CPC COMBINATION SETS - SEARCHED		
Symbol	**Date**	**Examiner**

US CLASSIFICATION SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/17/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	4/25/2014	mc

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
google searched "array coding" and "erasure OR error coding raid"	4/25/2014	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	10/3/2014	mc
google searched "RAID 0+1" "RAID storage randomize"	10/3/2014	mc
google searched "erasure-coding RAID"	6/11/2015	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	6/12/2015	mc
updated search	12/14/2015	Tae Kim

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	26 (with claim terms)	10/3/2014	mc
G06F21/ 6218, /606, /62, /602		12/14/2015	Tae Kim
H04L9/08, /3226, /3263		12/14/2015	Tae Kim
H04L63/04, /08, /0876, /0428		12/14/2015	Tae Kim

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2003/0110188-A1	06-12-2003	Howard et al.	
		US-20040193878-A1	09-30-2004	Dillinger et al.	
		US-20050210243-A1	09-22-2005	Archard et al.	
		US-2006/0090200-A1	04-27-2006	Oie	
		US-20060075225-A1	04-06-2006	Flynn et al.	
		US-2010/0191958-A1	07-29-2010	Chen	
		US-4,802,220	01-31-1989	Marker, Jr.	
		US-6,078,888	06-20-2000	Johnson, Jr.	
		US-6,898,285	05-24-2005	Hutchings et al.	
		US-6,981,141	12-27-2005	Mahne et al.	
		US-7,039,189	05-02-2006	Kienzle et al.	
		US-7,076,651	07-11-2006	Droge	
		US-7,346,773	03-18-2008	Cam-Winget et al.	
		US-7,464,152	12-09-2008	Ishizaki et al.	
		US-7,548,556	06-16-2009	Wittenschlaeger	
		US-7,584,285	09-01-2009	Hudson et al.	
		US-7,609,687	10-27-2009	Kobayashi et al.	
		US-7,940,932	05-10-2011	Paksoy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Tae Kim/	Date Considered	12/11/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

54258316_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,983,994	07-19-2011	Hurry	
		US-8,112,622	02-07-2012	Qi	
		US-8,135,980	03-13-2012	Dodgson et al.	
		US-8,190,905	05-29-2012	Chang et al.	
		US-8,213,387	07-03-2012	Xia et al.	
		US-8,397,083	03-12-2013	Sussland et al.	
		US-8,473,757	06-25-2013	Gladstone et al.	
		US-8,635,456	01-21-2014	Fascenda	
		US-8,755,322	06-17-2014	Miettinen et al.	
		US-8,761,401	06-24-2014	Sprunk et al.	
		US-8,959,199	02-17-2015	Peleg et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Tae Kim/	Date Considered	12/11/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

54258316_1
54258316_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,959,199	09/24/2009	Peleg et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 2 309 700	04/13/2011	Alcatel Lucent		
		JP 2005/244379	09/08/2005	NEC Communication Syst		√
		WO 2001/054370	07/26/2001	The University of Manitoba		

Examiner Signature	/Tae Kim/	Date Considered	12/11/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

53811906_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Goodson et al., "Efficient consistency for erasure-coded data via versioning servers," Retrieved from the Internet<URL:oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461126> 25 pages, March 2003.	
		Long et al., "Swift/RAID: A Distributed RAID System," Retrieved from the Internet<URL:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7183>pgs. 1-20 (1994).	

Examiner Signature	/Tae Kim/	Date Considered	12/11/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

53811906_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination O'HARE ET AL.	
	Examiner TAE KIM	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,782,436 B2	07-2014	Koifman; Chaim	G06F3/0623	380/269
*	B	US-8,793,510 B2	07-2014	Koifman; Chaim	G06F3/0623	380/269
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"8713189"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2015/12/13 22:15
S1	7	"13371363"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2015/12/11 16:53
S2	3	"8959199"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2015/12/11 16:53

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	7	"13371363"	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:29
L3	104	(ohare near3 mark).in.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:29
L4	103	(orsini near3 rick).in.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:29
L5	101	(davenport near3 roger).in.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:29
L6	50	(winick near3 steven).in.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:30
L7	141	(encrypt$3 secur$5) near4 (data set) same ((random different varying variety) near4 (amount total sum size)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:31
L8	13	l7 and (g06f21/6218 g06f21/606 g06f21/62 g06f21/602).cpc.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:33
L9	31	l7 and ((send$3 stor$3 sav$3) near6 (different many pluality) near3 (device location database storage))	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:35
L10	10	l7 and ((send$3 stor$3 sav$3) near6 (different many pluality) near3 (device location database storage)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:35
L11	0	l7 and (h04l9/085 h04l9/3226	US-	OR	ON	2015/12/13

		h04l9/3263).cpc.	PGPUB; USPAT; UPAD			22:39
L12	5	l7 and (h04l63/04 h04l63/08 h04l63/0876 h04l63/0428).cpc.	US-PGPUB; USPAT; UPAD	OR	ON	2015/12/13 22:40

12/ 13/ 2015 10:44:29 PM
C:\ Users\ tkim4\ Documents\ EAST\ Workspaces\ App13371363.wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
13371363	O'HARE ET AL.
Examiner	**Art Unit**
TAE KIM	2492

CPC						
Symbol					**Type**	**Version**
H04L		63	/	0428	F	2013-01-01
H04L		7	/	108	I	2013-01-01
G06F		11	/	1092	A	2013-01-01
G06F		1	/	606	I	2013-01-01
G06F		21	/	62	I	2013-01-01
H04L		9	/	085	I	2013-01-01
H04L		9	/	3226	I	2013-01-01
H04L			/	3263	I	2013-01-01
H04L		63	/	04	I	2013-01-01
H04L		63	/	08	I	2013-01-01
H04L		2209	/	80	A	2013-01-01
G06F		1	/	602	I	2013-01-01
H04L		63	/	0876	I	2013-01-01
H04L		69	/	14	I	2013-01-01
G06F		21	/	6218	I	2013-01-01
G06F		17	/	30312	I	2013-01-01
H04L		63	/	0823	I	2013-01-01

CPC Combination Sets						
Symbol				**Type**	**Set**	**Ranking**	**Version**
		/					
		/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	36	
/TAE KIM/ Primary Examiner.Art Unit 2492	12/14/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	21

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	O'HARE ET AL.
	Examiner	**Art Unit**
	TAE KIM	2492

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
		H 0 4 L 29 / 06 (2006.01.01)	
		H 0 4 L 9 / 00 (2006.01.01)	

CROSS REFERENCE(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	36	
/TAE KIM/ Primary Examiner.Art Unit 2492	12/14/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	21

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	O'HARE ET AL.
	Examiner	**Art Unit**
	TAE KIM	2492

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17		33										
	2		18		34										
	3		19		35										
	4		20		36										
	5		21												
	6		22												
	7		23												
	8		24												
	9		25												
	10		26												
	11		27												
	12		28												
	13		29												
	14		30												
	15		31												
	16		32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 36	
/TAE KIM/ Primary Examiner.Art Unit 2492 (Primary Examiner)	12/14/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 21

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: O'Hare et al.	Allowed: January 14, 2016
Application No.: 13/371,363	Confirmation No.: 7984
Filed: February 10, 2012	Art Unit: 2492
For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA	Examiner: T. K. Kim

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed after the mailing date of a Notice of Allowance, but on or before payment of the Issue Fee (37 C.F.R. § 1.97(d)). Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered.

I hereby certify, pursuant to 37 C.F.R. § 1.97(e)(1), that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted a copy of the U.S. patent.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 18-1945 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 18-1945, under Order No. 104093-0002-105.

Dated: January 19, 2016

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/371,363
				Filing Date	February 10, 2012
				First Named Inventor	Mark S. O'Hare
				Art Unit	2492
(Use as many sheets as necessary)				Examiner Name	T. K. Kim
Sheet	1	of	1	Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2003/0204605	10/30/2003	Hudson, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

54927108_1

Electronic Acknowledgement Receipt

EFS ID:	24658082
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	19-JAN-2016
Filing Date:	10-FEB-2012
Time Stamp:	16:30:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	3519
Deposit Account	181945
Authorized User	HAN, CHRISTOPHER

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	104093_0002_105_IDS_Statement.pdf	83326 e14a02767be681bb3dd08aba4da3cf098c8416f4	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_105_IDS_SB08.pdf	88400 5cb9bdb5ceedf83beaf7ba6baead0d7305b71920	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (SB06)	fee-info.pdf	30788 fb316089622a0129bfa3c0b2fa38063020dc03fd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	202514		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Receipt date: 01/19/2016

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	T. K. Kim
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2003/0204605	10/30/2003	Hudson, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Tae Kim/	Date Considered	01/28/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

54927108_1

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 Avenue of the Americas
New York, NY 10036-8704

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

TITLE OF INVENTION: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960.00	$0	$0	$960.00	04/14/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
T. K. Kim	2492	726-030000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- [ ] Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- [ ] "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Ropes & Gray LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Security First Corp.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Rancho Santa Margarita, California

Please check the appropriate assignee category or categories (will not be printed on the patent) : [ ] Individual [X] Corporation or other private group entity [ ] Government

4a. The following fee(s) are submitted:
- [X] Issue Fee
- [ ] Publication Fee (No small entity discount permitted)
- [ ] Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- [ ] A check is enclosed.
- [ ] Payment by credit card. Form PTO-2038 is attached.
- [X] The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 18-1945 (~~enclose an extra copy of this form~~).

5. **Change in Entity Status** (from status indicated above)
- [ ] Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- [ ] Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- [ ] Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Christopher J. Han/ Date February 4, 2016

Typed or printed name Christopher J. Han Registration No. 70,069

Electronic Acknowledgement Receipt

EFS ID:	24820533
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	04-FEB-2016
Filing Date:	10-FEB-2012
Time Stamp:	15:00:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$960
RAM confirmation Number	1380
Deposit Account	181945
Authorized User	HAN, CHRISTOPHER
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	104093_0002_105_Issue_Fee.pdf	110077 64cb39da652a9b7fa3662cfb32f50b9dfe0641d0	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30573 162d1b5cf8f97cb39e396389fa053df27fb21e1d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	140650		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105	7984

1473 7590 02/04/2016

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
KIM, TAE K	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
02/04/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com
pair_rg@firsttofile.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/371,363	10 February, 2012	O'HARE ET AL.	104093-0002-105

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
TAE KIM	
ART UNIT	PAPER
2492	20160128

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

IDS submitted on January 19, 2016 has been considered.

/TAE KIM/
Primary Examiner, Art Unit 2492

PTO-90C (Rev.04-03)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20030204605"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/01/28 16:59

EAST Search History (Interference)

< This search history is empty>

1/ 28/ 2016 5:02:18 PM
C:\ Users\ tkim4\ Documents\ EAST\ Workspaces\ App13371363.wsp

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Christopher Jinhyun Han/Paula Derby
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**960**

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,959,199 02/2015	~~09/24/2009~~	Peleg et al.	

Change(s) applied to document, /S.D./ 1/21/2016

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 2 309 700	04/13/2011	Alcatel Lucent		
		JP 2005/244379	09/08/2005	NEC Communication Syst		√
		WO 2001/054370	07/26/2001	The University of Manitoba		

Examiner Signature	/Tae Kim/	Date Considered	12/11/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

53811906_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

Change(s) applied to document, /S.D./ 1/21/2016

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,107,385	09-12-2006	Rajan et al.	
		US-7,085,854	08-01-2006	~~Gorente~~ Keane et al.	
		US-7,003,668	02-21-2006	Berson et al.	
		US-6,915,436	07-05-2005	Booth, III et al.	
		US-6,785,768	08-31-2004	Peters et al.	
		US-6,505,216	01-07-2003	Schutzman et al.	
		US-6,415,373	07-02-2002	Peters et al.	
		US-5,666,514	09-09-1997	Cheriton	
		US-5,623,549	04-22-1997	Ritter	
		US-5,603,003	02-11-1997	Akizawa et al.	
		US-2013/0042105	02-14-2013	Orsini et al.	
		US-2012/0266231	10-18-2012	Spiers et al.	
		US-2012/0255035	10-04-2012	Orsini et al.	
		US-2012/0255034	10-04-2012	Orsini et al.	
		US-2011/0145413	06-16-2011	Dawson et al.	
		US-2011/0093113	04-21-2011	Sager et al.	
		US-2010/0332617	12-30-2010	Goodwin et al.	
		US-2010/0318812	12-16-2010	Auradkar et al.	
		US-2010/0283734	11-11-2010	Hallbauer et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages. Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Michael Chao/	Date Considered	07/17/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

36663708_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	03/22/2016	9294444	104093-0002-105	7984

1473 7590 03/02/2016

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Electronic Acknowledgement Receipt

EFS ID:	25665065
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Paula Derby
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	03-MAY-2016
Filing Date:	10-FEB-2012
Time Stamp:	13:41:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	104093_0002_105_Request_For_Certificate_of_Correction.pdf	174343 913d44fd773b222b90fc6ee0d392e7ef9a0f206b	no	3
Warnings:					
Information:					

Total Files Size (in bytes):	174343

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
O'Hare et al.

Patent No.: 9,294,444

Issued: March 22, 2016

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

REQUEST FOR CERTIFICATE OF CORRECTION
PURSUANT TO 37 C.F.R. § 1.322

Attention: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted a typographical error which should be corrected.

On the front page of patent:

In item (60) (Second item under Related U.S. Application Data), **"60/222,146"** should be **--60/622,146--**

Patentee respectfully submits that the error was not in the application as filed by applicant and is not the result of Patentee's mistake. For example, both the original specification and the application data sheet as filed on February 10, 2012 indicate the provisional application No.

56058209_1

60/622,146. Accordingly, this error is believed to be the responsibility of the Patent and Trademark Office, the correction of which neither constitutes new matter nor requires reexamination.

Transmitted herewith is a proposed Certificate of Correction effecting such amendment. Patentee respectfully solicits the granting of the requested Certificate of Correction.

Because this error is believed to be the responsibility of the Patent and Trademark Office, Applicant believes no fee is due with this request. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: May 3, 2016

Respectfully submitted,

/Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Agent For Applicants

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.	:	9,294,444
APPLICATION NO.	:	13/371,363
ISSUE DATE	:	March 22, 2016
INVENTOR(S)	:	O'Hare et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the front page of the patent:

In item (60) (Second item under Related U.S. Application Data), **"60/222,146"** should be **--60/622,146--**

MAILING ADDRESS OF SENDER (Please do not use customer number below):
Christopher J. Han
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199

56058115_1

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 9,294,444 B2
APPLICATION NO.	: 13/371363
DATED	: March 22, 2016
INVENTOR(S)	: O'Hare et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the title page of the patent:

In item (60) (Second item under Related U.S. Application Data), "**60/222,146**" should be **--60/622,146--**

Signed and Sealed this
Seventh Day of June, 2016

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	28911435
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	1473
Filer:	Alexander Shvarts/Juanita Alvarez
Filer Authorized By:	Alexander Shvarts
Attorney Docket Number:	104093-0002-105
Receipt Date:	12-APR-2017
Filing Date:	10-FEB-2012
Time Stamp:	18:42:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	104093_0002_105_POA.pdf	222335 78f5a6500500983e73b2d95f1fc663d44fab6222	no	1
Warnings:					

Information:					
2	Assignee showing of ownership per 37 CFR 3.73	104093_0002_105_STATEMENT_373b.pdf	32640 575b350b34feef1942c7d281da08220eca3384bb	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	254975	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Security First Corp.

Application No./Patent No.: 13/371,363 Filed/Issue Date: February 10, 2012

Titled: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

Security First Corp. , a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 028094, Frame 0896, or for which a copy therefore is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Alexander Shvarts/ April 12, 2017

Signature Date

Alexander Shvarts Attorney for Assignee

Printed or Typed Name Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 15314

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 15314

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Security First Corp.
29811 Santa Margarita Parkway, Suite 600
Rancho Santa Margarita, CA 92688

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	3/17/2017
Name	James Varner	Telephone	
Title	President & CEO, Security First Corp.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105

CONFIRMATION NO. 7984

POWER OF ATTORNEY NOTICE

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

OC000000090768501

Date Mailed: 04/21/2017

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/12/2017.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/mabebe/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105

CONFIRMATION NO. 7984

15314
Shvarts & Leiz LLP
111 North Market Street, Suite 820
San Jose, CA 95113

POA ACCEPTANCE LETTER

OC000000090768512

Date Mailed: 04/21/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/12/2017.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/mabebe/

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT5185448

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	RELEASE OF SECURITY INTEREST

CONVEYING PARTY DATA

Name	Execution Date
MR. ANDY GYENES	10/11/2018
AUBER INVESTMENTS LTD.	10/11/2018
MS BARBARA SIMONS	10/11/2018
BLT1	10/11/2018
MR COLIN O'REILLY	10/11/2018
COOPER ROAD LLC	10/11/2018
COYDOG FOUNDATION	10/11/2018
DASA INVESTMENTS LLC	10/11/2018
MR DAVID E LAKOFF	10/11/2018
MR DAVID LEES	10/11/2018
MR. DAVID O'REILLY	10/11/2018
MR DAVID OKST	10/11/2018
MR DEAN C KEHLER	10/11/2018
MS DOROTHY KOBAK	10/11/2018
MS ELIZABETH CRAWFORD	10/11/2018
MR ERIC ALTMANN	10/11/2018
MR GERALD R JORDAN JR	10/11/2018
GRANDPRIX LIMITED	10/11/2018
MR H.W. RAUTENBERG	10/11/2018
MR JAMES W HARPEL	10/11/2018
MR JASPER WU	10/11/2018
MR. JAIME PEISACH	10/11/2018
LG MANAGEMENT LLC	10/11/2018
LTE PARTNERS	10/11/2018
MR MARK RAUTENBERG	10/11/2018
MR MAURICE PINTO	10/11/2018
MEYTHALER INVESTMENT PARTNERS LLC	10/11/2018
MR MICHAEL MASELLI	10/11/2018
MR PETER GYENES	10/11/2018
MR RAYMOND GINTHER	10/11/2018
MR RICHARD M BERKELEY	10/11/2018

Name	Execution Date
MR ROBERT MERCER	10/11/2018
ROLA INVESTMENTS LLC	10/11/2018
SOS & CO.	10/11/2018
MR STANKO BARLE	10/11/2018
MR SANDOR STRAUS	10/11/2018
MR SYLVAIN MIROCHNIKOFF	10/11/2018
MS REBEKAH MERCER	10/11/2018
TOPSPIN SFC HOLDINGS LLC	10/11/2018
MR WESLEY W BARTON	10/11/2018
ZUG VENTURES LLC	10/11/2018
MR CHARLES ZUCKER	10/11/2018
MR ROGER T COLEMAN	10/11/2018
MS MARGARET E COLEMAN	10/11/2018
MS THERESA M COLEMAN	10/11/2018
MR JOHN T COLEMAN	10/11/2018
MR STEPHEN PERLBINDER	10/11/2018

RECEIVING PARTY DATA

Name:	SECURITY FIRST CORP.
Street Address:	29811 SANTA MARGARITA PARKWAY
City:	RANCHO SANTA MARGARITA
State/Country:	CALIFORNIA
Postal Code:	92688

PROPERTY NUMBERS Total: 91

Property Type	Number
Patent Number:	7260724
Patent Number:	9189777
Patent Number:	7187771
Patent Number:	6853988
Patent Number:	7391865
Patent Number:	7577621
Patent Number:	8266438
Patent Number:	8009830
Patent Number:	7802104
Patent Number:	8155322
Patent Number:	8904080
Patent Number:	8135134

Property Type	Number
Patent Number:	8473756
Patent Number:	8656167
Patent Number:	8494969
Patent Number:	8654971
Patent Number:	8214650
Patent Number:	8745372
Patent Number:	9195839
Patent Number:	8650434
Patent Number:	8601498
Patent Number:	8320560
Patent Number:	8656189
Patent Number:	9275071
Patent Number:	9165137
Patent Number:	8769270
Patent Number:	8677148
Patent Number:	8271802
Patent Number:	9294444
Patent Number:	8332638
Patent Number:	9397827
Patent Number:	8787583
Patent Number:	9100186
Patent Number:	9338140
Patent Number:	9047475
Patent Number:	8769699
Patent Number:	8904194
Patent Number:	9294445
Patent Number:	9009848
Patent Number:	8726033
Patent Number:	8745379
Patent Number:	8644502
Patent Number:	9213857
Patent Number:	9098718
Patent Number:	8898464
Patent Number:	9177159
Patent Number:	9015480
Patent Number:	9064127
Patent Number:	9317705
Patent Number:	9215218

Property Type	Number
Patent Number:	9264224
Patent Number:	9300649
Patent Number:	9407431
Patent Number:	9298937
Patent Number:	9135456
Application Number:	12148365
Application Number:	13024791
Application Number:	13024804
Application Number:	13077770
Application Number:	13371364
Application Number:	13468428
Application Number:	13831164
Application Number:	13831273
Application Number:	13831313
Application Number:	13866345
Application Number:	13866452
Application Number:	13866477
Application Number:	13915081
Application Number:	13915570
Application Number:	14057902
Application Number:	14164995
Application Number:	14180151
Application Number:	14253588
Application Number:	14317742
Application Number:	14546887
Application Number:	14659008
Application Number:	14710522
Application Number:	14710528
Application Number:	14713792
Application Number:	14749058
Application Number:	14749172
Application Number:	14750562
Application Number:	14828377
Application Number:	14875687
Application Number:	14918176
Application Number:	14931169
Application Number:	14949370
Application Number:	14949519

Property Type	Number
Application Number:	14969651
Application Number:	14984087
PCT Number:	US2015062188

CORRESPONDENCE DATA

Fax Number: (516)622-9212

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: (516) 622-9200
Email: AEDERER@WESTERMANLLP.COM
Correspondent Name: ALAN C. EDERER
Address Line 1: 1201 RXR PLAZA
Address Line 2: C/O WESTERMAN BALL EDERER MILLER ZUCKER & SHARFSTE
Address Line 4: UNIONDALE, NEW YORK 11556

NAME OF SUBMITTER:	ALAN EDERER
SIGNATURE:	/Alan Ederer/
DATE SIGNED:	10/12/2018
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 10

source=Termination Agreement (Executed) (01884807xB2F1A)#page1.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page2.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page3.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page4.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page5.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page6.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page7.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page8.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page9.tif
source=Termination Agreement (Executed) (01884807xB2F1A)#page10.tif

TERMINATION OF SECURITY INTEREST IN PATENTS

WHEREAS, Security First Corp., a Delaware corporation with its principal place of business at 29811 Santa Margarita Parkway, Suite 600, Rancho Santa Margarita, CA 92688 (the "***Grantor***"), is the owner of record of the patents and patent applications listed on the attached Exhibit A, now issued or pending in the United States Patent and Trademark Office (the "***Patents***"); and

WHEREAS, the Grantor entered into that certain Patent Security Agreement dated as of April 12, 2016 (the "***Security Agreement***"), between the Grantor and the secured parties identified therein (collectively, the "***Secured Party***"), a true and correct copy of which was recorded by the United States Patent and Trademark Office on June 24, 2016, at Reel 039153, Frame 0321; and

WHEREAS, pursuant to that certain Written Consent and Agreement of the Secured Party dated February 6, 2017 (the "***Consent***"), the Secured Party, among other things, released its lien and security interest in the Patents, and authorized the Grantor to file with the U.S. Patent and Trademark Office any and all termination statements in order to release such lien and security interest;

NOW, THEREFORE, for good and valuable consideration, receipt of which is hereby acknowledged, the Grantor, pursuant to the authority granted by the Security Party in the Consent hereby:

1. Releases and reassigns to the Grantor any and all liens, security interests, right, title and interest of Secured Party pursuant to the Security Agreement in the patents and applications more fully described on Exhibit A, without recourse or representation or warranty, express or implied; and

2. Authorizes and requests the Commissioner of Patents and Trademarks of the United States of America to note and record the existence of the release hereby given.

[Remainder of Page Intentionally Left Blank]

IN WITNESS WHEREOF, the Grantor has caused this Termination of Security Interest in Patents to be signed by its duly authorized representative as of this 11th day of October, 2018.

GRANTOR:

Security First Corp.

By: _____

James Varner, President and CEO

Sworn to before me this 11 day of October, 2018

Notary Public

TODD R. BENWARE
NOTARY PUBLIC
Durham County, North Carolina
My Commission Expires May 25, 2020

Commission Expires 05/25/2020

[Signature Page to Termination of Security Interest in Patents]

EXHIBIT A

Patents and Applications

See attached.

01557069

EXHIBIT A

Patents and Applications

See attached.

APPLICATION NUMBER: 09666377 FILING DATE: 09/20/2000
PATENT NUMBER: 7260724 ISSUE DATE: 08/21/2007
TITLE: CONTEXT SENSITIVE DYNAMIC AUTHENTICATION IN A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 09666378 FILING DATE: 09/20/2000
PATENT NUMBER: 9189777 ISSUE DATE: 11/17/2015
TITLE: ELECTRONIC COMMERCE WITH CRYPTOGRAPHIC AUTHENTICATION

APPLICATION NUMBER: 09666519 FILING DATE: 09/20/2000
PATENT NUMBER: 7187771 ISSUE DATE: 03/06/2007
TITLE: SERVER-SIDE IMPLEMENTATION OF A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 09666647 FILING DATE: 09/20/2000
PATENT NUMBER: 6853988 ISSUE DATE: 02/08/2005
TITLE: CRYPTOGRAPHIC SERVER WITH PROVISIONS FOR INTEROPERABILITY BETWEEN CRYPTOGRAPHIC SYSTEMS

APPLICATION NUMBER: 10458928 FILING DATE: 06/11/2003
PATENT NUMBER: 7391865 ISSUE DATE: 06/24/2008
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 11014967 FILING DATE: 12/20/2004
PATENT NUMBER: 7577621 ISSUE DATE: 08/18/2009
TITLE: CRYPTOGRAPHIC SERVER WITH PROVISIONS FOR INTEROPERABILITY BETWEEN CRYPTOGRAPHIC SYSTEMS

APPLICATION NUMBER: 11258839 FILING DATE: 10/25/2005
PATENT NUMBER: 8266438 ISSUE DATE: 09/11/2012
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 11602667 FILING DATE: 11/20/2006
PATENT NUMBER: 8009830 ISSUE DATE: 08/30/2011
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 11839927 FILING DATE: 08/16/2007
PATENT NUMBER: 7802104 ISSUE DATE: 09/21/2010
TITLE: CONTEXT SENSITIVE DYNAMIC AUTHENTICATION IN A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 11983355 FILING DATE: 11/07/2007
PATENT NUMBER: 8155322 ISSUE DATE: 04/10/2012
TITLE: SYSTEMS AND METHODS FOR DISTRIBUTING AND SECURING DATA

APPLICATION NUMBER: 11999575 FILING DATE: 12/05/2007
PATENT NUMBER: 8904080 ISSUE DATE: 12/02/2014
TITLE: TAPE BACKUP METHOD

APPLICATION NUMBER: 12148365 FILING DATE: 04/18/2008
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 12209703 FILING DATE: 09/12/2008
PATENT NUMBER: 8135134 ISSUE DATE: 03/13/2012
TITLE: SYSTEMS AND METHODS FOR MANAGING CRYPTOGRAPHIC KEYS

APPLICATION NUMBER: 12349897 FILING DATE: 01/07/2009
PATENT NUMBER: 8473756 ISSUE DATE: 06/25/2013
TITLE: SYSTEMS AND METHODS FOR SECURING DATA USING MULTI-FACTOR OR KEYED DISPERSAL

APPLICATION NUMBER: 12391025 FILING DATE: 02/23/2009
PATENT NUMBER: 8656167 ISSUE DATE: 02/18/2014
TITLE: SYSTEMS AND METHODS FOR SECURE WORKGROUP MANAGEMENT AND COMMUNICATION

APPLICATION NUMBER: 12542468 FILING DATE: 08/17/2009
PATENT NUMBER: 8494969 ISSUE DATE: 07/23/2013
TITLE: CRYPTOGRAPHIC SERVER WITH PROVISIONS FOR INTEROPERABILITY BETWEEN CRYPTOGRAPHIC SYSTEMS

APPLICATION NUMBER: 12783276 FILING DATE: 05/19/2010
PATENT NUMBER: 8654971 ISSUE DATE: 02/18/2014
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN THE CLOUD

APPLICATION NUMBER: 12878317 FILING DATE: 09/09/2010
PATENT NUMBER: 8214650 ISSUE DATE: 07/03/2012
TITLE: CONTEXT SENSITIVE DYNAMIC AUTHENTICATION IN A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 12953877 FILING DATE: 11/24/2010
PATENT NUMBER: 8745372 ISSUE DATE: 06/03/2014
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13024783 FILING DATE: 02/10/2011
PATENT NUMBER: 9195839 ISSUE DATE: 11/24/2015
TITLE: TAPE BACKUP METHOD

APPLICATION NUMBER: 13024791 FILING DATE: 02/10/2011
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13024804 FILING DATE: 02/10/2011
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13077770 FILING DATE: 03/31/2011
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13077802 FILING DATE: 03/31/2011
PATENT NUMBER: 8650434 ISSUE DATE: 02/11/2014
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13117791 FILING DATE: 05/27/2011
PATENT NUMBER: 8601498 ISSUE DATE: 12/03/2013
TITLE: ACCELERATOR SYSTEM FOR USE WITH SECURE DATA STORAGE

APPLICATION NUMBER: 13172682 FILING DATE: 06/29/2011
PATENT NUMBER: 8320560 ISSUE DATE: 11/27/2012
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13208132 FILING DATE: 08/11/2011
PATENT NUMBER: 8656189 ISSUE DATE: 02/18/2014
TITLE: SYSTEMS AND METHODS FOR SECURE MULTI-TENANT DATA STORAGE

APPLICATION NUMBER: 13209167 FILING DATE: 08/12/2011
PATENT NUMBER: 9275071 ISSUE DATE: 03/01/2016
TITLE: SYSTEMS AND METHODS FOR SECURE REMOTE STORAGE

APPLICATION NUMBER: 13212360 FILING DATE: 08/18/2011
PATENT NUMBER: 9165137 ISSUE DATE: 10/20/2015
TITLE: SYSTEMS AND METHODS FOR SECURING VIRTUAL MACHINE COMPUTING ENVIRONMENTS

APPLICATION NUMBER: 13237781 FILING DATE: 09/20/2011
PATENT NUMBER: 8769270 ISSUE DATE: 07/01/2014
TITLE: SYSTEMS AND METHODS FOR SECURE DATA SHARING

APPLICATION NUMBER: 13360385 FILING DATE: 01/27/2012
PATENT NUMBER: 8677148 ISSUE DATE: 03/18/2014
TITLE: SYSTEMS AND METHODS FOR SECURING DATA

APPLICATION NUMBER: 13371361 FILING DATE: 02/10/2012
PATENT NUMBER: 8271802 ISSUE DATE: 09/18/2012
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13371363 FILING DATE: 02/10/2012
PATENT NUMBER: 9294444 ISSUE DATE: 03/22/2016
TITLE: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA

APPLICATION NUMBER: 13371364 FILING DATE: 02/10/2012
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13399923 FILING DATE: 02/17/2012
PATENT NUMBER: 8332638 ISSUE DATE: 12/11/2012
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13403142 FILING DATE: 02/23/2012
PATENT NUMBER: 9397827 ISSUE DATE: 07/19/2016
TITLE: SYSTEMS AND METHODS FOR MANAGING CRYPTOGRAPHIC KEYS

APPLICATION NUMBER: 13412111 FILING DATE: 03/05/2012
PATENT NUMBER: 8787583 ISSUE DATE: 07/22/2014
TITLE: SYSTEMS AND METHODS FOR DISTRIBUTING AND SECURING DATA

APPLICATION NUMBER: 13413195 FILING DATE: 03/06/2012
PATENT NUMBER: 9100186 ISSUE DATE: 08/04/2015
TITLE: SECURE FILE SHARING METHOD AND SYSTEM

APPLICATION NUMBER: 13468383 FILING DATE: 05/10/2012
PATENT NUMBER: 9338140 ISSUE DATE: 05/10/2016
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468428 FILING DATE: 05/10/2012
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468450 FILING DATE: 05/10/2012
PATENT NUMBER: 9047475 ISSUE DATE: 06/02/2015
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468523 FILING DATE: 05/10/2012
PATENT NUMBER: 8769699 ISSUE DATE: 07/01/2014
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468562 FILING DATE: 05/10/2012
PATENT NUMBER: 8904194 ISSUE DATE: 12/02/2014
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468584 FILING DATE: 05/10/2012
PATENT NUMBER: 9294445 ISSUE DATE: 03/22/2016
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13468605 FILING DATE: 05/10/2012
PATENT NUMBER: 9009848 ISSUE DATE: 04/14/2015
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13540030 FILING DATE: 07/02/2012
PATENT NUMBER: 8726033 ISSUE DATE: 05/13/2014
TITLE: CONTEXT SENSITIVE DYNAMIC AUTHENTICATION IN A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 13589894 FILING DATE: 08/20/2012
PATENT NUMBER: 8745379 ISSUE DATE: 06/03/2014
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13668433 FILING DATE: 11/05/2012
PATENT NUMBER: 8644502 ISSUE DATE: 02/04/2014
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13831164 FILING DATE: 03/14/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING AND RESTORING VIRTUAL MACHINES

APPLICATION NUMBER: 13831273 FILING DATE: 03/14/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING AND RESTORING VIRTUAL MACHINES

APPLICATION NUMBER: 13831313 FILING DATE: 03/14/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13866345 FILING DATE: 04/19/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13866411 FILING DATE: 04/19/2013
PATENT NUMBER: 9213857 ISSUE DATE: 12/15/2015
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13866452 FILING DATE: 04/19/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13866477 FILING DATE: 04/19/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 13903444 FILING DATE: 05/28/2013
PATENT NUMBER: 9098718 ISSUE DATE: 08/04/2015
TITLE: SYSTEMS AND METHODS FOR SECURING DATA USING MULTI-FACTOR OR KEYED DISPERSAL

APPLICATION NUMBER: 13910798 FILING DATE: 06/05/2013
PATENT NUMBER: 8898464 ISSUE DATE: 11/25/2014
TITLE: SYSTEMS AND METHODS FOR SECURE WORKGROUP MANAGEMENT AND COMMUNICATION

APPLICATION NUMBER: 13915081 FILING DATE: 06/11/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13915518 FILING DATE: 06/11/2013
PATENT NUMBER: 9177159 ISSUE DATE: 11/03/2015
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13915570 FILING DATE: 06/11/2013
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 13973637 FILING DATE: 08/22/2013
PATENT NUMBER: 9015480 ISSUE DATE: 04/21/2015
TITLE: SYSTEMS AND METHODS FOR SECURE MULTI-TENANT DATA STORAGE

APPLICATION NUMBER: 14057902 FILING DATE: 10/18/2013
PATENT NUMBER: ISSUE DATE:
TITLE: ACCELERATOR SYSTEM FOR USE WITH SECURE DATA STORAGE

APPLICATION NUMBER: 14083333 FILING DATE: 11/18/2013
PATENT NUMBER: 9064127 ISSUE DATE: 06/23/2015
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN THE CLOUD

APPLICATION NUMBER: 14133903 FILING DATE: 12/19/2013
PATENT NUMBER: 9317705 ISSUE DATE: 04/19/2016
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14164995 FILING DATE: 01/27/2014
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA

APPLICATION NUMBER: 14180151 FILING DATE: 02/13/2014
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR A CRYPTOGRAPHIC FILE SYSTEM LAYER

APPLICATION NUMBER: 14181257 FILING DATE: 02/14/2014
PATENT NUMBER: 9215218 ISSUE DATE: 12/15/2015
TITLE: SYSTEMS AND METHODS FOR SECURE WORKGROUP MANAGEMENT AND COMMUNICATION

APPLICATION NUMBER: 14247971 FILING DATE: 04/08/2014
PATENT NUMBER: 9264224 ISSUE DATE: 02/16/2016
TITLE: SYSTEMS AND METHODS FOR SECURE DATA SHARING

APPLICATION NUMBER: 14253588 FILING DATE: 04/15/2014
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 14256841 FILING DATE: 04/18/2014
PATENT NUMBER: 9300649 ISSUE DATE: 03/29/2016
TITLE: CONTEXT SENSITIVE DYNAMIC AUTHENTICATION IN A CRYPTOGRAPHIC SYSTEM

APPLICATION NUMBER: 14305993 FILING DATE: 06/16/2014
PATENT NUMBER: 9407431 ISSUE DATE: 08/02/2016
TITLE: SYSTEMS AND METHODS FOR DISTRIBUTING AND SECURING DATA

APPLICATION NUMBER: 14317742 FILING DATE: 06/27/2014
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN MOTION

APPLICATION NUMBER: 14473387 FILING DATE: 08/29/2014
PATENT NUMBER: 9298937 ISSUE DATE: 03/29/2016
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14473813 FILING DATE: 08/29/2014
PATENT NUMBER: 9135456 ISSUE DATE: 09/15/2015
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14546887 FILING DATE: 11/18/2014
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14659008 FILING DATE: 03/16/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURE MULTI-TENANT DATA STORAGE

APPLICATION NUMBER: 14710522 FILING DATE: 05/12/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14710528 FILING DATE: 05/12/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14713792 FILING DATE: 05/15/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA IN THE CLOUD

APPLICATION NUMBER: 14749058 FILING DATE: 06/24/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING VIRTUAL MACHINE COMPUTING ENVIRONMENTS

APPLICATION NUMBER: 14749172 FILING DATE: 06/24/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE FILE SHARING METHOD AND SYSTEM

APPLICATION NUMBER: 14750562 FILING DATE: 06/25/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURING DATA USING MULTI-FACTOR OR KEYED DISPERSAL

APPLICATION NUMBER: 14828377 FILING DATE: 08/17/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SECURE DATA PARSER METHOD AND SYSTEM

APPLICATION NUMBER: 14875687 FILING DATE: 10/05/2015
PATENT NUMBER: ISSUE DATE:
TITLE: ELECTRONIC COMMERCE WITH CRYPTOGRAPHIC AUTHENTICATION

APPLICATION NUMBER: 14918176 FILING DATE: 10/20/2015
PATENT NUMBER: ISSUE DATE:
TITLE: TAPE BACKUP METHOD

APPLICATION NUMBER: 14931169 FILING DATE: 11/03/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURE WORKGROUP MANAGEMENT AND COMMUNICATION

APPLICATION NUMBER: 14949370 FILING DATE: 11/23/2015
PATENT NUMBER: ISSUE DATE:
TITLE: GATEWAY FOR CLOUD-BASED SECURE STORAGE

APPLICATION NUMBER: 14949519 FILING DATE: 11/23/2015
PATENT NUMBER: ISSUE DATE:
TITLE: GATEWAY FOR CLOUD-BASED SECURE STORAGE

APPLICATION NUMBER: 14969651 FILING DATE: 12/15/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURE REMOTE STORAGE

APPLICATION NUMBER: 14984087 FILING DATE: 12/30/2015
PATENT NUMBER: ISSUE DATE:
TITLE: SYSTEMS AND METHODS FOR SECURE DATA SHARING

APPLICATION NUMBER: FILING DATE: 11/23/2015
PATENT NUMBER: ISSUE DATE:
PCT NUMBER: US2015062188
TITLE: GATEWAY FOR CLOUD-BASED SECURE STORAGE

ASSIGNMENT RECORDATION BRANCH
PUBLIC RECORDS DIVISION

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 33438

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Security First Corp.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Andrew S. Price		
Title	CFO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/82C (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

No more than ten (10) patent practitioners total may be appointed as set forth below by name and registration number. This page need not be submitted if appointing the Patent Practitioner(s) associated with a Customer Number (see form PTO/AIA/82B):

Name	Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/371363
Filing Date	February 10, 2012
First Named Inventor	Mark S. O'Hare
Title	Systems and Methods for Cryptographically Splitting and Storing Data
Art Unit	2492
Examiner Name	Tae K. Kim
Attorney Docket Number	T00531-C1-B

SIGNATURE of Applicant or Patent Practitioner

Signature	/Kent B. Chambers/	Date (Optional)	January 20, 2021
Name	Kent B. Chambers	Registration Number	38,839
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	41696275
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	104093-0002-105
Receipt Date:	20-JAN-2021
Filing Date:	10-FEB-2012
Time Stamp:	16:02:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	SecurityFirst_POA_82B.pdf	189734 46d2dc88cf8db0f87d2e41a49f19f2167b6db9f9	no	3

Warnings:

Information:					
2	Assignee showing of ownership per 37 CFR 3.73	T00531-C1-B_Statement_373.pdf	118551 de71794a71c0b0850315db2a5bdee736925641c8	no	3
Warnings:					
Information:					
3	Power of Attorney	T00531-C1-B_POA_82A.pdf	213487 1355c801533966b5948bb62ec59d2c588d37dd88	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	521772	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Security First Corp.

Application No./Patent No.: 13/371363 Filed/Issue Date: February 10, 2012

Titled: Systems and Methods for Cryptographically Splitting and Storing Data

Security First Corp., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: Orsini et al. To: Security First Corp.

      The document was recorded in the United States Patent and Trademark Office at

      Reel 028094, Frame 0896, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Kent B. Chambers/	January 20, 2021
Signature	Date
Kent B. Chambers	38,839
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	T00531-C1-B

CONFIRMATION NO. 7984

33438
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

POA ACCEPTANCE LETTER

OC00000122860184

Date Mailed: 01/27/2021

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/20/2021.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/vnguyen/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	104093-0002-105

CONFIRMATION NO. 7984

POWER OF ATTORNEY NOTICE

15314
Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

OC000000122860129

Date Mailed: 01/27/2021

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/20/2021.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/vnguyen/

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Attorney Docket No.: 0890103C2

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: **Security First Innovations, LLC**

Application No./Patent No.: **13/371,363** Filed/Issue Date: **2/10/2012**

Titled: **SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA**

Security First Innovations, LLC, a **Limited Liability Company**,
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3, or 4 below):

1. [X] The assignee of the entire right, title, and interest

2. [ ] An assignee of less than the entire right, title and interest (check applicable box):

   [ ] The extent (by percentage) of it's ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   [ ] There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. [ ] The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made).

   The other parties, including inventors, who together won the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. [ ] The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified documents(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. [ ] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel, Frame, or for which a copy thereof is attached.

OR

B. [X] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: O'Hare, et al. To: SECURITY FIRST CORP.

   The document was recorded in the United States Patent and Trademark Office at Reel 028094, Frame 0896, or for which a copy thereof is attached.

2. From: SECURITY FIRST CORP. To: SECURITY FIRST INNOVATIONS, LLC

   The document was recorded in the United States Patent and Trademark Office at Reel 061262, Frame 0865, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From:_____ To:_____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From:_____ To:_____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From:_____ To:_____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From:_____ To:_____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/farshad farjami/	February 16, 2023
Signature	Date
Farshad **Farjami, Esq.**	**41,014**
Printed or Typed Name	Title or Registration Number

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	47548272
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	33438
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	T00531-C1-B
Receipt Date:	16-FEB-2023
Filing Date:	10-FEB-2012
Time Stamp:	18:41:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		0890103C2_POA_Feb_16_23.pdf	1161103 7f52d43694672efa0e8a082919f991544fd15ad1	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Power of Attorney	2	6
Warnings:			
Information:			
	Total Files Size (in bytes):	1161103	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/371,363
Filing Date	2/10/2012
First Named Inventor	O'Hare
Title	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
Art Unit	
Examiner Name	
Attorney Docket Number	0890103C2

SIGNATURE of Applicant or Patent Practitioner

Signature	/Farshad Farjami/	Date (Optional)	2/16/2023
Name	Farshad Farjami	Registration Number	41014
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/80 (11-08)
Approved for use through 11/30/2020. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 189503

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 189503

OR

☐ Firm or individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Security First Innovations, LLC
44095 Pipeline Plaza, Suite 140
Ashburn, VA 20147

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	8/30/2022
Name	Mr. Leo Guthart	Telephone	5169460376
Title	Member, Security First Innovations, LLC		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM
www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: February 16, 2023

To: United States Patent and Trademark Office
Examiner: Kim, Tae K.; Art Unit: 2492

Re: **Application Serial No.: 13/371,363**
Filing Date: 2/10/2012; First-Named Inventor: O'Hare
Attorney Docket No.: 0890103C2

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 6

Message:

Enclosed, please find:

1. Transmittal for Power of Attorney (Form PTO/AIA/82A);
2. Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96); and
3. Power of Attorney Document (Form PTO/AIA/82B)

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain PRIVILEGED AND CONFIDENTIAL information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	0890103C2

CONFIRMATION NO. 7984

189503
Security First Innovations, LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

POA ACCEPTANCE LETTER

OC000000137491950

Date Mailed: 03/07/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/16/2023.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sstephanos/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Mark S. O'Hare	T00531-C1-B

CONFIRMATION NO. 7984

POWER OF ATTORNEY NOTICE

33438
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

OC000000137491936

Date Mailed: 03/07/2023

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/16/2023.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sstephanos/

Electronic Acknowledgement Receipt

EFS ID:	47878911
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	189503
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	0890103C2
Receipt Date:	20-APR-2023
Filing Date:	10-FEB-2012
Time Stamp:	19:46:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		0890103C2_Req_for_Cert_of_Correction_Apr_20_23.pdf	84710 70b137a68bb2e7a4e9facceba062757f57e4f74d	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Request for Certificate of Correction	2	4
Warnings:			
Information:			
	Total Files Size (in bytes):	84710	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): **O'Hare et al.** Patent No.: **9,294,444** Issue Date: **3/22/2016** Filing Date: **2/10/2012** Application Serial No.: **13/371,363** Title: **SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA**	Group Art Unit: 2492 Examiner: Kim, Tae K.

REQUEST FOR A CERTIFICATE OF CORRECTION FOR PTO'S ERROR

Commissioner for Patents
Office of Patent Publication
Attention: Certificates of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

Applicants respectfully request that a certificate of correction be issued to correct some clerical errors made by the Patent Office on the face of the above-referenced patent, and no fault of applicant, as shown in the enclosed copy of Form PTO-1050.

The Assistant Commissioner is hereby authorized to charge or credit Deposit Account No. **50-0731** for any deficiency or overpayment in the fees required for the filing of this request for a certificate of correction.

A certificate of correction is respectfully requested. Applicants respectfully invite the examiner to contact the undersigned for any questions.

Respectfully submitted,
Farjami & Farjami LLP

Dated: April 20, 2023

By: */farshad farjami/*
Farshad Farjami
Reg. No. 41,014
Attorney for Applicants

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Ste. 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

April 20, 2023
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature

PTO/SB/44 (09-07)
Approved for use through 08/31/2010. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : **9,294,444**

APPLICATION NO. : **13/371,363**

ISSUE DATE : **3/22/2016**

INVENTOR(S) : **O'Hare et al.**

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the face of the patent, in Section (60), "provisional application No. 60/222,146." should be -- provisional application No. 60/622,146.--

MAILING ADDRESS OF SENDER:

PATENT NO: 9,294,444

Farshad Farjami, Esq.
Farjami & Farjami LLP
26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: April 20, 2023

To: Office of Patent Publication, Attention: Certificates of Correction Branch
United States Patent and Trademark Office
Examiner: Kim, Tae K.; Art Unit: 2492

Re: **Application Serial No.: 13/371,363**
Patent No: 9,294,444
Filing Date: 2/10/2012; First-Named Inventor: O'Hare
Attorney Docket No.: 0890103C2

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 4

Message:

Enclosed, please find the Request for a Certificate of Correction and Form PTO-1050.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain PRIVILEGED AND CONFIDENTIAL information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.