300
350
310
354
352
356
322
320
318
Memory unit
Secure CPU (RISC)
Crypto HW
Memory
Control CPU (RISC)
Host IF
Clear TS
360
316
314
368
Fuse bank
HW Security Controller
Descrambler
Encrypted TS
Demod
External memory IF
362
366
324
312
311
Key Manager
Control IF
Control IF
Tuner

FIG. 3

Integrated
450 secure element
400
Host IF
HW
accelerator #1
Secure
CPU
452
480
453
466
HW
accelerator #2
BOOT
ROM
Demod
IF
Demod logic
and SOC
infrastructure
420
Remote
Flash
455
456
460
HW
accelerator #n
NVM
registers
Secure
RAM
410

FIG. 4

FIG. 5

Petitioner Samsung Ex-1004, 0503

600
Secure Sub system Process
HUK
(OTP)
S610
1st
AES
unit
S620
SEED
RNG
Seed generation process
(on- chip RNG)
Encryption
key
CLEAR DATA
RAM
2nd
AES
unit
S630
S640
ENCRYPTED
DATA RAM
S650
SEED
Stored in off-chip
remote memory

FIG. 6

700
Power on reset
t1
HOST IF disabled
HOST IF enabled
HOST IF disabled
Secure CPU task
OTP sensing
Data Wipe off
SE READY
SE LOCKED
t3
Security Element (SE) State
X
SECURE MODE (default)
SECURE MODE
SE_RST_IN
DCPU action
t2
SE_READY_OUT
t4
SE_BOOTSTART_IN
D-CPU or S-CPU downloads CAS FW into internal SE memory
t5
S-CPU Activity
710
Boot process (from ROM)
t6

FIG. 7

Off-chip non-volatile memory
Remote
NVM (Flash)
880
Firmware
882
850
Demodulator SOC 800
Integrated Secure Element
852
S-CPU
864
Firewall
862
Demod interface
(Slave)
Download
process
(Master)
Interface
unit
854
S-RAM
856
BOOT
ROM
HW Accelerator
#2
858
Firmware
860
NVM
HW Accelerator
#n
Demod Logic and
SOC infrastructure
870
810

FIG. 8

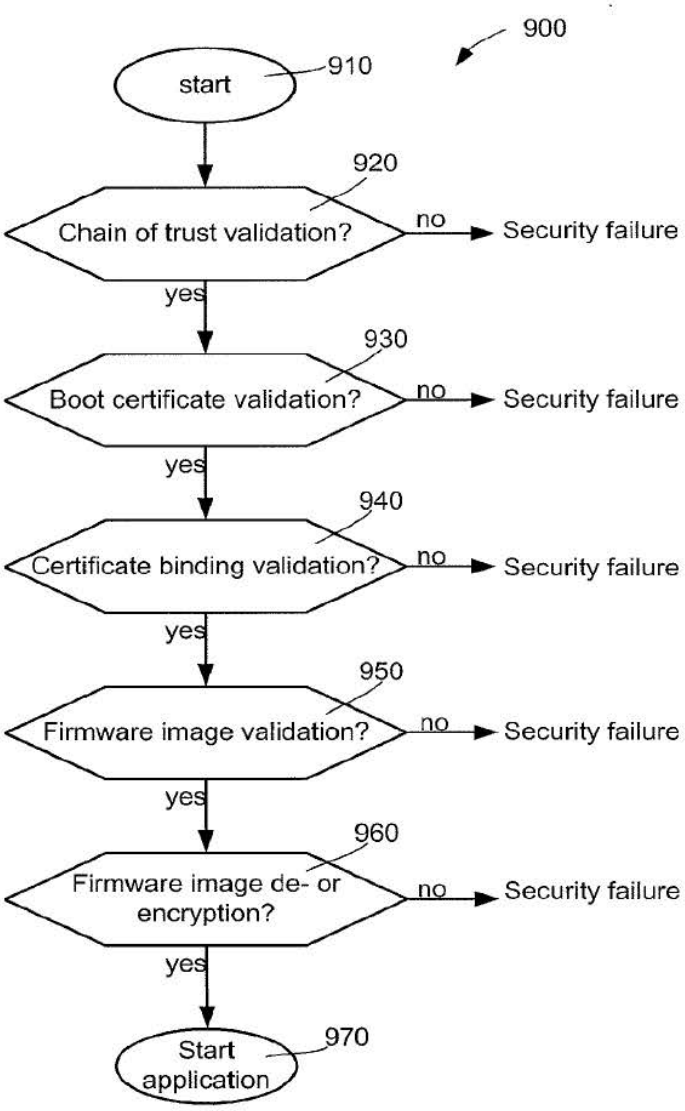


FIG. 9

Petitioner Samsung Ex-1004, 0507

1000
Certificate loaded into RAM
Certificate
1100
RPK
1102
SHA
1104
HV
SAME ?
1105
OTP register
DRPK
1108
Yes - continue
No
1107
SECURITY FAILURE
1114
SVPbK_SIG
1112
RSA
EK1
1115
SVPbK
1116
SAME ?
1117
SECURITY FAILURE
Yes - continue
SDPbK_SIG
1122
RSA
1124
EK2
1125
SDPbK
1126
SAME ?
1127
SECURITY FAILURE
Yes - continue
SPPbK_SIG
1132
RSA
1134
Ek3
1135
SPPbK
1136
SAME ?
1137
SECURITY FAILURE
Yes - continue

FIG. 10

1100
Certificate loaded into RAM
1100
Certificate
Data...
...
SPPbK
CERT_SIG
1166
1156
1152
SHA
HV1
1154
RSA
EK5
1175
SAME?
No
SECURITY FAILURE
1177
Yes- continue

FIG. 11

1200
Certificate loaded into RAM
Certificate
1100
...
1205
1208
1202
OTP register
DVID
SAME?
DVID
...
No 1207
SECURITY FAILURE
Yes- continue

FIG. 12

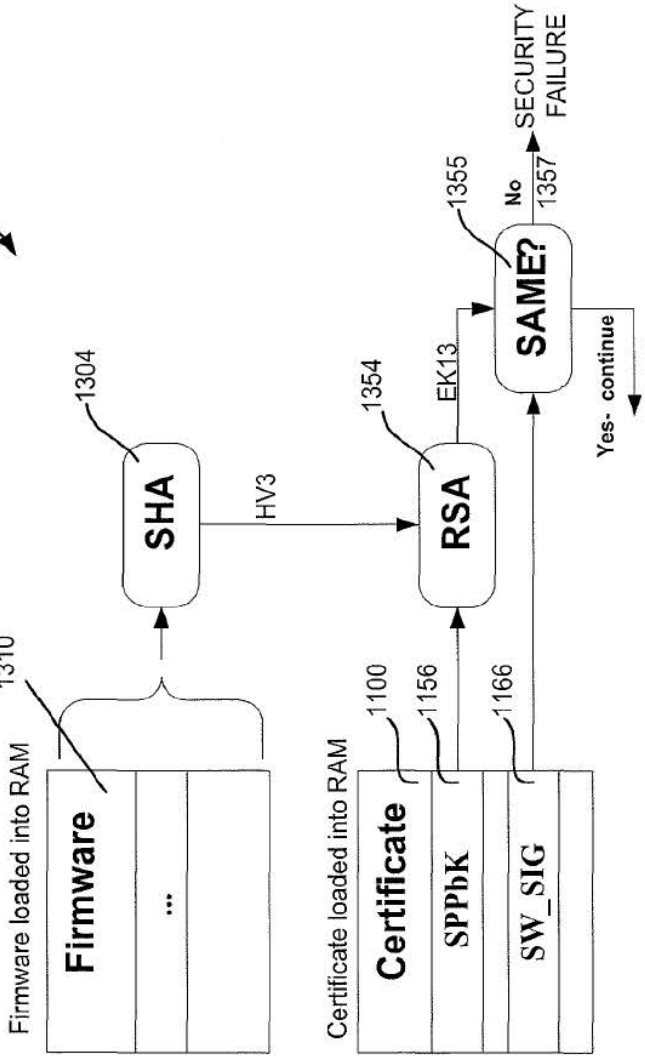


FIG. 13

Petitioner Samsung Ex-1004, 0511

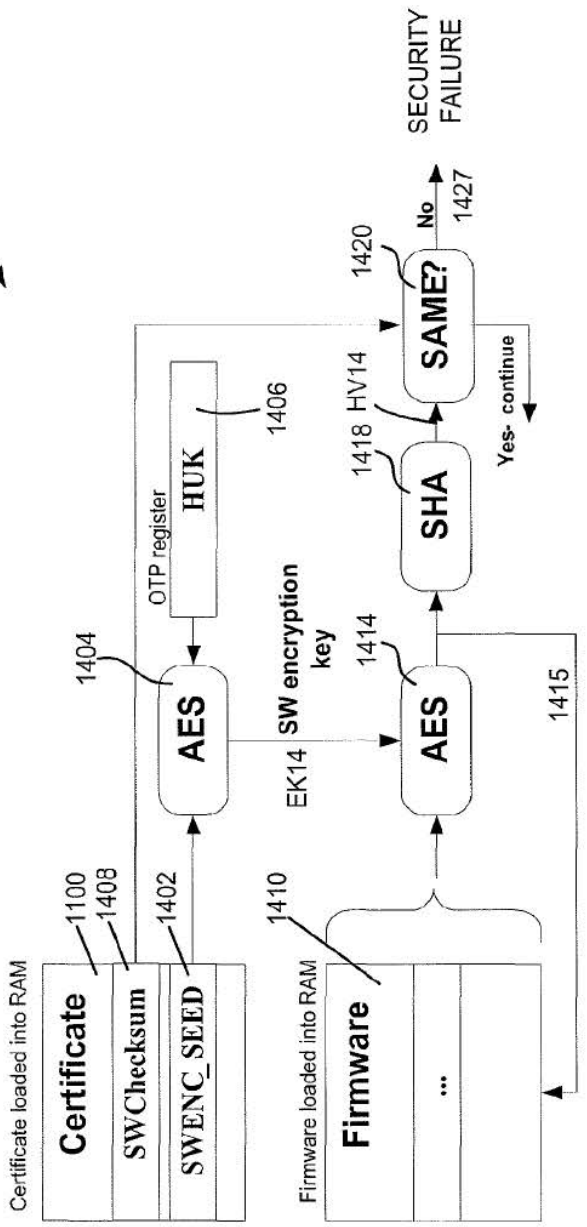


FIG. 14A

Petitioner Samsung Ex-1004, 0512

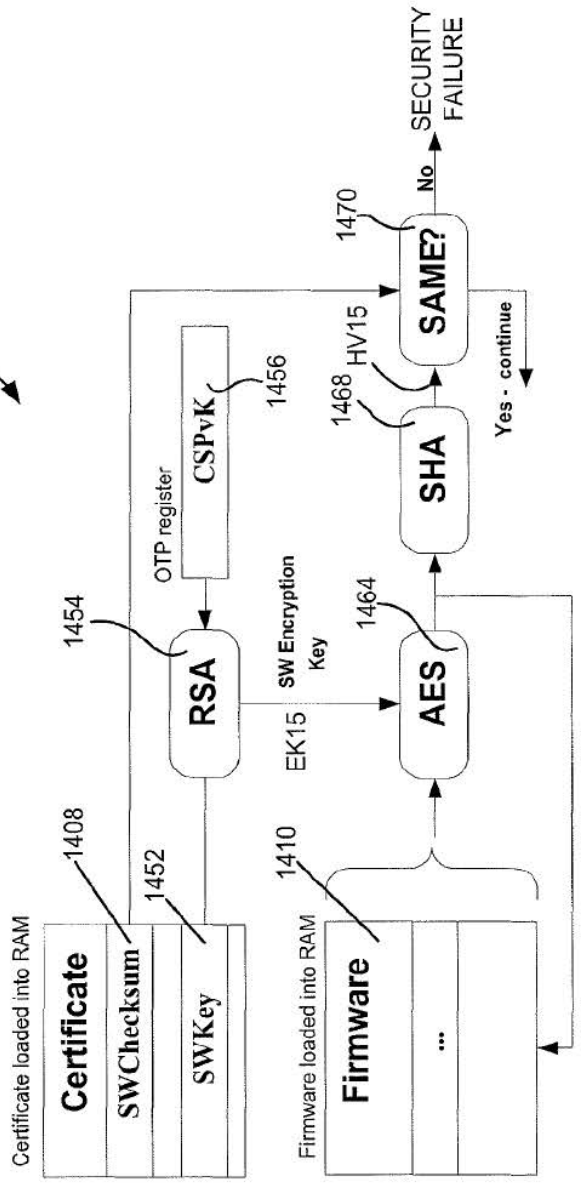


FIG. 14B

Petitioner Samsung Ex-1004, 0513

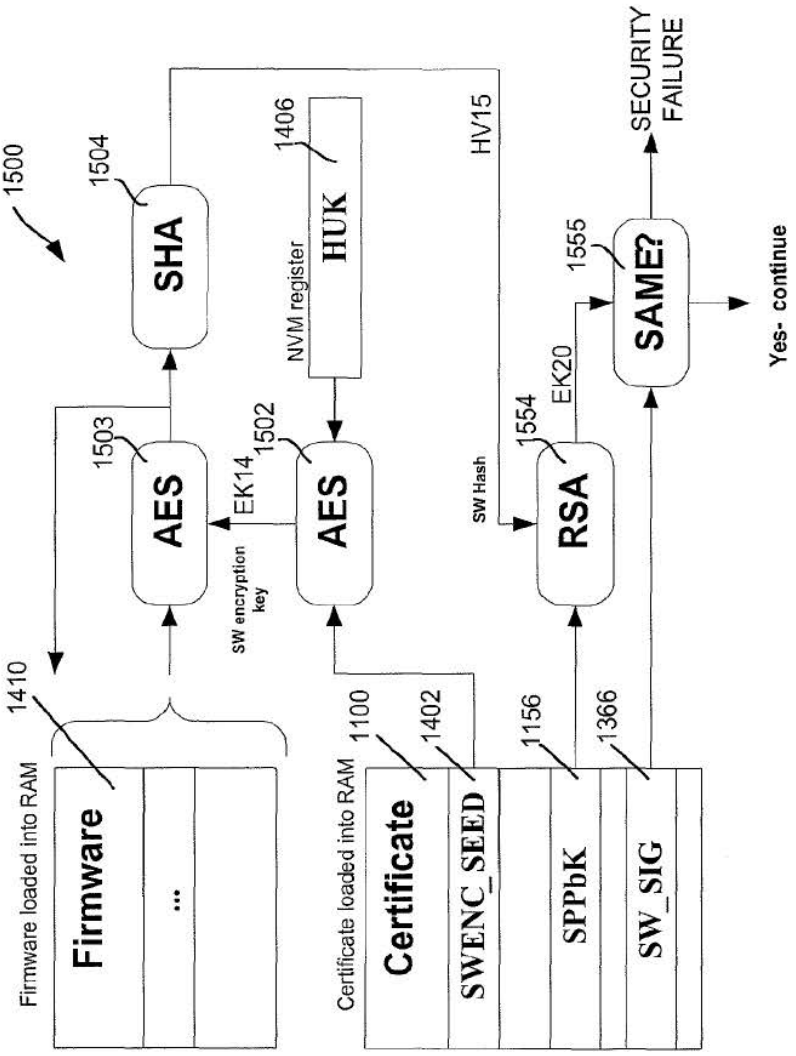


FIG. 15

Petitioner Samsung Ex-1004, 0514

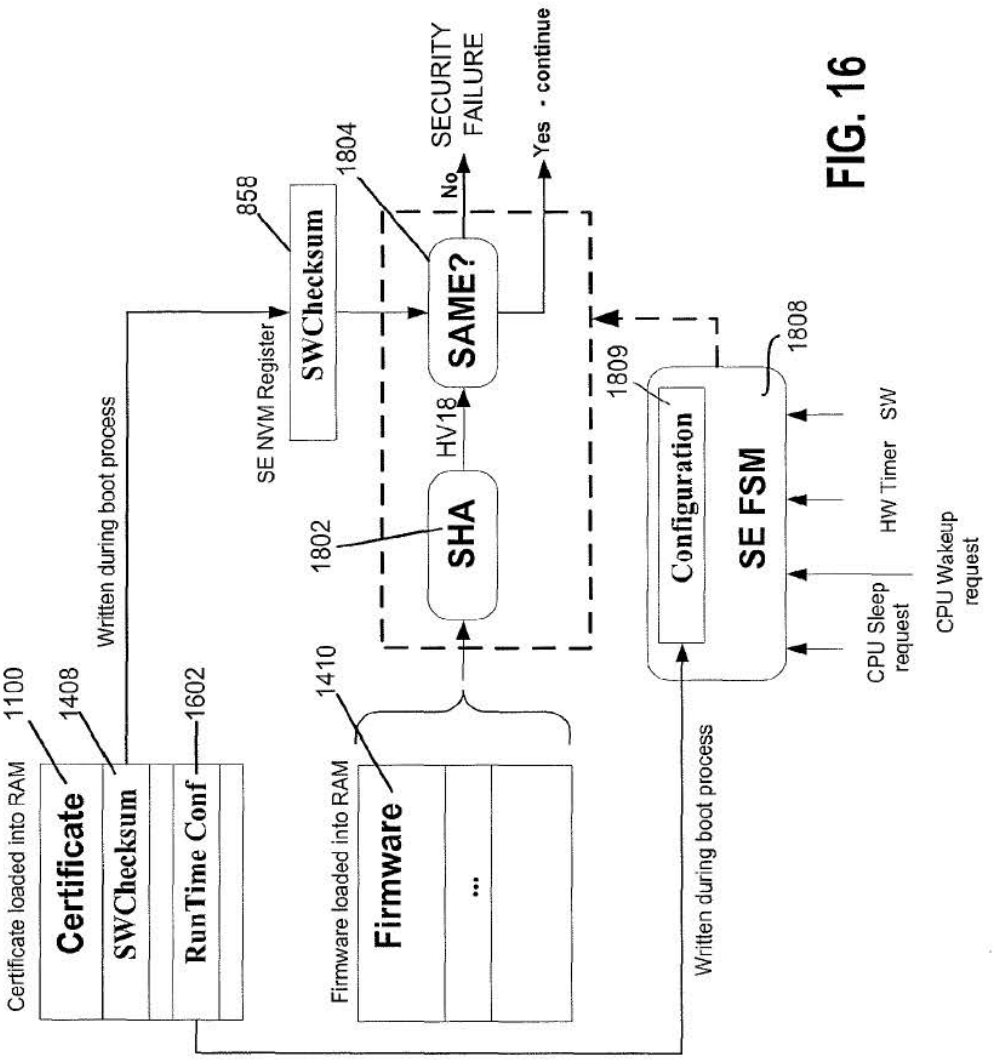


FIG. 16

Petitioner Samsung Ex-1004, 0515

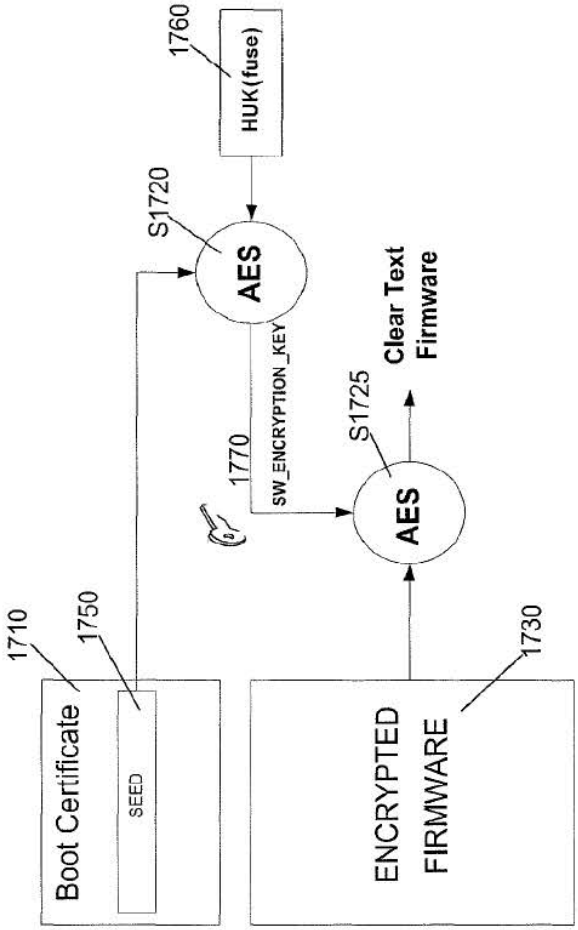


FIG. 17

Petitioner Samsung Ex-1004, 0516

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 05/06/2016

Barnes & Thornburg LLP (Intel)
c/o CPA Global
900 2nd Avenue South, Suite 600
Minneapolis, MN 55402

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
05/06/2016	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Petitioner Samsung Ex-1004, 0517

Office Action Summary	Application No. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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 *2/15/2016*.

☐ 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) *48-71* 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) *48-71* 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 *2/17/2016*.

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

4) ☐ Other: _____.

Petitioner Samsung Ex-1004, 0518

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 02/17/2016 has been considered by the Examiner.

Status of Claims

3. This Office Action is issued in response to the Amendment filed on 02/15/2016.

Claims 48-71 are pending in this Office Action.

Claims 48-56, 58, 59, 62-71 are amended.

Claims 1-47 are cancelled.

Drawing

4. The previous drawing objection has been withdrawn in response to applicants' amendments.

Claim Rejections - 35 U.S.C § 112

5. Previous 112(b) rejection has been withdrawn in response to applicants' amendments.

Claim Rejections - 35 U.S.C § 101

6. The previous 101 rejections have been withdrawn in response to applicant's amendments**.**

Response to Arguments

7. Applicants' arguments regarding 35 U.S.C. § 103 Claim Rejections are moot in view of new grounds of rejection.

Claim Rejections - 35 U.S.C. § 103

8. The following is a quotation of pre-AIA 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.

9. Claims 48-52, 56-61, 64-69 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar".

Regarding claim 48, Chou discloses system-on-a-chip apparatus comprising:

[a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to:]

generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce (Fig. 1 and associated text: Client hello message 150 is sent from first network device-client- to second network device-server. Fig. 2A and associated text: Client hello message 150 includes first random number-random nonce. Chou discloses that a random number is generated internally within the second device (Col. 6, line 67 and Col.7, line1 and claim 7). Therefore, it is obvious to apply this feature of generating random number internally within a device so that the first device can generate its own random number);

perform a cryptographic key exchange with the server (Fig. 1, step 180 and associated text: client key exchange message is sent to second network device-server) to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session (Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120);

[encrypt the session key based on the security key]; and

store the encrypted session key in [the secure memory] (Chou does not explicitly disclose about storing the session key; however, in order for using the key to communicate between the two device in a period of time-a session of communication-, it is obvious that the key must be stored), [the system-on-a-chip] to establish the secure communication session with the server over the network using the session key(Col. 4, lines 60-63: Client Hello message 150 is a message that provides second network

device 120 with information that is used to establish secured communications between network devices 110 and 120. Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120).

Chou does not explicitly disclose **a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key** and is stored **in the secure memory**.

However, in the field of protecting data, Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: It is obvious that Processor 22 could also be a secure processor-TPM/system-on-a chip-with Proc. Unit 30 is a secure nonvolatile and the Proc. Unit 30 is the execution engine. Col. 2, lines 17-19: In a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM.) that was encoded in the secure memory during a manufacturing process of the system-on-a-chip (Fig. 1: Proc. Unit 30 has PUK 70. Col. 3, lines 2-7: a processing unit key or PUK is a

cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form), the session key is encrypted based on the security key and is stored in the secure memory (Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, it is obvious that PKU is also used to encrypt SK to protect SK from attacker.)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou's invention of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key and the session is encrypted using a key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip as taught by Kumar. The motivation to do so would be to protect data and to seal sensitive information or secrets to a secure area as taught by Kumar (Col. 1, line 8 and Col. 2, lines 17-19).

Regarding claim 49, Chou and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein,

the security engine is further to receive a server nonce from the server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (Chou, Figs. 1, 2B and associated text: server hello message 160-response message- includes random number 260. Chou does not explicitly disclose that the server nonce is stored. However, it is known in the art to store data for later retrieving. Combining with Kumar's

teaching of secure memory as in claim 48 above, it is obvious to have the server's nonce stored in the secure memory to protect the nonce from being compromised).

Regarding claim 50, Chou and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the server (Chou, Col. 5, lines 50-61: first network device generates Pre-Master key. Pre-master key is encrypted with the public key of second network device and is sent to second network device-server. Kumar, Col. 3, lines 27-34: 3PKs are used to generate session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. The combination of Chou and Kumar's teaching makes it obvious that pre-master key is generated and encrypted using the security key of the security engine).

Regarding claim 51, Chou and Kumar disclose the system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Kumar, Col. 1, lines 41-46: The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, the combination of Chou and Kumar's teachings make it obvious that PKU is also used to encrypt pre-master key and store it in the secure memory to protect it from attacker.)

Regarding claim 52, Chou and Kumar disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine is further to:

generate the session key as a function of the pre-master key (Col. 5, lines 61-65: a master key is produced from the pre-master key); and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Claims 56-58 and 64-66 are rejected because they disclose similar subject matter to claims 48-50 respectively.

Claims 59 and 67 are rejected because they disclose similar subject matter to claim 48.

Claims 60-61 and 68-69 are rejected because they disclose similar subject matter to claim 52.

10. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho".

Regarding claim 53, Chou and Kumar disclose the system-on-a-chip apparatus of claim 48. Chou further discloses that client hello message includes list of cryptographic algorithms supported by first network device 110 such as Ephemeral Diffie-Hellman (DHE). Chou also discloses data is encrypted with server's private key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server).

Chou and Kumar do not explicitly disclose wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie- Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.

However, in the field of data communication and security, Ho discloses the security engine to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key (Fig. 3, step 0a and associated text: a secret (private) key is chosen and a public key is computed. Paragraph [0038]: public key generated initiating device A-client- is used for Diffie-Hellman key exchange), sign the public Diffie-Hellman client key using a security key of the security engine (it is obvious to apply Chou's teaching of encrypting-signing- data before sending as stated above), and send the signed public

Diffie-Hellman key to the server (Fig. 3, Step 2a and associated text: Public key PKa is sent to device B-server).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Kumar's inventions of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Ho's invention of using Diffie-Hellman for generating key. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Regarding claim 54, Chou, Kumar, and Ho disclose the system-on-a-chip apparatus of claim 53. Ho further discloses wherein the security engine to receive a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A) and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key (step 5a and associated text: DHkey-session key- is computed based on Private key of device A –client- and public key of Device B-server).

Regarding claim 63, Chou and Kumar disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 9 above). Chou further disclose:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by

each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

signing the hash code using a security key stored in a secure memory of the security engine (Chou discloses data is encrypted with server's private key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server. Kumar, Col. 1, lines 41-46: The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. The combination of Chou and Kumar' teachings makes it obvious that the hash code could be signed using a security key stored in the secure memory of the security engine).

Chou and Kumar do not explicitly disclose sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

However, in the field of data communication and security, Ho discloses sending a hash client certificate verification message to the server, the client certificate verification message including the signed hash code (Fig. 3, steps 5a and 7a and associated text: Verification Va1 is computed and sent to device B-server. With Chou's teaching of signing data before sending as above, the client certificate verification message including the signed hash code is sent to the server).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Kumar's inventions of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Ho's invention of using hash code for verification message. The motivation to do so would be to ensure secure communication for involved parties.

Claims 62 and 70 are rejected because they disclose similar subject matter to the combination of claims 53 and 54.

Claim 71 is rejected because it discloses similar subject matter to claim 63.

11. Claim 55 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho", and further in view of Peyravian et al (US application No. 2004/0158715), hereinafter "Peyravian".

Regarding claim 55, Chou and Kumar disclose the system-on-a-chip apparatus of claim 48. Kumar also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou and Kumar do not explicitly disclose wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server.

However, in the field of data communication and security, Ho discloses the security engine to receive Diffie-Hellman [global values] and a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A-client).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Kumar' s inventions of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Ho's invention of using Diffie-Hellman for generating key. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Chou, Kumar, and Ho do not explicitly disclose the security engine to receive Diffie-Hellman global values.

However, in the field of data security, Peyravian discloses a prime modulus-global Diffie-Hellman value- is sent to a device (paragraph [0011]: prime modulus is sent to server, so that the server can use this prime modulus as one of parameters to generate Diffie-Hellman symmetric secret key-session key. It is obvious that the client

and server can switch roles. In other words, the server can be the sender instead of receiver of the prime modulus).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Kumar, and Ho' inventions of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to sensitive information with using Diffie-Hellman for generating key and with Peyravian's invention of sending a global value. The motivation to do so would be to provide an improved way to distribute and authenticate public cryptographic keys as taught by Peyravian (paragraph [0010].

The combination of Chou and Ho's references discloses store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage (Chou, Abstract: secure memory stores cryptographic key. Ho, Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A-client).

Conclusion

12. 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 mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH T. LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-Th 7:00 am- 1:00 pm.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. 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.

/THANH T. LE/

Examiner, Art Unit 2495

/Jason K. Gee/

Primary Examiner AU 2495

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,657,390 A	08-1997	Elgamal; Taher	H04L29/06	713/151
*	B	US-2005/0005093 A1	01-2005	Bartels, Andrew	G06F21/606	713/150
*	C	US-2005/0213766 A1	09-2005	Goss, Steven C.	G06F21/72	380/277
*	D	US-2005/0289343 A1	12-2005	Tahan, Thomas	G06F21/72	713/169
*	E	US-2006/0041938 A1	02-2006	Ali; Asad Mahboob	G06Q20/341	726/14
*	F	US-7,069,352 B2	06-2006	Pezzini; Saverio	G06F13/385	710/3
*	G	US-7,096,352 B2	08-2006	Kang; Kyoung Jin	H04L67/04	380/270
*	H	US-2009/0280905 A1	11-2009	Weisman; Jordan K.	A63F13/08	463/40
*	I	US-2010/0042839 A1	02-2010	Ho; Jin-Meng	H04L9/3226	713/169
*	J	US-2010/0205443 A1	08-2010	Zhao; Yunlei	H04L9/3218	713/171
*	K	US-7,966,646 B2	06-2011	Chou; Randy	H04L63/166	726/2
*	L	US-2011/0231923 A1	09-2011	Bollay; Benn Sapin	H04L63/166	726/9
*	M	US-2011/0235806 A1	09-2011	Fukuda; Naohiro	H04L9/0825	380/282

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.

Petitioner Samsung Ex-1004, 0534

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,364,975 B2	01-2013	Kumar; Mohan J.	G06F21/57	380/277
*	B	US-8,615,787 B2	12-2013	Murray; Bruce	H04L63/0853	380/281
*	C	US-8,627,440 B2	01-2014	Mowers; David R.	H04L63/0807	380/279
*	D	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
*	E	US-2007/0094503 A1	04-2007	Ramakrishna; Preetam	H04L9/0822	713/172
	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	
	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.

Petitioner Samsung Ex-1004, 0535

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

CPC- SEARCHED		
Symbol	Date	Examiner
H04L9/0838 H04L9/0841 H04L9/0861 with text	8/14/2015	T.L

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and assignee search with text	8/14/2015	T.L
Interference search with text	8/14/2015	T.L
International and foreign search	8/14/2015	T.L
713/171 with text	8/14/2015	T.L
text based search of claim keywords and synonyms	8/14/2015	T.L
NPL search in IP.com	8/14/2015	T.L
Update Search	4/27/2016	T.L

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

Petitioner Samsung Ex-1004, 0536

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	8014530		2011-09-06	Ernest Brickell	
/T.L./	2	7802085		2010-09-21	Gary L. Graunke	
/T.L./	3	7747862		2010-06-29	Shlomo Ovadia	
/T.L./	4	7350083		2008-03-25	Steven E. Wells	
/T.L./	5	6948065		2005-09-20	David W. Grawrock	
/T.L./	6	7600132		2009-10-06	Fadi A. Mahmoud	
/T.L./	7	6401208		2002-06-04	DEREK L DAVIS	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Petitioner Samsung Ex-1004, 0537

Receipt date: 02/17/2016

13997412 - GAU: 2495

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	20080244267		2008-10-02	Vincent J. Zimmer	
/T.L./	2	20070138229		2007-06-21	Yasuyuki Fujimoto	
/T.L./	3	20110154023		2011-06-23	Ned M. Smith	
/T.L./	4	20060005011		2006-01-05	Masakazu Satoh	
/T.L./	5	20070240200		2007-10-11	Hee-chul Han	
/T.L./	6	20130297936		2013-11-07	Hormuzd M. Khosravi	
/T.L./	7	20050144436		2005-06-30	Tse-Min Chen	
/T.L./	8	20030236970		2003-12-25	Rodney Wendell Palmer	
/T.L./	9	20090319804		2009-12-24	Zheng QI	
/T.L./	10	20080256363		2008-10-16	Boris Balacheff	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

/T.L./	11	20070192611		2007-08-16	Shamanna M. Datta	
/T.L./	12	20020112161		2002-08-15	Fred C. Thomas	
/T.L./	13	20080077809		2008-03-27	Don L. Hayler	
/T.L./	14	20110161645		2011-06-30	Jiang Zhang	
/T.L./	15	20050213766		2005-09-29	Steven C. Goss	
/T.L./	16	20080005586		2008-01-03	Peter Munguia	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/T.L./	1	2011119985	WO		2011-09-29	Maxlinear, Inc.		
/T.L./	2	2013089725	WO		2013-06-20	Intel Corporation		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Receipt date: 02/17/2016

13997412 - GAU: 2495

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
/T.L./	1	Taiwanese Office Action issued in connection with Taiwanese Application No. 101147203, completed December 29, 2014, 11 pages	X
/T.L./	2	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065072, mailed June 26, 2014, 6 pages.	☐
/T.L./	3	International Search Report and Written Opinion received for International Application No. PCT/US2011/065072, Mailed July 18, 2012, 10 Pages	☐
/T.L./	4	Platform Independent Overall Security architecture in multi-processor system-on-chip intergrated circuits for use in mobile phones and handheld devices. Ashkenazi et al. ElSevier (2007)	☐
/T.L./	5	Data Security Architure using Embedded Chip. Thomas et al. IJCSNS (May 2011)	☐
/T.L./	6	Scalable Architectural Support for Trusted Software. Champagne et al. IEEE (2009)	☐
/T.L./	7	Secure Memory Accesses on Networks-on Chip. Fiorin et al. IEEE (2009)	☐
/T.L./	8	Extended European Search Report issued in connection with European Application No. 11877254.0 - 1853, dated July 17, 2015, 8 pages	☐
/T.L./	9	"HITACHI, Ltd., "Digital Transmission Content Protection Specification Revision 1.7," December 14, 2011, Retrieved from the Internet: URL: http://www.dtcp.com/documents/dtcp/info-20111214-dtcp-v1-rev-1-p-7.pdf (retrieved on 2014-07-21), Chapter 4: Full Authentication and Chapter 6: Content Channel Management and Protection.	☐
/T.L./	10	Intel Corp., Product Brief: Intel Atom Processor CE4100, 2009, Pg. 1-4	☐

Petitioner Samsung Ex-1004, 0540

Receipt date: 02/17/2016

13997412 - GAU: 2495

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

/T.L./	11	Digital Transmission License Administrator, Digital Transmission Content Protection Specification, March 19, 2010, Volume 1, Pg. 11, 26-29, and 36-38	☐
/T.L./	12	Broadcom, August 24, 2011, What is BCM7309 - Single-Chip Back-End Set-Top Decoder, http:// Web.archive.org/web/20110824145230/httP//www.broadcom.com/products/Cable/Cable-Set-Top-Box-Soluctions/BCM7309	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Thanh Le/	Date Considered	04/27/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Petitioner Samsung Ex-1004, 0541

Receipt date: 02/17/2016

13997412 - GAU: 2495

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Scott R. Powell/	Date (YYYY-MM-DD)	2015-02-17
Name/Print	Scott R. Powell	Registration Number	58378

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0542

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 record s.

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.

Petitioner Samsung Ex-1004, 0543

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S72	2	("20040243823").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/04/27 13:17
S73	3	("20050114687").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/04/27 13:21
S74	2	("20070156987").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/04/27 13:24
S75	3	("20080022395").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/04/27 13:25
S76	5846	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) with ((static non-volatile built-in manufactur$3) near2 key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 13:35
S77	4765	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) near5 ((static non-volatile built-in manufactur$3) near2 key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 13:36
S78	201	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) near5 ((static non-volatile built-in manufactur$3) near2 key)) and ((H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.(713/171).ccls.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 13:40

Petitioner Samsung Ex-1004, 0544

S79	31	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) near5 ((static non-volatile built-in manufactur$3) near2 ((cryptographic encrypt$3 decrypt$3) adj key))) and ((H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.(713/171).ccls.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 13:41
S80	25	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) near5 (manufactur$3 near5 ((cryptographic encrypt$3 decrypt$3) adj key))) and ((H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc. (713/171).ccls.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 14:00
S81	14	S80 not S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/27 14:01
S82	7	(("20110154023") or ("7350083") or ("20130046981")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/04/27 14:11
S83	12	(US-20080244267-$ or US-20120257757-$ or US-20130046981-$ or US-20110154023-$).did. or (US-8254578-$ or US-6449720-$ or US-8571221-$ or US-8549297-$ or US-8364975-$ or US-8296581-$ or US-7366306-$ or US-7350083-$).did.	US-PGPUB; USPAT	OR	ON	2016/04/27 17:07
S84	10	S83 and (manufactur$3 near5 ((cryptographic encrypt$3 decrypt$3) adj key))	US-PGPUB; USPAT	OR	ON	2016/04/27 17:09
S85	17	(@pd<"20111215" @ad<"20111215") and ((chip token storage device CPU processor hardware SOC system-on-a-chip microprocessor memory microcontroller circuit) near5 ((static non-volatile built-in manufactur$3) near2 key)) and ((encrypted adj session adj key) with stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/28 17:44
S86	266	(@pd<"20111215" @ad<"20111215") and ((encrypted adj session adj key) near5 stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/28 17:51
S87	259	S86 not S85	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2016/04/28 17:52

Petitioner Samsung Ex-1004, 0545

			EPO; JPO; DERWENT; IBM_TDB			
S88	9	(@pd<"20111215" @ad<"20111215") and ((encrypted adj session adj key) near5 stor$3 with secure with (storage memory))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/04/28 18:10

EAST Search History (Interference)

< This search history is empty>

4/28/2016 6:35:24 PM
C:\Users\tle22\Documents\EAST\Workspaces\13997412.wsp

Petitioner Samsung Ex-1004, 0546

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016							
	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	-	-							

Petitioner Samsung Ex-1004, 0547

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016							
	37	-	-							
	38	-	-							
	39	-	-							
	40	-	-							
	41	-	-							
	42	-	-							
	43	-	-							
	44	-	-							
	45	-	-							
	46	-	-							
	47	-	-							
	48	✓	✓							
	49	✓	✓							
	50	✓	✓							
	51	✓	✓							
	52	✓	✓							
	53	✓	✓							
	54	✓	✓							
	55	✓	✓							
	56	✓	✓							
	57	✓	✓							
	58	✓	✓							
	59	✓	✓							
	60	✓	✓							
	61	✓	✓							
	62	✓	✓							
	63	✓	✓							
	64	✓	✓							
	65	✓	✓							
	66	✓	✓							
	67	✓	✓							
	68	✓	✓							
	69	✓	✓							
	70	✓	✓							
	71	✓	✓							

Petitioner Samsung Ex-1004, 0548

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
P41624US/45631-225521	13/997,412	April 3, 2014
First Named Inventor:	**Title:**	
Hormuzd M. Khosravi	Method and Device for Secure Communications Over a Network Using a Hardware Security Engine	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
   - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
   - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
     - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
     - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
       - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
       - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/Scott Rylan Powell/	June 28, 2016
Name (Print/Typed) Scott Rylan Powell	**Practitioner Registration No.** 58378

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

[✓] * Total of 1 forms are submitted.

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.

BARNES & THORNBURG LLP
11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	2495
Examiner:	Le, Thanh T.
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	April 3, 2014
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

June 28, 2016

RESPONSE TO FINAL OFFICE ACTION

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

Sir:

In response to the Office Action dated May 6, 2016, and contemporaneously with a request for consideration under the After Final Consideration Pilot Program 2.0 ("AFCP 2.0"), please consider the following:

Amendments to the Claims, which begin on page **2**; and

Remarks, which begin on page **9**.

AMENDMENTS TO THE CLAIMS

1-47. (Canceled)

48. (Currently Amended) A system-on-a-chip apparatus comprising:

a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to:

generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce;

perform a cryptographic key exchange with the remote server; [[to]]

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the symmetric session key based on the security key; and

store the encrypted session key in the secure memory,

the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key.

49. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory.

50. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server.

Petitioner Samsung Ex-1004, 0552

51. (Previously Presented) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory.

52. (Currently Amended) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to:

generate the session key as a function of the pre-master key; and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

53. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using the security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

54. (Currently Amended) The system-on-a-chip apparatus of claim 53, wherein the security engine is further to receive a public Diffie-Hellman server key from the remote server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

55. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the remote server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure memory.

56. (Currently Amended) A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

initiating, using the client device, a request for a secure communication session with a remote server over a network, the request including the random nonce;

Petitioner Samsung Ex-1004, 0553

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server; [[to]]

generate a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypting the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

storing the encrypted session key in the secure memory of the security engine of the system-on-a-chip; and

establishing, using the client device, the secure communication session with the remote server using the session key.

57. (Currently Amended) The method of claim 56, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the remote server; and further comprising:

receiving a ServerHello message from the remote server, the ServerHello message including a server nonce; and

storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

58. (Currently Amended) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating a pre-master key in the security engine;

encrypting the pre-master key using the security key of the security engine; and

sending the encrypted pre-master key to the remote server.

59. (Previously Presented) The method of claim 58, further comprising:

wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and

storing the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

Petitioner Samsung Ex-1004, 0554

60. (Currently Amended) The method of claim 58, wherein performing the cryptographic key exchange with the remote server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

61. (Currently Amended) The method of claim 60, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

62. (Currently Amended) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

signing the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

sending the signed public Diffie-Hellman key to the remote server;

receiving a public Diffie-Hellman server key from the remote server; and

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

63. (Currently Amended) The method of claim 56, further comprising:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the remote server;

signing the hash code using the security key stored in the secure memory of the security engine; and

sending a client certificate verification message to the remote server, the client certificate verification message including the signed hash code.

Petitioner Samsung Ex-1004, 0555

64. (Currently Amended) One or more non-transitory machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to:

generate a random nonce in a security engine of a system-on-a-chip of the computing device;

initiate a request for a secure communication session with a remote server over a network, the request including the random nonce;

perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server; [[to]]

generate, based on the cryptographic key exchange, a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

store the session key in the secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the remote server using the session key.

65. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to initiate a request for a secure communication session comprises to send a ClientHello message, including the nonce, to the remote server; and

wherein the plurality of instructions further cause the computing device to:

receive a ServerHello message from the remote server, the ServerHello message including a server nonce; and

store the server nonce in the secure memory of the security engine of the system-on-a-chip.

Petitioner Samsung Ex-1004, 0556

66. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate a pre-master key in the security engine;

encrypt the pre-master key using the security key of the security engine; and

send the encrypted pre-master key to the remote server.

67. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 66, wherein the plurality of instructions further cause the computing device to:

wrap the pre-master key in the security engine of the system-on-a-chip with a server public key, and

store the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

68. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the remote server comprises to generate the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

69. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 68, wherein to generate the session key in the security engine comprises to calculate, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

70. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

Petitioner Samsung Ex-1004, 0557

sign the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

send the signed public Diffie-Hellman key to the remote server;

receive a public Diffie-Hellman server key from the remote server; and

generate, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

71. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein the plurality of instructions further cause the computing device to:

generate, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the remote server;

sign the hash code using the security key stored in the secure memory of the security engine; and

send a client certificate verification message to the remote server, the client certificate verification message including the signed hash code.

Petitioner Samsung Ex-1004, 0558

REMARKS

Applicants thank the Examiner for consideration of the present application. Applicants have carefully reviewed the Office Action dated May 6, 2016 (hereinafter "the Office Action"). Claims 48-71 are pending in this application. In the present Response, Applicants have amended claims 48-50, 52-58, 60-66, and 68-71 without prejudice or disclaimer of subject matter. Applicants respectfully request reconsideration of the present application in light of the above amendments and the remarks presented below.

I. 35 U.S.C. § 103 REJECTIONS

Each of claims 48-52, 56-61, and 64-69 stands rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 7,966,646 of Chou et al. (hereinafter "Chou") in view of U.S. Patent No. 8,364,975 of Kumar et al. (hereinafter "Kumar"). Further, each of claims 53, 54, 62, 63, 70, and 71 stands rejected under 35 U.S.C. § 103 as being unpatentable over Chou in view of Kumar and further in view of U.S. Patent Application No. 2010/0042839 of Ho (hereinafter "Ho"). Additionally, claim 55 stands rejected under Chou in view of Kumar and Ho, and further in view of U.S. Patent Application Publication No. 2004/0158715 of Peyravian et al. (hereinafter "Peyravian"). It is well settled that the analysis required under 35 U.S.C. § 103(a) must be resolved on the basis of the factual inquiries outlined in *Graham v. John Deere, Co.*, 383 U.S. 1, 148 USPQ 459 (1966); *see KSR v. Teleflex*, 127 S.Ct. at 1740. The *Graham* Court stated that as part of any analysis under Section 103,

> the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

148 USPQ at 467. The analysis of obviousness therefore requires an inquiry into the scope and content of the prior art and, more particularly, an inquiry into whether the prior art discloses all of the elements of the claimed invention.

A. Independent Claim 48

In support of the 35 U.S.C. § 103 rejection of independent claim 48, the Office Action asserts that Chou in view of Kumar describes or suggests every feature of independent claim 48.

Petitioner Samsung Ex-1004, 0559

Applicants disagree. However, in order to expedite prosecution of the present application, Applicants have amended independent claim 48 to clarify that the session key encrypted by the security engine is generated based on a cryptographic key exchange with a *remote* server, to encrypt and decrypt messages exchanged with the remote server. More specifically, claim 48 has been amended to recite: a system-on-a-chip that includes a security engine to "perform a cryptographic key exchange with the remote server . . . generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session...." Chou does not disclose this feature. In fact, the Office Action acknowledges, on page 5, that Chou does not disclose a system-on-a-chip that includes a security engine. Kumar also fails to disclose the features amended into claim 48. Rather, Kumar describes a processor 22 establishing communication with a trusted platform module (TPM) 44 *within the same processing system* (i.e., within the same computer). See Kumar at col. 8, lines 49-52. Further, Kumar describes, at col. 8, lines 49-52, *generating* a session key using a third party key that was embedded in the processor at the time of assembly. This is in contrast to *encrypting* a session key generated from a cryptographic key exchange, wherein the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture, in accordance with claim 48.

For at least the reasons discussed above, Applicants respectfully submit that the proposed combination of Chou and Kumar does not render claim 48 obvious and Applicants respectfully request withdrawal of the Section 103 rejection of claim 48.

B. Independent Claim 56

The Office Action also rejected claim 56 under Section 103 as being rendered obvious by Chou and Kumar, using similar rational as set forth in the rejection of claim 48. Although Applicants respectfully disagree, Applicants have amended independent claim 56 in a manner similar to amended independent claim 48, in order to expedite prosecution. As such, all of the arguments presented above with regard to amended independent claim 48 apply with equal force to the rejection of amended claim 56 and are incorporated into this section by reference. Accordingly, Applicants submit that the proposed combination of Chou and Kumar does not

Petitioner Samsung Ex-1004, 0560

render claim 56 obvious and Applicants respectfully request withdrawal of the Section 103 rejection of claim 56.

C. Independent Claim 64

The Office Action also rejected claim 64 under Section 103 as being rendered obvious by Chou and Kumar, using similar rational as set forth in the rejection of claim 48. Although Applicants respectfully disagree, Applicants have amended independent claim 64 in a manner similar to amended independent claim 48, in order to expedite prosecution. As such, all of the arguments presented above with regard to amended independent claim 48 apply with equal force to the rejection of amended claim 64 and are incorporated into this section by reference. Accordingly, Applicants submit that the proposed combination of Chou and Kumar does not render claim 64 obvious and Applicants respectfully request withdrawal of the Section 103 rejection of claim 64.

D. Dependent Claims 49-55, 57-63, and 65-71

Each of claims 49-55 includes independent claim 48 as a base claim; each of claims 57-63 includes independent claim 56 as a base claim; and each of clams 65-71 includes independent claim 64 as a base claim. Ho and Peyravian do not cure the deficiencies of Chou and Kumar with respect to independent claims 48, 56, and 64. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claims 49-55, 57-63, and 65-71. Any arguments specific to claims 49-55, 57-63, and 65-71 are held in abeyance without prejudice or admission to any assertion made in the Office Action in order to expedite prosecution.

II. CONCLUSION

In view of the foregoing, it is submitted that this application is in a condition for allowance. Action to that end is hereby solicited. If there are any questions or comments that would expedite prosecution of this application, the Examiner is invited to call the undersigned at (317) 231-7307.

It is respectfully requested that, if necessary to effect a timely response, this paper be considered as a Petition for an Extension of Time sufficient to effect a timely response. The Commissioner is hereby authorized to charge the fee for such Petition, if needed, and any

Petitioner Samsung Ex-1004, 0561

shortage of fees, and credit any overpayment of fees, to the Account of Barnes & Thornburg, Deposit Account No. 10-0435 with reference to file P41624US/45631-225521.

Respectfully submitted,

/Scott R Powell/

Scott R. Powell
Registration No. 58,378
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-7307

Petitioner Samsung Ex-1004, 0562

Electronic Acknowledgement Receipt

EFS ID:	26190369
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/kim tyree
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	28-JUN-2016
Filing Date:	03-APR-2014
Time Stamp:	08:12:31
Application Type:	U.S. National Stage under 35 USC 371

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	After Final Consideration Program Request	P41624US_AFCP.pdf	226624 b7ab5085746e9f1194d9a65922b3d951898b66cb	no	2

Warnings:

Information:					
2	Response After Final Action	P41624US_RFOA.pdf	60904 29d4a314f1bf163e600cd8c911bee0fae365 52f4	no	12
Warnings:					
Information:					
			Total Files Size (in bytes):	287528	

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.

BARNES & THORNBURG LLP
11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	2495
Examiner:	Le, Thanh T.
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	April 3, 2014
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

June 28, 2016

RESPONSE TO FINAL OFFICE ACTION

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

Sir:

In response to the Office Action dated May 6, 2016, and contemporaneously with a request for consideration under the After Final Consideration Pilot Program 2.0 ("AFCP 2.0"), please consider the following:

Amendments to the Claims, which begin on page **2**; and

Remarks, which begin on page **9**.

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 13/997,412	Filing Date 04/03/2014	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	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	06/28/2016	(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))	* 24	Minus	** 24	= 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
/VIKKI GRAY/

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.

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 08/08/2016

Barnes & Thornburg LLP (Intel)
c/o CPA Global
900 2nd Avenue South, Suite 600
Minneapolis, MN 55402

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
08/08/2016	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Petitioner Samsung Ex-1004, 0567

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/997,412	**Applicant(s)** KHOSRAVI ET AL.	
	Examiner THANH T. LE	**Art Unit** 2495	**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 28 June 2016 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 _____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): _____.
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: amended limitations need further search and considerarion.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☒ Other: PTOL-2323.

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: 48-71.
    Claim(s) withdrawn from consideration: .

/FARID HOMAYOUNMEHR/ Supervisory Patent Examiner, Art Unit 2495	/THANH T LE/ Examiner, Art Unit 2495

Petitioner Samsung Ex-1004, 0568

DO NOT ENTER: /T.L./

08/03/2016

BARNES & THORNBURG LLP
11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	2495
Examiner:	Le, Thanh T.
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	April 3, 2014
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

June 28, 2016

RESPONSE TO FINAL OFFICE ACTION

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

Sir:

In response to the Office Action dated May 6, 2016, and contemporaneously with a request for consideration under the After Final Consideration Pilot Program 2.0 ("AFCP 2.0"), please consider the following:

Amendments to the Claims, which begin on page **2**; and

Remarks, which begin on page **9**.

AFCP 2.0 Decision	Application No.	Applicant(s)
	13/997,412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T. LE	2495

This is in response to the After Final Consideration Pilot request filed 06/28/2016.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.

   ☐ Other:

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☒ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action. See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☐ 5. Other:

   Examiner Note: Please attach an interview summary when necessary as described above.

Petitioner Samsung Ex-1004, 0570

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050213766	A1	2005-09-29	Goss	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	WO00/02358	WO	A1	2000-01-13	Nokia Mobile Phones Limited		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0571

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

	1	First Office Action for Chinese Application No. 201180075550.4, dated June 1, 2016, 5 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Petitioner Samsung Ex-1004, 0572

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2016-08-11
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0573

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 record s.

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.

Petitioner Samsung Ex-1004, 0574

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, 12/22

A1

(11) International Publication Number: **WO 00/02358**

(43) International Publication Date: 13 January 2000 (13.01.00)

(21) International Application Number: PCT/EP99/04720

(22) International Filing Date: 2 July 1999 (02.07.99)

(30) Priority Data:
PA 1998 00867 3 July 1998 (03.07.98) DK

(71) Applicant *(for all designated States except US)*: NOKIA MOBILE PHONES LIMITED [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: IMMONEN, Olli [FI/FI]; Tuohuskuja 16 A 5, FIN–00670 Helsinki (FI).

(74) Agents: HIGGIN, Paul et al.; Nokia House, Summit Avenue, Southwood, Farnborough, Hampshire GU14 0NG (GB).

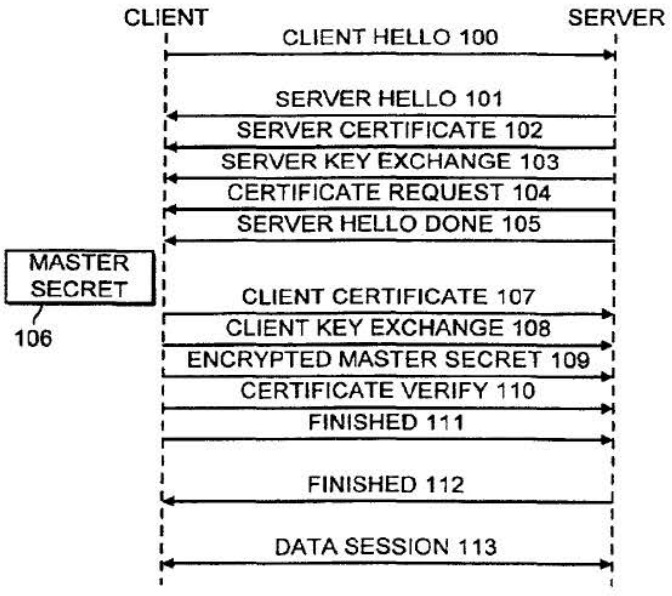
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE SESSION SET UP BASED ON THE WIRELESS APPLICATION PROTOCOL

(57) Abstract

Method, apparatus, memory card, and system for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol. The wireless communication apparatus is provided with contact means for receiving information from a separate unit provided with memory means. The memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus.



Petitioner Samsung Ex-1004, 0575

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Petitioner Samsung Ex-1004, 0576

Secure session set up based on the Wireless Application Protocol.

Technical Field of the Invention

The Wireless Application Protocol (WAP) defines an industry-wide specification for developing applications that operate over wireless communication networks. The wireless market is growing very quickly, and reaching new customers and services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation and fast/flexible service creation a set of protocols has been designed in transport, security, transaction, session and application layers.

Background of the Invention

WAP security functionality includes the Wireless Transport Layer Security (WAPWTLS) and application level security, accessible using Wireless Markup Language Script (WMLScript). For optimum security, some parts of the security functionality need to be performed by a tamper-resistant device, so that an attacker cannot retrieve sensitive data. Such data is especially the permanent private keys used in WTLS handshake with client authentication, and for making application level electronic signatures (such as confirming an application level transaction). In WTLS, also master keys (master secrets) are relatively long living - which could be several days - this is in order to avoid frequent full handshakes which are quite heavy both computationally and due to relatively large data transfer. Master secrets are used as a source of entropy, to calculate MAC keys and message encryption keys which are used to secure a limited number of messages, depending on usage of WTLS.

Petitioner Samsung Ex-1004, 0577

US-A-5,307,411 describe the set up of a secure communication session between two communication units, such as phones or facsimile machines. The secure session is controlled by separate smart cards based verification units associated with a respective one of the communication units. These two verification units exchanges random number, encrypts these numbers by using private keys, returns the encrypted random numbers to their origin. Then the encrypted random number is decrypted based on public keys. If the received numbers corresponds to the transmitted numbers, the parties verifies each other an the secure session may take place. However, this requires that both communication units are provided with a smart card reader, which is not a necessary requirement in a server, like e.g. an Internet server. Thus, this document is quite restricting for the user, since it requires that both parties have a smart card reader, and is less suitable for communication between a wireless communication apparatus and a data communication apparatus. Also, every time a session is going to be established between the two communication apparatuses, an exchange of keys must be done.

Also, US-A-5,371,794, by Sun Microsystems, discloses a way to providing a secure wireless communication link between a mobile nomadic device and a base computing unit. The mobile device sends a host certificate to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms. The base sends random number (RN1) encrypted in the mobile's public key and an identifier for the chosen algorithm back to the mobile. The base saves the RN1 value and adds the CH1 value and the chosen algorithm to the mobile. The mobile verifies under the public key of the base the signature on the message. When the public key is verified, the mobile determines the value of RN1 by decrypting the public key under the private key of the mobile. The mobile then generates RN2 and a session key, and encrypts RN2 under the public key of the base to the base. The base verifies and decrypting the RN2, and determines the session key. Finally, the

Petitioner Samsung Ex-1004, 0578

mobile and the base can enter a data transfer phase using encrypted data which is decrypted using the session key which is RN1 + RN2. The values of RN1 and RN2 are always derived from the last key exchange, which may be from the initial connection setup or from the last key change message, whichever is more recent. This means that each time a data transfer is made, two new numbers is generated based on RN1 and RN2, which will make the data transfer quite slow. Thus, as in US-A-5,307,411, every time a session is going to be established between the two apparatuses, in this case the mobile nomadic device and the base computing unit, an exchange of keys must be done.

Summary of the Invention

The main object of the present invention is to establish a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol.

Another object is to enable the user to re-establish a secure at a later occasion, since establishing a secure connection is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret for a relatively long time. The problem is to store the master key in a secure way. Partly due to that problem, it is common practice to restrict the lifecycle of the master secret and the associated secure session to e.g., 24 hours, after which it is required to perform the heavy key establishment procedure a new.

The main object is achieved in accordance with the present invention by connecting a wireless communication apparatus, e.g. a cellular phone, to a separate unit, e.g. a smart card, a SIM (Subscriber Identity Module) card, etc., which may store sensitive data of a secure connection. This means that the wireless communication apparatus having some kind of contact means, for

Petitioner Samsung Ex-1004, 0579

example wireless (e.g. infra-red, radio frequency, etc.) or physical (i.e. an electrical contact), for receiving information from the separate unit, i.e. the unit is provided with memory means. The memory means comprises information to control an access of the wireless communication apparatus through a wireless communication network, e.g. a cellular phone network, connected to a data communication apparatus, e.g. a server, which supports a Wireless Application Protocol (WAP).

One advantage of using a separate unit, when establishing a secure connection, is that it will be much easier to re-establish a connection to the data communication apparatus. Thus, it is possible to save information, e.g. signatures, secret keys, etc., in the memory means, and may be re-used in another secure connection. In order to avoid fraud, the re-use of a secure connection can be restricted for limited period of time. By saving this information in the memory means the second object will be achieved.

Another advantage is that the user pays less when re-establishing a secure session, in case of the necessary information to re-establishing is saved.

To establish a connection, the wireless communication apparatus connects to the separate unit, accessing the wireless communication network connected to said data communication apparatus. Then the wireless communication apparatus transmits a request to the data communication apparatus. This request comprises information of which pre-defined algorithm(s) the wireless communication apparatus supports. When the data communication apparatus receives this request, it chooses at least one algorithm, associated with a public key and a private key, and transmits a message back to the wireless communication apparatus. This message comprises the public key and information about which algorithm the data communication apparatus has chosen. When the wireless communication apparatus receives the message,

Petitioner Samsung Ex-1004, 0580

comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the wireless communication apparatus will transmit a respond to the data communication apparatus. This respond comprises the calculated signature. When the data communication apparatus receives the respond, comprising the signature, it will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally, the data communication apparatus will be able to establish a secure connection to the wireless communication apparatus.

Further advantages of the vane arrangement according to the present invention will be apparent from the dependent claims.

Brief Description of the Drawing

Fig. 1 schematically illustrates a preferred embodiment of a hand portable phone according to the invention.

Fig. 2 schematically shows the essential parts of a telephone for communication with a cellular or cordless network.

Fig. 3 schematically shows how the secure session is set up between a client /phone and a server according to the invention.

Fig. 4 illustrates the message structure for setting up a secure connection according to the invention.

Detailed Description of Embodiments

Petitioner Samsung Ex-1004, 0581

Fig. 1 shows a preferred embodiment of a phone according to the invention, and it will be seen that the phone, which is generally designated by 1, comprises a user interface having a keypad 2, a display 3, an on/off button 4, a speaker 5, and a microphone 6. The phone 1 according to the preferred embodiment is adapted for communication via a cellular network, but could have been designed for a cordless network as well. The keypad 2 has a first group 7 of keys as alphanumeric keys, by means of which the user can enter a telephone number, write a text message (SMS), write a name (associated with the phone number), etc. Each of the twelve alphanumeric keys 7 is provided with a figure "0-9" or a sign "#" or "*", respectively. In alpha mode each key is associated with a number of letters and special signs used in text editing.

The keypad 2 additionally comprises two soft keys 8, two call handling keys 9, and a navigation key 10.

The two soft keys 8 have a functionality corresponding to what is known from the phones Nokia 2110™, Nokia 8110™ and Nokia 3810™. The functionality of the soft key depends on the state of the phone and the navigation in the menu by using a navigation key. The present functionality of the soft keys 8 is shown in separate fields in the display 3 just above the keys 8.

The two call handling keys 9 according to the preferred embodiment are used for establishing a call or a conference call, terminating a call or rejecting an incoming call.

The navigation key 10 is an up/down key and is placed centrally on the front surface of the phone between the display 3 and the group of alphanumeric keys 7. Hereby the user will be able to control this key with his thumb. This is the best site to place an input key requiring precise motor movements. Many

Petitioner Samsung Ex-1004, 0582

experienced phone users are used to one-hand handling. They place the phone in the hand between the finger tips and the palm of the hand. Hereby the thumb is free for inputting information.

Fig. 2 schematically shows the most important parts of a preferred embodiment of the phone, said parts being essential to the understanding of the invention. The preferred embodiment of the phone of the invention is adapted for use in connection with the GSM network, but, of course, the invention may also be applied in connection with other phone networks, such as cellular networks and various forms of cordless phone systems or in dual band phones accessing sets of these systems/networks. The microphone 6 records the user's speech, and the analog signals formed thereby are A/D converted in an A/D converter (not shown) before the speech is encoded in an audio part 14. The encoded speech signal is transferred to the controller 18, which i.a. supports the GSM terminal software. The controller 18 also forms the interface to the peripheral units of the apparatus, including a RAM memory 17a and a Flash ROM memory 17b, a SIM card 16, the display 3 and the keypad 2 (as well as data, power supply, etc.). The controller 18 communicates with the transmitter/receiver circuit 19. The audio part 14 speech-decodes the signal, which is transferred from the controller 18 to the earpiece 5 via an D/A converter (not shown).

The controller 18 is connected to the user interface. Thus, it is the controller 18 which monitors the activity in the phone and controls the display 3 in response thereto.

Therefore, it is the controller 18 which detects the occurrence of a state change event and changes the state of the phone and thus the display text. A state change event may be caused by the user when he activates the keypad including the navigation key 10, and this type of events is called entry events

Petitioner Samsung Ex-1004, 0583

or user events. However, the network communicating with the phone may also cause a state change event. This type of event and other events beyond the user's control are called non user events. Non user events comprise status change during call set-up, change in battery voltage, change in antenna conditions, message on reception of SMS, etc.

An example of a tamper-resistant device is a smart card (SC). In the phone, it can be the Subscriber Identity Module (SIM) or an external smart card.

The way which a phone and a smart card interact is specified as a command-response protocol. The goal of this protocol is to provide means for a WAP handset to utilize smart cards in performing WTLS and application level security functions. The functionality presented here is based on the requirement that sensitive data, especially keys, can be stored in the card, and all operations where these key are involved can be performed in the card. Different classes of the cards are introduced in order to define how widely the functionality is implemented.

This specification is based on ISO7816 series of standards on smart cards. In particular, it uses the ISO7816-8 standard (draft) [ISO7816-8]. When this functionality is applied to GSM SIM there may be a need to extend also the related GSM specifications [GSM11.11], where applicable.

According to the invention the smart card 16 is used to enhance security of the implementation of the Security Layer and certain functions of the Application Layer. The smart card 16 can be used for several purposes for WTLS. The major purpose of the smart card 16 is to perform cryptographic operations during the handshake, especially when the handshake is used for client authentication. Furthermore the memory of the smart card 16 is used for securing a master secret, a public key and other type of confidential material

Petitioner Samsung Ex-1004, 0584

during long-living WTLS sessions. Finally the memory of the smart card 16 is used for recording the level security of the sessions. According to the invention the WTLS support in a smart card 16 can be described with reference to the following three embodiments.

First embodiment.

According to this embodiment, the smart card 16 is used for storage of permanent, typically certified, private keys and for performing operations using these keys. The operations includes signing operation (e.g., ECDSA or RSA) for client authentication when needed for the selected handshake scheme; key exchange operation using a fixed client key (e.g., ECDH key, in ECDH_ECDSA handshake).

The smart card 16 is not required to perform the calculation of the master secret or operations using the master key. These calculations may advantageously be performed by the controller 18 of the phone. However, the smart card 16 may act as a persistent storage for WTLS secure session (and connection) data, including master secrets. In this case, master secrets would be calculated and used for key derivation in the volatile phone memory (the RAM 17a) but erased from there when not needed at that moment, e.g., when the user exits from secure WAP applications. Not storing session data persistently in phone 1 may improve security, e.g., in the case of a stolen phone 1. It also brings better usability in the case of changing the smart card 16 from one phone 1 to another.

Additionally, for portability, the smart card 16 may store needed certificates. Storage of trusted root certificates (or public keys) has significance also from security point of view: they must not be altered - but they can be exposed without danger.

Petitioner Samsung Ex-1004, 0585

Note that when public key encryption based key exchange (e.g., RSA) is used according to the first embodiment of the invention, there is no advantage in doing public key encryption on the smart card 16 when the pre-master secret would anyway be returned to the phone1, for master secret calculation in the controller 18.

When client authentication is not supported in WTLS, at the minimum, the smart card 16 only acts as a storage for session data. If client authentication is supported, the card would be able to perform a signing operation based on a private key (e.g., ECDSA or RSA) stored in the card, or key agreement calculation (e.g., ECDH) based on a fixed key stored in the card.

Second embodiment.

According to the second embodiment, the smart card 16 is used as a tamper resistant device for all crypto-critical functionality: storage of all persistent keys and operations using these keys. Besides the operations performed according the first embodiment, the smart card 16 now also supports the calculation (ECDH key exchange) or generation (RSA key exchange) of the pre-master secret; calculation and storage of the master secret for each secure session; and derivation and output of key material (for MAC, encryption keys, IV, finished check), based on the master secret

The phone 1 stores MAC and message encryption keys as long as they are currently needed. These keys have a limited lifetime which may be negotiated during the WTLS handshake - in the extreme case they are used for a single message only. The phone 1 has to delete the from its RAM memory 17a when the user exits from the secure WAP applications. These keys can always be derived anew from the master secret if needed.

Petitioner Samsung Ex-1004, 0586

An attacker who obtains a message encryption key can read as many messages as is agreed in the key refresh configuration (in the extreme case, a single message). An attacker who obtains a MAC key can impersonate the compromised party during as many messages as is agreed in the configuration (in the extreme case, a single message).

Third embodiment.

Certain specialized smart cards 16 may act as full-blown security engines for WTLS. This requires that the smart card 16 is equipped with its own processing unit and only uses the phone 1 as an interface to the cellular network during the secure session set up or the handshake procedure. Besides the operations according to the second embodiment, the smart card 16 may store MAC and encryption keys for each secure connection; and perform MAC calculation/verification and encryption/decryption of messages.

Furthermore the smart card 16 may be responsible for the verification of certificates and the verification of digital signatures.

Note that having message encryption in the smart card 16 does not necessarily bring any additional security because in any case the data is as plain text in the phone 1. The same is true for MAC calculation: the phone 1 must be trusted to input and output data in a correct way. The only advantage here would be not having to take encryption keys out of the card 16. However, the keys have a limited lifetime which is negotiated during the WTLS handshake - in the extreme case they are used for single message only. According to the third embodiment, the smart card 16 will contain all algorithms so that they could be controlled by smart card issuers.

Smartcard.

Petitioner Samsung Ex-1004, 0587

The term "smartcard" covers a card-like unit having some memory means in which some secret information identifying the card holder is stored. The memory means may be a magnet strip that may be read by a magnet reader, or it may be provided as discrete memory components as a ROM, EEPROM etc. When the user inserts the smart card in a more or less public apparatus he may become authorized to perform some operations such as banking operations. Presently the user of a GSM phone is identified by a so-called Subscriber Identity Module or a SIM card 16, and the structure of this type of smart card is defined in the GSM specification "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface", GSM 11.11 version 5.5.0, published by European Telecommunications Standards Institute; ETSI. The present type of smartcards will be able to support the first embodiment explained above.

Gemplus has recently launched a smartcard, GemXpresso RAD, based on a 32-bit chip from Texas Instruments using ARM7 RISC core technology. This 32 bit RISC processor has a 32 kbyte of non volatile flash memory and 8 kbyte of ROM. When the mechanical interface of the Gemplus card is adapted to fulfill the GSM specification this type of smartcard will be able to support the second and the third embodiment.

Network.

Fig. 3 schematically shows how the secure session, i.e. a secure connection, between a data communication apparatus and a wireless communication apparatus, e.g. a cellular phone 1. Basically the WAP content and applications are specified in a set of well-known content formats based on the familiar WWW content formats. Content is transported using a set of standard communication protocols based on the WWW communication protocols. A browser in the phone 1 co-ordinates the user interface and is analogous to a standard web browser.

Petitioner Samsung Ex-1004, 0588

The wireless communication apparatus 1 is a client 1 who wants to establish a secure connection to a server 20,30,40, which is the data communication apparatus 20,20,30. The client is provided in an environment, which make it possible to reach a wide variety of different wireless platforms, e.g. world wide web (WWW). The environment provided may be referred to as Wireless Application Environment (WAE). This means that the client 1 may be supported by some kind of browser, e.g. a micro-browser, to access the different services connected to the server. In order to access these services the browser may comprise following functionalities:

· Wireless Markup Language (WML) – a lightweight markup language, similar to HTML, but optimised for use in hand-held mobile terminals;

· WMLScript – a lightweight scripting language, similar to JavaScript™;

· Wireless Telephony Application (WTA, WTAI) – telephony services and programming interfaces; and

· Content Formats – a set of well-defined data formats, including images, phone book records and calendar information.

The server 20 is using a wireless application protocol, and may comprise a gateway 30 and an origin server 40. The gateway 30 is also a server, which may identify and encrypt/decrypt information between the client 1 and the origin server 40. This means that the gateway is provided with encoders and decoders (not shown). Also, the server 20 comprises different algorithms to make the encryption/decryption. The encryption/decryption itself may be performed by well-known methods, e.g. RSA, Diffie-Hellman, etc. The origin server 40 comprises different scripts to support WAP and data to be accessed by the client. This data may be all kind of information, e.g. weather reports, news, information from stock markets, etc.

Petitioner Samsung Ex-1004, 0589

In order to access the server 20, from the client 1, the server has to be connected to a wireless communication network 50, e.g. a cellular phone network. Therefore, in accordance with the present invention, the client is provided with contact means (not shown) for receiving information from a separate unit (not shown) provided with memory means. This separate unit may be a smart card, subscriber identity module (SIM), or the like. The memory means may be a random access memory (RAM), read only memory (ROM), or the like. Further, the memory means comprises information to control the access of the server 20 through the wireless communication network 50.

To establish a secure connection, the client 1 connects to the separate unit, accessing the wireless communication network 50 connected to the server 20. Then the client 1 transmits an encrypted request 60 through the gateway 30. This encrypted request 60 comprises information of which pre-defined algorithm(s) the client 1 supports. When the gateway 30 receives this encrypted request 60, it sends 70 the encrypted request to the origin server 40. The origin server 40 chooses at least one algorithm, associated with a public key and a private key, and transmits a message 80 back to the gateway 30. The gateway encrypts the message and send it 90 to the client 1. This message 90 comprises the public key and information about which algorithm the server 20 has chosen. When the client 1 receives the encrypted message 90, comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the client 1 will transmit an encrypted respond 65 to the gateway 30. This encrypted respond 65 comprises the calculated signature. When the gateway 30 receives the encrypted respond 80, comprising the signature, it will decrypt the respond 75 and send it to the origin server 40. The origin server will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally,

Petitioner Samsung Ex-1004, 0590

the origin server 40 sends a final message 85 to the client through the gateway 30. If the origin server 40 has accepted the clients 1 request 60, the server will be able to establish a secure connection between the origin server 40 and the client 1, else the connection will be terminated.

Setting up a secure connection.

Fig. 4 illustrates the message structure for setting up a secure connection according to the invention.

The cryptographic parameters of the secure session are produced by the WTLS Handshake Protocol, which operates on top of the WTLS Record Layer. When a WTLS client and server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public-key encryption techniques to generate a shared secret.

The WTLS Handshake Protocol is described Wireless Transport Layer Security Specification dated 30. April 1998 and is a part of the Wireless Application Protocol.

The WTLS Handshake Protocol involves the following sequence of steps. When the a WAP session has been set between the phone 1 (the client) and the server 20 (e.g. a bank), and the client (phone 1) wants to establish a secure connection he sends a client hello message 100 as his first message. This message includes a key exchange list that contains the cryptographic key exchange algorithms supported by the client in decreasing order of preference. In addition, each entry defines the certificate or public key the client wishes to use. The server will select one or, if no acceptable choices are presented, return a handshake_failure alert and close the secure connection.

Petitioner Samsung Ex-1004, 0591

In response to the client hello message 100 the server 20 will send a server hello message 101 when it was able to find an acceptable set of algorithms. If it cannot find such a match, it must respond with a handshake_failure alert. The server hello message 101 will identify the session and set up the parameters need for the session.

The server 20 will furthermore transmit a server certificate message 102. The server certificate message 102 will always immediately follow the server hello message 101, and the purpose of this server certificate message 102 identify the cryptation algorithm selected by the server from the key exchange list included in the client hello message 100. The server certificate message 102 will include a so-called certificate carrying a public key for the selected encryption algorithm. The server certificate message 102 includes information about issuer of the certificate, the beginning and the end of the validity period, and parameters relevant or the public key. The server controls the validity period and when the granted validity period is expired the client has to renew the secure connection. The length of the validity period will typically be in the level of a week or more. The maximum number of session will also have to be defined.

A Server Key Exchange Message 103 will be send as a third message immediately after the server certificate message 102. The server key exchange message 103 is optionally and will be sent by the server 20 only when the server certificate message102 does not contain enough data to allow the client 1 to exchange a pre-master secret. This message 103 conveys cryptographic information to allow the client to communicate the pre-master secret: either an RSA public key to encrypt a secret with, or Elliptic Curve Diffie-Hellman parameters with which the client can complete a key exchange (with the result being the pre-master secret). As additional Key

Petitioner Samsung Ex-1004, 0592

Exchange Suites are defined for WTLS which include new key exchange algorithms, the server key exchange message will be sent if and only if the certificate type associated with the key exchange algorithm does not provide enough information for the client to exchange a pre-master secret.

Also a forth message - a Server Certificate message 104 - is optionally. This message 104 requests a certificate from the client, if appropriate for the selected cipher suite. This message will immediately follow the Server Certificate message 102 and Server Key Exchange message 103.

In order to inform the client that the server has ended of the Server Hello session, it transmits a Server Hello Done message 105. After sending this message 105 the server 20 will wait for a client response. This message indicates that the server 20 has send messages to support the key exchange, and that the client 20 can proceed with its phase of the key exchange.
Upon receipt of the server hello done message the client should verify that the server provided a valid certificate if required and check that the server hello parameters are acceptable.

If the server 20 asks for an Client Certificate message 107, the client 1 has to transmit such a after receiving a Server Hello Done message 105. This message is only sent if the server 20 requests a certificate. If no suitable certificate is available, the client must send a certificate message containing no certificates. If client authentication is required by the server for the handshake to continue, it may respond with a fatal handshake_failure alert. Client certificates are sent using the Certificate structure defined previously for server certificates.

Now the phone 1 or the client starts to calculate a 20 byte random number to be used as a Master Secret 106 for the secure sessions. The master secret

Petitioner Samsung Ex-1004, 0593

106 is used to derive key material needed for Message Authentication Code (MAC) keys and data encryption keys. MAC and data encryption provide data integrity and privacy between communicating parties. A public key based key establishment is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret 106 for a relatively long time.

The processor or the controller 18 of the phone 1 calculates the master secret. A smart card, e.g. the SIM card16, which can be regarded as a tamper resistant device, is used for storage of the sensitive data of the secure session, and performing operations using that sensitive data, so that this data never leaves the card. In practice the secure information will be transferred from the SIM card 16 to the working RAM 17a of the processor 18 but these information will be overwritten when no session is ongoing or when the phone 1 is switched off.

According to the first embodiment of the invention the controller 18 performs the operations needed for the key establishment, e.g., Diffie-Hellman calculation or RSA encryption and complementary calculations. Then the controller 18 persistently stores the resulting secret key (master secret 106) in the SIM card 16. Then the controller 18 performs the key derivation based on the master secret 106 and additional data (e.g., seed), producing key material for MAC calculation and encryption. The key derivation function is security protocol specific. It is typically based on some secure hash function, e.g., SHA-1.

Preferably the SIM card 16 is provided as a smart card having its own processor, whereby both the operations needed for performing the key establishment and the key derivation based on the master secret may be performed inside the smart card. Then the master secret, and data used to

Petitioner Samsung Ex-1004, 0594

calculate it, would never have to leave smart card. So, the secure session associated with the master secret can be used during a long period

A Client Key Exchange Message 108 will immediately follow the client certificate message 107, if it is sent. Otherwise it will be the first message sent by the client 1 after it receives the Server Hello Done message 105. With this message 108, a pre-master secret is set, either through direct transmission of the RSA-encrypted secret, or by the transmission of EC Diffie-Hellman public key which will allow each side to agree upon the same pre-master secret.

Then the Master Secret 106 is encrypted by using the public key from the server's certificate and the agreed RSA algorithm. The result is send to the server 20 in an encrypted master secret message 109.

A Certificate Verify message 110 is used to provide explicit verification of a client certificate. This message is only sent by the client following a client certificate Message 107 that has signing capability (i.e., RSA certificates).

Both ends has to send finished messages 111 and 112 at the end of the handshake to verify that the key exchange and authentication processes were successful.

The finished messages 111 and 112 is the first messages protected with the just-negotiated algorithms, keys, and secrets. Recipients of finished messages must verify that the contents are correct. Once a side has sent its Finished message and received and validated the Finished message from its peer, it may begin to send and receive application data 113 over the secure connection. It is a critical or fatal error if a finished message is not preceded by a change cipher spec message at the appropriate point in the handshake.

Petitioner Samsung Ex-1004, 0595

The value handshake_messages includes all handshake messages starting at client hello up to, but not including, this finished message. The handshake_messages for the finished message sent by the client will be different from that for the finished message sent by the server, because the one which is sent second will include the prior one.

As long as a secure connection is valid application data session 113 may be initiated just by using Client Hello messages 100 and Server Hello messages 101.

Acronyms.

APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certification Authority
CBC	Cipher Block Chaining
DF	Dedicated File
DH	Diffie-Hellman
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
GSM	Global System for Mobile Communication
IV	Initialization Vector
MAC	Message Authentication Code
ME	Management Entity
OSI	Open System Interconnection
PDU	Protocol Data Unit
PRF	Pseudo-Random Function
SAP	Service Access Point

Petitioner Samsung Ex-1004, 0596

SDU	Service Data Unit
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAP	Wireless Application Protocol
WML	Wireless Markup Language
WMLScript	Wireless Markup LanguageScript
WDP	Wireless Datagram Protocol
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol

The list above includes the acronyms used in the present text. Detailed discussion and explanation of the acronyms may be found in the technical specifications defining the Wireless Application Protocol on the Internet homepage for WAPFORUM, http://www.wapforum.org/.

Petitioner Samsung Ex-1004, 0597

CLAIMS

1. Method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, said memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising the following steps:
   - connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication apparatus
   - the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
   - upon reception of said request, the data communication apparatus choose at least one algorithm, associated with a public key and a private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen,
   - upon reception of the message, comprising the public key, the wireless communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a respond to the data communication apparatus, said respond comprising the calculated signature,

Petitioner Samsung Ex-1004, 0598

- upon reception of the respond comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and
- saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion.

2. A method according to claim 1, and comprising a step of saving said master secret under a pre-defined time.

3. A method according to claim 1 or 2, and comprising a step of re-establishing the connection by
   - transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and
   - upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.

4. A method according to claim 1, 2, or 3, and comprising a step of providing said memory means in a smart card.

5. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

Petitioner Samsung Ex-1004, 0599

- communication means for establishing a connection to a wireless communication network connected to said data communication apparatus,
- contact means for receiving information from a separate unit provided with memory means, said memory means is provided with information to control the access of the data communication apparatus through the wireless communication network,
- reading means for reading information received from the data communication apparatus and the information provided on said memory means,
- random generating means, for generating a master secret code,
- pre-defined algorithm(s), to generate a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication apparatus, and
- said reading means comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

6. A wireless communication apparatus according to claim 5, having its memory means exchangeable.

7. An apparatus according to claim 5 or 6, said memory means is a smart card.

8. An apparatus according to claim 5, 6, or 7, said memory means is a subscriber identity module.

Petitioner Samsung Ex-1004, 0600

9. Memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to said wireless communication apparatus having contact means for receiving information from the memory card, and said memory card is provided with information to control the access of the data communication apparatus through a wireless communication network.

10. A memory card according to claim 9, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection.

11. A memory card according to claim 9 or 10, comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

12. A memory card according to claim 9, 10, or 11, is provided on a smart card.

13. System for establishing a secure connection when using a wireless application protocol, comprising:

- a data communication apparatus based on the wireless application protocol,
- a wireless communication network, connected to said data communication apparatus,
- a wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, and

Petitioner Samsung Ex-1004, 0601

- the separate unit provided with the memory means, said memory means, comprising information to control the access of the wireless communication apparatus through the wireless communication network, wherein
- the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
- upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will choose,
- upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a respond to the data communication apparatus, said respond comprising the calculated signature,
- upon reception of the respond comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key, and, thus establish a secure connection to the wireless communication apparatus, and
- said memory means and the data communication apparatus are arranged to save said master secret code, in order to re-establish the connection at a later occasion.

Petitioner Samsung Ex-1004, 0602

14. A system according to claim 13, said master secret is arranged to be saved under a pre-defined time.

15. A system according to claim 13, or 14, said memory means is a smart card.

Petitioner Samsung Ex-1004, 0603

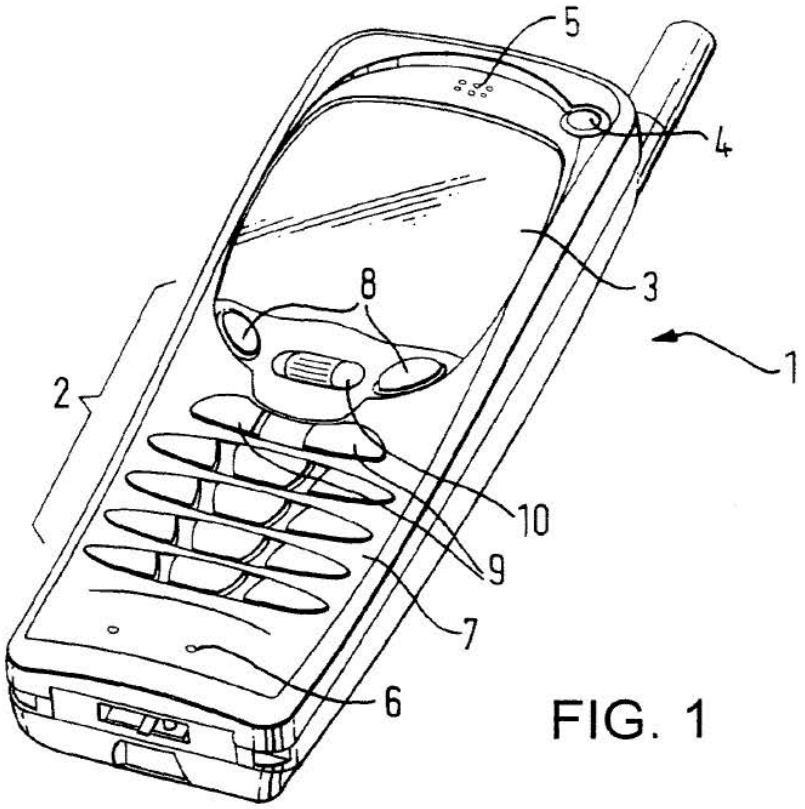


FIG. 1

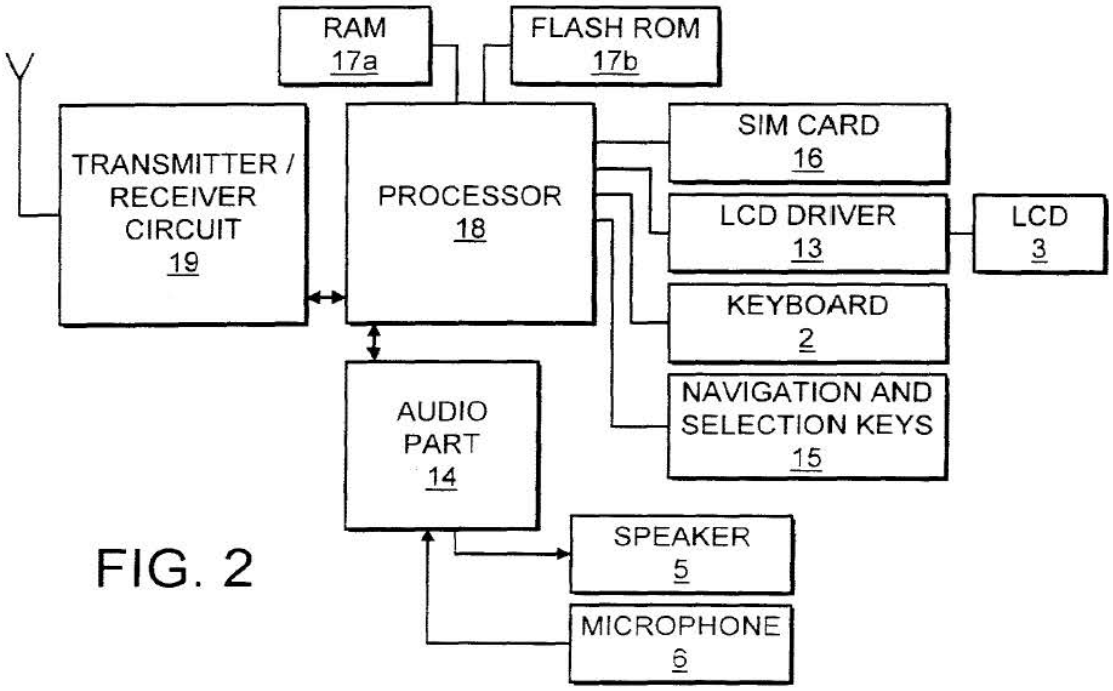


FIG. 2

Petitioner Samsung Ex-1004, 0604

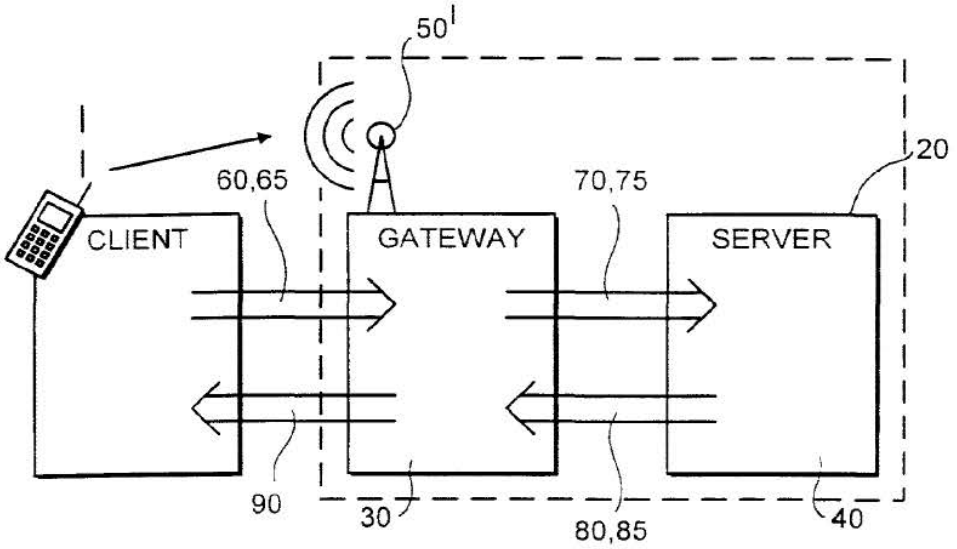


FIG. 3

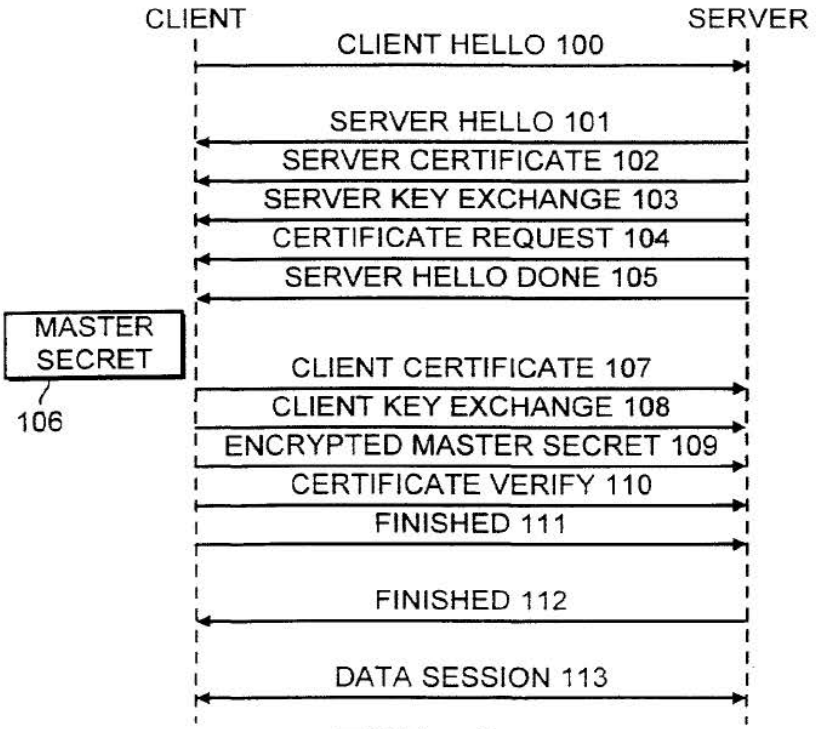


FIG. 4

Petitioner Samsung Ex-1004, 0605

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/EP 99/04720

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 195 42 732 A (SCHEINERT STEFAN) 22 May 1997 (1997-05-22) abstract column 1, line 21 -column 3, line 1 column 3, line 45-57	1-15
A	EP 0 538 216 A (TELEVERKET) 21 April 1993 (1993-04-21) cited in the application abstract column 1, line 29-40 column 2, line 5-30 column 3, line 28-52 column 5, line 8-27	1-15

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 November 1999	03/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lázaro Lõpez, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

Petitioner Samsung Ex-1004, 0606

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/EP 99/04720

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SIEMENS: "Banking by Mobile Phone" TELCOMREPORT, 30 June 1998 (1998-06-30), XP002123311 Available from Internet <http://www.siemens.de/telcom/articles/e0198/198habak.html> 30 June 1998 the whole document	1-15

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Petitioner Samsung Ex-1004, 0607

INTERNATIONAL SEARCH REPORT

Information on patent family members

In ational Application No
PCT/EP 99/04720

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19542732 A	22-05-1997	NONE	
EP 0538216 A	21-04-1993	SE 470001 B	18-10-1993
		DE 69218335 D	24-04-1997
		DE 69218335 T	09-10-1997
		ES 2099243 T	16-05-1997
		JP 6125342 A	06-05-1994
		SE 9102641 A	13-03-1993
		US 5307411 A	26-04-1994

Petitioner Samsung Ex-1004, 0608

US 20050213766A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2005/0213766 A1

Goss (43) Pub. Date: Sep. 29, 2005

(54) HYBRID CRYPTOGRAPHIC ACCELERATOR AND METHOD OF OPERATION THEREOF

(75) Inventor: Steven C. Goss, Rockwall, TX (US)

Correspondence Address:
TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

(73) Assignee: Texas Instruments Incorporated, Dallas, TX

(21) Appl. No.: 10/806,963

(22) Filed: Mar. 23, 2004

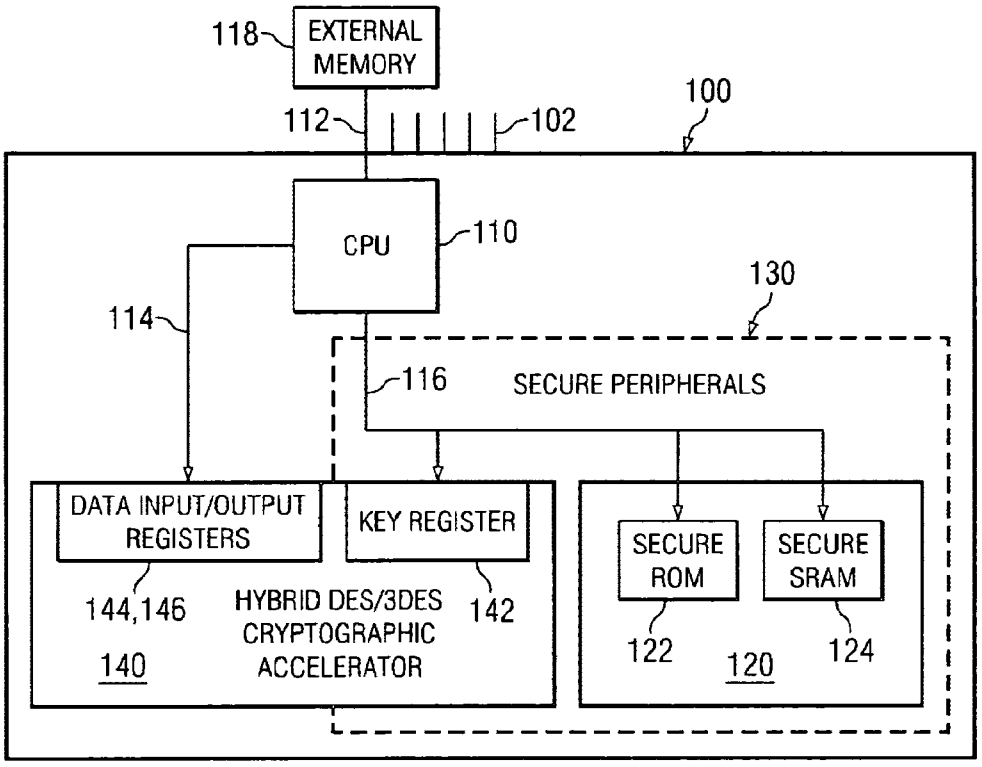
Publication Classification

(51) Int. Cl.[7] H04K 1/00

(52) U.S. Cl. 380/277

(57) ABSTRACT

For use in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, a cryptographic accelerator, a method of performing cryptography therewith and an SoC incorporating the cryptographic accelerator or the method. In one embodiment, the cryptographic accelerator includes: (1) a key register located within the SEE and coupled to the secure memory to receive a cryptographic key therefrom and (2) data input and output registers located outside of the SEE and coupled to the key register to allow the cryptographic key to be applied to input data arriving via the data input register to yield output data via the data output register.



Petitioner Samsung Ex-1004, 0609

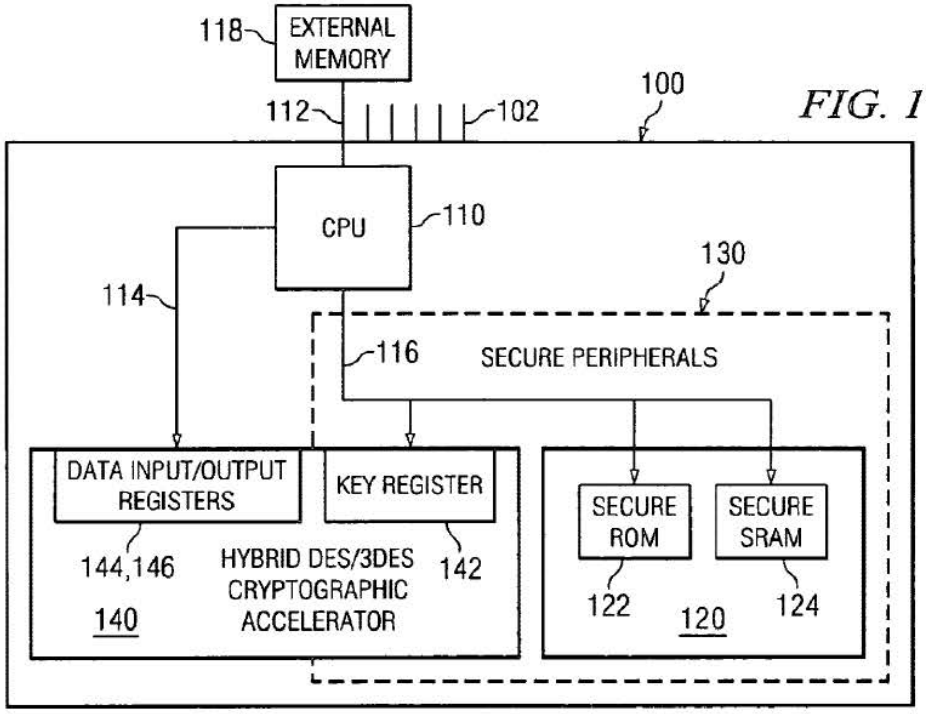


FIG. 1

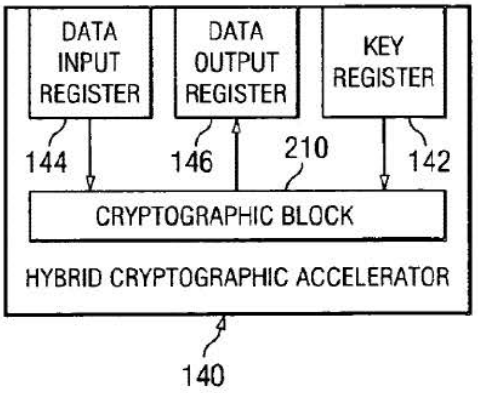


FIG. 2

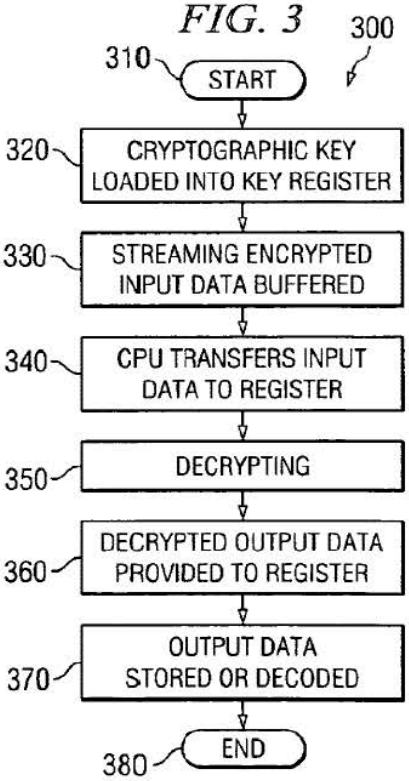


FIG. 3

Petitioner Samsung Ex-1004, 0610

HYBRID CRYPTOGRAPHIC ACCELERATOR AND METHOD OF OPERATION THEREOF

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention is directed, in general, to cryptographic systems and, more specifically, to a hybrid cryptographic accelerator and method of encryption and decryption using a hybrid cryptographic operation.

BACKGROUND OF THE INVENTION

[0002] Decades ago, cryptography and cryptanalysis were relegated to the backrooms of covert organization such as the United States' Central Intelligence Agency and the United Kingdom's MI-6. Nowadays, however, electronic computing and communication have become so commonplace that everyone it seems is concerned about the sanctity of their computers and the privacy of their data and communications. The ever-increasing popularity of wireless communication has only heightened that concern. As a result, engineers with cryptographic skills are in great demand, and the latest computing and communication systems are coming to market with cryptographic capability and data security as a cornerstone of their design. Wireless communication devices have certainly obeyed this trend.

[0003] To this end, a concept called a Secure Execution Environment, or "SEE," has begun to find its way into computing and communications systems. An SEE is designed to perform according to the following objectives: (1) programs are authenticated and therefore free of unexpected code before being admitted to run within the SEE, (2) programs and data within the SEE are free from unwanted interference from outside the SEE and (3) programs and data within the SEE cannot be read from outside the SEE. An elaborate authentication process, often involving permissions and digital signatures, is employed to meet all three objectives. Further, components within the SEE are isolated from user-accessible memory, buses or external pins to meet the second and third objectives. For this reason, SEEs are often provided with their own isolated, secure memory and buses. In fact, SEEs are advantageously implemented in Systems-on-a-Chip, or SoCs, allowing user-accessible external pins to be kept to a minimum.

[0004] SoC designers wanting to incorporate cryptographic capability into their systems have found SEEs to be a valuable way to ensure that cryptographic keys and processes remain secret. Unfortunately, while cryptography can certainly be carried out securely within an SEE, the data to be provided as input to the cryptographic process must pass securely into the SEE before it is encrypted or decrypted, and then it must pass out of the SEE. From an architectural perspective, the central processing unit is heavily involved in the movement of the data into and out of the SEE, and resource-consuming authentication must be done to ensure that false data are not allowed into the SEE. The result is that cryptography occurring within an SEE comes at a great cost in terms of processing overhead and resulting throughput. If a particular application calls for the encryption or decryption of time-sensitive streaming data or large files (as might well be encountered in a wireless environment), a diminished throughput would be particularly undesirable or even unacceptable.

[0005] In an effort to address the overall problem of encryption and decryption speed, hardware cryptographic "accelerators" have been introduced. A cryptographic accelerator uses dedicated cryptographic hardware to perform the same cryptographic functions that a central processing unit would otherwise perform with software. Not only can encryption and decryption be performed faster in hardware than in software, but the computational burden of the central processing unit can also be dramatically reduced, allowing it to perform other important tasks. A cryptographic accelerator may therefore be thought of as a "cryptographic co-central processing unit." Unfortunately, even with the availability of a cryptographic accelerator, SoC designers are faced with having to choose between placing the cryptographic accelerator within the SEE and continuing to suffer performance penalties by virtue of the required secure data movement, or placing the accelerator outside of the SEE and compromising the secrecy of the cryptographic key or process.

[0006] Accordingly, what is needed in the art is a way to achieve a higher encryption or decryption throughput in an SoC than uses a cryptographic accelerator without compromising key or process security.

SUMMARY OF THE INVENTION

[0007] To address the above-discussed deficiencies of the prior art, in one aspect the present invention provides, for use in an SoC having an SEE containing secure memory, a cryptographic accelerator. In one embodiment, the cryptographic accelerator includes (1) a key register located within the SEE and coupled to the secure memory to receive a cryptographic key therefrom and (2) data input and output registers located outside of the SEE and coupled to the key register to allow the cryptographic key to be applied to input data arriving via the data input register to yield output data via the data output register.

[0008] In another aspect, the present invention provides a method of performing cryptography in an SoC having an SEE containing secure memory. In one embodiment, the method includes: (1) loading a key register located within the SEE with a cryptographic key from the secure memory, the key register forming a part of a cryptographic accelerator and (2) applying the cryptographic key to input data arriving via a data input register to yield output data via a data output register, the data input and output registers located outside of the SEE.

[0009] In another aspect, the present invention provides an SoC. In one embodiment, the SoC includes: (1) a central processing unit (CPU), (2) a secure memory coupled to the CPU and having (2a) secure read-only memory (ROM) and (2b) secure static random-access memory (SRAM), the CPU and secure memory configured to provide an SEE and (3) a cryptographic accelerator, having: (3a) a key register located within the SEE and coupled to the secure memory to receive a cryptographic key therefrom and (3b) data input and output registers located outside of the SEE and coupled to the key register to allow the cryptographic key to be applied to input data arriving via the data input register to yield output data via the data output register.

[0010] The foregoing has outlined preferred and alternative features of the present invention so that those skilled in the art may better understand the detailed description of the invention that follows. Additional features of the invention will be described hereinafter that form the subject of the

Petitioner Samsung Ex-1004, 0611

claims of the invention. Those skilled in the art should appreciate that they can readily use the disclosed conception and specific embodiment as a basis for designing or modifying other structures for carrying out the same purposes of the present invention. Those skilled in the art should also realize that such equivalent constructions do not depart from the spirit and scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

[0012] **FIG. 1** illustrates a block diagram of one embodiment of an SoC incorporating a hybrid cryptographic accelerator constructed according to the principles of the present invention;

[0013] **FIG. 2** illustrates a block diagram of one embodiment of a hybrid cryptographic accelerator constructed according to the principles of the present invention; and

[0014] **FIG. 3** illustrates a flow diagram of one embodiment of a method of performing cryptography in an SoC having an SEE containing secure memory carried out according to the principles of the present invention.

DETAILED DESCRIPTION

[0015] Referring initially to **FIG. 1**, illustrated is a block diagram of one embodiment of a System-on-a-Chip (SoC), generally designated **100**, incorporating a hybrid cryptographic accelerator constructed according to the principles of the present invention.

[0016] SoCs in general are familiar to those skilled in the pertinent art and thus will not be described in detail greater than necessary to convey the inventive concepts introduced herein. The SoC **100** includes a central processing unit (CPU) **110**. The CPU **110** is coupled via buses (some of which are shown and designated **112**, **114**, **116**) to various peripheral components. Among those peripheral components is a secure memory space **120** composed in the specific embodiment of **FIG. 1** of a secure read-only memory (ROM) **122** and secure static random-access memory (SRAM) **124**. The CPU **110** has access to external memory **118** and other components (not shown) via the bus **112**. Because it goes outside the SoC **100**, the bus **112** requires various external pins (only one of which is designated **102**) of the SoC **100**. Thus, the CPU **110** and peripheral components can receive and transmit programs, data and control signals from and to the external memory **116** and other external system components in a manner that is well known to those skilled in the pertinent art.

[0017] The SoC **100** is illustrated as having the capability to create a secure execution environment (SEE) **130**. In **FIG. 1**, the SEE **130** is represented as a broken line encompassing the secure ROM **122** and secure SRAM **124**. Although the SEE **130** is an architectural abstraction, those skilled in the pertinent art understand that system components within the SEE **130** (e.g., the secure ROM **122** and the secure SRAM **124**) are secured as against unwanted infiltration and interference as described above in the Background of the Invention section. As a practical matter, the SEE **130** is created by physically and/or logically isolating components within the SEE **130** from those outside of the SEE **130** and the various external pins (e.g., the pin **102**) and by equipping the CPU **110** with a secure mode or state of operation in which the CPU **110** isolates itself from external components and renders its registers user-inaccessible for either read or write purposes.

[0018] **FIG. 1** also illustrates a schematic representation of a hybrid cryptographic accelerator **140** constructed according to the principles of the present invention. The term "hybrid" is appropriately used because, as **FIG. 1** illustrates, the cryptographic accelerator **140** straddles both the SEE **130** and the portion of the SoC **100** that is outside of the SEE **130**. More particularly, a key register **142** of the hybrid cryptographic accelerator **140** lies within the SEE **130** and is coupled to the secure ROM **122** and the secure SRAM **124** by a secure bus **126**. In contrast, data input and output registers **144**, **146** of the hybrid cryptographic accelerator **140** lie outside of the SEE **130** and are coupled to the CPU **110** by a bus **112** that is not secure and therefore is wholly separate from the secure bus **126**. Thus, the hybrid cryptographic accelerator **140** operates partially within and partially without the SEE **130**. As will be described below, this arrangement yields a particularly advantageous operation that accommodate both cryptographic key security and high data throughput.

[0019] Turning now to **FIG. 2**, illustrated is a more detailed block diagram of one embodiment of the cryptographic accelerator **140** constructed according to the principles of the present invention. The cryptographic accelerator **140** includes the key register **142** first illustrated in **FIG. 1**. The key register **142** is coupled to the secure memory as detailed above so as to receive a cryptographic key in a secure manner. The key register **142** may advantageously be a write-only register and may be writeable only when the CPU (**110** of **FIG. 1**) is in a secure state. The cryptographic key is advantageously never transmitted in the clear outside the SEE **130**.

[0020] The cryptographic accelerator **140** further includes the data input and output registers **144**, **146** first illustrated in **FIG. 1**. The data input register(s) **144** receives input data to be encrypted or decrypted, and the data output register(s) provide output data that has been encrypted or decrypted.

[0021] Also illustrated is a cryptographic block **210**. Those skilled in the pertinent art are familiar with the structure and function of cryptographic blocks in general. They understand that cryptographic blocks employ a cryptographic key and a cryptographic algorithm to perform a cryptographic operation on input data to yield output data. The cryptographic operation may be one of encryption or decryption. The cryptographic block **210** is therefore coupled to the key register **142** and the data input and output registers **144**, **146** to receive the key and input data and produce the output data based thereon. In the embodiment illustrated in **FIG. 2**, the cryptographic block **210** is a Data Encryption Standard (DES) block or a triple Data Encryption Standard (3DES) block. Those skilled in the pertinent art will understand, however, that any conventional or later-developed cryptographic block or combination of multiple cryptographic blocks falls within the broad scope of the present invention and is employable as the cryptographic block **210**.

[0022] Important to an understanding of the present invention is that, while the cryptographic register **142** and the

Petitioner Samsung Ex-1004, 0612

cryptographic key the register contains remain within the SEE (**130** of **FIG. 1**), the data input and output registers **144**, **146** remain outside of the SEE. Since, in the illustrated embodiment, the CPU mediates movement of the input data and the output data between the data input and output registers and the external memory, bandwidth-consuming security operations that would otherwise be required to move the input data to within the SEE are wholly avoided such that the speed at which the SoC (**100** of **FIG. 1**) can encrypt or decrypt can be significantly enhanced. In fact, direct memory access (DMA) can be advantageously employed further to reduce any CPU involvement in data transfer. All the while, the key register **142** remains unreachable from the data input and output registers **144**, **146**, thereby preserving the secrecy of the cryptographic key.

[**0023**] Turning now to **FIG. 3**, illustrated is a flow diagram of one embodiment of a method, generally designated **300**, of performing cryptography in an SoC having an SEE containing secure memory carried out according to the principles of the present invention.

[**0024**] The method **300** begins in a start step **310**, wherein it is desired, for example, to decrypt streaming input data received by a mobile telecommunications device. In a step **320**, the CPU of the SoC enters a secure state and calls for an appropriate cryptographic key to be conveyed from a secure SRAM to a secure key register of a hybrid cryptographic accelerator via a secure bus. Afterwards, the CPU is free to exit the secure state, though it need not. Then, in a step **330**, the mobile telecommunications device buffers the streaming encrypted input data in a memory external to the SoC.

[**0025**] Next, in a step **340**, the CPU of the SoC mediates a transfer of the streaming encrypted input data from the external memory to one or more insecure data input registers of a hybrid cryptographic accelerator without. At no point does the streaming encrypted input data enter the SEE.

[**0026**] Then, in a step **350**, a cryptographic block within the hybrid cryptographic accelerator operates on the streaming encrypted input data to yield streaming decrypted output data. In a step **360**, the streaming decrypted output data are provided to one or more insecure data output registers of the hybrid cryptographic accelerator. Next, in a step **370**, the streaming decrypted output data, which may now take the form of a file or coded voice or video, is stored or decoded for hearing or watching, as the case may be. The method **300** ends in an end step **380**.

[**0027**] While the method disclosed herein has been described and shown with reference to particular steps performed in a particular order, it will be understood that these steps may be combined, subdivided, or reordered to form an equivalent method (including, of course, various other decrypting or encrypting methods) without departing from the teachings of the present invention. Accordingly, unless specifically indicated herein, the order and the grouping of the steps are not limitations of the present invention.

[**0028**] Although the present invention has been described in detail, those skilled in the art should understand that they can make various changes, substitutions and alterations herein without departing from the spirit and scope of the invention in its broadest form.

What is claimed is:

1. For use in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, a cryptographic accelerator, comprising:

a key register located within said SEE and coupled to said secure memory to receive a cryptographic key therefrom; and

data input and output registers located outside of said SEE and coupled to said key register to allow said cryptographic key to be applied to input data arriving via said data input register to yield output data via said data output register.

2. The cryptographic accelerator as recited in claim 1 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

3. The cryptographic accelerator as recited in claim 1 wherein a cryptographic block coupled to said key register and said data input and output registers is selected from the group consisting of:

a Data Encryption Standard (DES) block, and a triple Data Encryption Standard (3DES) block.

4. The cryptographic accelerator as recited in claim 1 wherein said key register is a write-only register and writeable only when a central processing unit of said SoC is in a secure state.

5. The cryptographic accelerator as recited in claim 1 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

6. The cryptographic accelerator as recited in claim 1 wherein a central processing unit mediates movement of said input data and said output data between said input and output registers and memory external to said SoC.

7. The cryptographic accelerator as recited in claim 1 wherein said secure memory comprises secure read-only memory and secure static random-access memory.

8. A method of performing cryptography in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, comprising:

loading a key register located within said SEE with a cryptographic key from said secure memory, said key register forming a part of a cryptographic accelerator; and

applying said cryptographic key to input data arriving via a data input register to yield output data via a data output register, said data input and output registers located outside of said SEE.

9. The method as recited in claim 8 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

10. The method as recited in claim 8 wherein said applying is carried out in a cryptographic block coupled to said key register and said data input and output registers, said cryptographic block selected from the group consisting of:

a Data Encryption Standard (DES) block, and

a triple Data Encryption Standard (3DES) block.

11. The method as recited in claim 8 wherein said key register is a write-only register and writeable only when a central processing unit of said SoC is in a secure state.

Petitioner Samsung Ex-1004, 0613

12. The method as recited in claim 8 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

13. The method as recited in claim 8 further comprising mediating movement of said input data and said output data between said input and output registers and memory external to said SoC with a central processing unit.

14. The method as recited in claim 8 wherein said secure memory comprises secure read-only memory and secure static random-access memory.

15. A system-on-a-chip (SoC), comprising:

a central processing unit;

a secure memory coupled to said central processing unit (CPU) and including:

secure read-only memory (ROM), and

secure static random-access memory (SRAM), said CPU and said secure memory configured to provide a secure execution environment (SEE); and

a cryptographic accelerator, including:

a key register located within said SEE and coupled to said secure memory to receive a cryptographic key therefrom, and

data input and output registers located outside of said SEE and coupled to said key register to allow said cryptographic key to be applied to input data arriving via said data input register to yield output data via said data output register.

16. The SoC as recited in claim 15 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

17. The SoC as recited in claim 15 wherein a cryptographic block coupled to said key register and said data input and output registers is selected from the group consisting of:

a Data Encryption Standard (DES) block, and

a triple Data Encryption Standard (3DES) block.

18. The SoC as recited in claim 15 wherein said key register is a write-only register and writeable only when said CPU is in a secure state.

19. The SoC as recited in claim 15 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

20. The SoC as recited in claim 15 wherein said CPU mediates movement of said input data and said output data between said input and output registers and memory external to said SoC.

* * * * *

Petitioner Samsung Ex-1004, 0614

Electronic Patent Application Fee Transmittal

Application Number:	13997412
Filing Date:	03-Apr-2014
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Filer:	Glen Madison Kellett
Attorney Docket Number:	P41624US/45631-225521

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

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**

Electronic Acknowledgement Receipt

EFS ID:	26619194
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Glen Madison Kellett/Stacy Tebo
Filer Authorized By:	Glen Madison Kellett
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	11-AUG-2016
Filing Date:	03-APR-2014
Time Stamp:	17:23:20
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	4086
Deposit Account	504238
Authorized User	KELLETT, GLEN

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 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)	
Charge any Additional Fees required under 37 CFR 1.492(a) (basic national fee only)	

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)	P41624US_IDS.pdf	1035119 fafefe7640666f7d0c82a66f6e75466b22fda35b	no	4
Warnings:					
Information:					
2	Foreign Reference	WO0002358.pdf	1731231 050beadd192f81a8a5176ac3990d1d0965fdbb12	no	40
Warnings:					
Information:					
3	Non Patent Literature	P41624CN_OA.pdf	260594 873a8ad7d73777bc5ae4a758fbc2df497bf11d7a	no	5
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	31122 62a6e54fb4f98bc63e3dbe0e66a89dc02c70b488	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3058066		

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: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
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.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13997412	Filing Date	2014-04-03	Docket Number (if applicable)	P41624US/45631-225521	Art Unit	2495
First Named Inventor	Hormuzd M. Khosravi			Examiner Name	LE, THANH T.		

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, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

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).

☒ 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.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other Response to Final Office Action filed June 28, 2016

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ 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)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504238

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

Petitioner Samsung Ex-1004, 0620

PTO/SB/30EFS (07-14)
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.

Signature of Registered U.S. Patent Practitioner			
Signature	/Scott R. Powell/	Date (YYYY-MM-DD)	2016-08-12
Name	Scott R. Powell	Registration Number	58378

This collection of information is required by 37 CFR 1.114. 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.

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 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.

Petitioner Samsung Ex-1004, 0622

Electronic Patent Application Fee Transmittal

Application Number:	13997412
Filing Date:	03-Apr-2014
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Filer:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

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 - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
Request for Continued Examination	1801	1	1200	1200
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt	
EFS ID:	26629614
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/Stacy Tebo
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	12-AUG-2016
Filing Date:	03-APR-2014
Time Stamp:	15:48:23
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1400
RAM confirmation Number	2185
Deposit Account	504238
Authorized User	POWELL, SCOTT R.
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 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

Charge any Additional Fees required under 37 CFR 1.492(a) (basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	P41624US_RCE.pdf	1349922 7ede5d1d4bb867086acf4cde28c0dd4a2177fd10	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32980 47867bd9683d6a0de7808dca6ddd0455d184283a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1382902		

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/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 13/997,412	Filing Date 04/03/2014	☐ 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 08/12/2016

	(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))	* 24	Minus	** 24	= 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
JEFFERY L. OLSEN

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040158715	A1	2004-08-12	Peyravian et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	201008309	TW	A	2010-02-16	Silver Spring Networks Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0628

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

	1	Office Action, Search Report, and English Translation of R.O.C. Patent Application No. 101147511, dated October 24, 2016, 11 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2017-01-19
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0630

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 record s.

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.

Petitioner Samsung Ex-1004, 0631

Abstract of D3: TW 201008309

Methods and systems a provided for security in a wireless utility network. The methods and systems use different levels of trust to securely enroll new nodes into a network through other nodes acting as proxies. A node's security state with respect to another node in the network is categorized into one of several trust levels. A node responds to certain requests, actions or messages depending based on its trust level with the other entity. Initially, a node is not trusted. A first trust level is established based on a digital certificate that is stored in a node when the node is manufactured. A second trust level is established based on a second digital certificate obtained from a certifying authority while a node is in the first trust level. A node with a verified second certificate can be fully enrolled in the network and participate as a network node with minimal or no constraints.

Electronic Acknowledgement Receipt

EFS ID:	28109380
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Glen Madison Kellett/Stacy Tebo
Filer Authorized By:	Glen Madison Kellett
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	19-JAN-2017
Filing Date:	03-APR-2014
Time Stamp:	16:53:12
Application Type:	U.S. National Stage under 35 USC 371

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	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	1035118 e88892b52badc09546596ef55d67c47cd0b433bc	no	4

Warnings:

Information:					
2	Foreign Reference	TW201008309ABST.pdf	5685 4c810257d2aee8b0338a14e594b585a001d632db	no	1
Warnings:					
Information:					
3	Non Patent Literature	TW_OA.pdf	5480086 9f6b5d1e11e90354ea727f99b46b4bbada9bec94	no	11
Warnings:					
Information:					
			Total Files Size (in bytes):	6520889	

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 01/23/2017

Barnes & Thornburg LLP (Intel)
11 S. Meridian Street
Indianapolis, IN 46204

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
01/23/2017	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Petitioner Samsung Ex-1004, 0635

Office Action Summary	Application No. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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 *6/28/2016*.

☐ 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) *48-71* 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) *48-71* 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 *08/11/2016*.

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

4) ☐ Other: _____.

Petitioner Samsung Ex-1004, 0636

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/12/2016 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 08/11/2016 has been considered by the Examiner.

Status of Claims

4. This Office Action is issued in response to the Amendment filed on 06/28/2016.

Claims 1-47 are cancelled.

Claims 48-71 are pending in this Office Action.

Claims 48-50, 52-58, 60-66, 68-71 are amended.

Response to Arguments

5. Applicants' arguments regarding Kumar is not persuasive because Kumar is used to remedy the deficiencies of Chou which are security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip and the security key is used to encrypt session key. Other limitations regarding session key have been taught by Chou.

Applicant's argument regarding amended limitation is moot in view of new ground of rejections. See new applied rejections below.

Claim Rejections - 35 U.S.C. § 103

6. The following is a quotation of pre-AIA 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.

7. Claims 48-52, 56-61, 64-69 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali" and further in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar".

Regarding claim 48, Chou discloses system-on-a-chip apparatus comprising:

[a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to]:

generate a random nonce for initiating a request for a secure communication session with a [remote] server over a network using the nonce (Fig. 1 and associated text: Client hello message 150 is sent from first network device-client- to second network device-server. Fig. 2A and associated text: Client hello message 150 includes first random number-random nonce. Col. 7, lines 22-23: “the first random number generated by the first network device”);

perform a cryptographic key exchange with the [remote] server (Fig. 1, step 180 and associated text: client key exchange message is sent to second network device-server);

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the [remote] server and decrypt messages received from the [remote] server during the secure communication session (Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120);

[encrypt the symmetric session key based on the security key]; and

store the encrypted session key in the [secure memory] (Chou does not explicitly disclose about storing the session key; however, in order for using the key to

communicate between the two device in a period of time-a session of communication-, it is obvious that the key must be stored), [the system-on-a-chip] to establish the secure communication session with the remote server over the network using the session key (Col. 4, lines 60-63: Client Hello message 150 is a message that provides second network device 120 with information that is used to establish secured communications between network devices 110 and 120. Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120).

Chou does not explicitly disclose the secure communication session is with a ***remote*** server. However, generating session key for secure communication with a remote server is known in the art and Ali's teaching is an example (Paragraph [0039]: "Client applications on the Internet, such as standard web browsers, can connect to the web server on the smart card using HTTPS protocol. The TLS client side implementation allows the smart card to initiate a secure HTTPS connection to a remote web server on the Internet."

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou's invention of establishing a secure communication session with the server over the network using a session key with Ali's invention of secure communication session is with a remote server. The motivation to do so would be enable secure communications end-to-end between the resource-constrained device and the remote node as taught by Ali (paragraph [0007]).

Chou and Ali do not explicitly disclose **a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key** and is stored **in the secure memory**.

However, in the field of protecting data, Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: It is obvious that Processor 22 could also be a secure processor-TPM/system-on-a chip-with Proc. Unit 30 is a secure nonvolatile and the Proc. Unit 30 is the execution engine. Col. 2, lines 17-19: In a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM) that was encoded in the secure memory during a manufacturing process of the system-on-a-chip (Fig. 1: Proc. Unit 30 has PUK 70. Col. 3, lines 2-7: a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form), the session key is encrypted based on the security key and is stored in the secure memory (Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP.

Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, it is obvious that PKU is also used to encrypt SK to protect SK from attacker.)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Ali's invention of establishing a secure communication session with the remote server over the network using a session key with a system on a chip that contains a secure memory to store session key and the session is encrypted using a key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip as taught by Kumar. The motivation to do so would be to protect data and to seal sensitive information or secrets to a secure area as taught by Kumar (Col. 1, line 8 and Col. 2, lines 17-19).

Regarding claim 49, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (Chou, Figs. 1, 2B and associated text: server hello message 160-response message- includes random number 260. Col. 4, lines 43-57: previously required and stored elements are used for second phase of authentication. It is obvious that server nonce is saved for using in second phase authentication. Combining with Kumar's teaching of secure memory as in claim 48 above, it is obvious to have the server's nonce stored in the secure memory to protect the nonce from being compromised).

Regarding claim 50, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server (Chou, Col. 5, lines 50-61: first network device generates Pre-Master key. Pre-master key is encrypted with the public key of second network device and is sent to second network device-server. Kumar, Col. 3, lines 27-34: 3PKs are used to generate session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. The combination of Chou and Kumar's teaching makes it obvious that pre-master key is generated and encrypted using the security key of the security engine).

Regarding claim 51, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Kumar, Col. 1, lines 41-46: The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, the combination of Chou and Kumar's teachings make it obvious that PKU is also used to encrypt pre-master key and store it in the secure memory to protect it from attacker.)

Regarding claim 52, Chou and Kumar disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine is further to:

generate the session key as a function of the pre-master key (Col. 5, lines 61-65: a master key is produced from the pre-master key); and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Claims 56-58 and 64-66 are rejected because they disclose similar subject matter to claims 48-50 respectively.

Claims 59 and 67 are rejected because they disclose similar subject matter to claim 48.

Claims 60-61 and 68-69 are rejected because they disclose similar subject matter to claim 52.

8. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (*http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf*), *hereinafter, "Stallings", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho"..*

Regarding claim 53, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48. Chou further discloses that client hello message includes list of cryptographic algorithms supported by first network device 110 such as Ephemeral Diffie-Hellman (DHE). Chou also discloses data is encrypted with server's public key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server).

Chou, Ali, and Kumar do not explicitly disclose wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie- Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

However, using Diffie-Hellman public and private keys in handshake process, signing and sending data are well-known in the art and Stallings' teaching is an example

(page 540: “Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key.”)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings’ invention of using Diffie-Hellman keys, signing and sending data. The motivation to do so would be to provide authentication.

Chou, Ali, Kumar and Stallings do not explicitly disclose that the security engine ***generate*** the Diffie-Hellman keys itself. However, generating Diffie-Hellman keys by sender is known in the art and Ho’s teaching is an example ((Fig. 3, step 0a and associated text: a secret (private) key is chosen and a public key is computed. Paragraph [0038]: public key generated initiating device A-client- is used for Diffie-Hellman key exchange).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, Kumar and Stallings' inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store

sensitive information with using Diffie-Hellman keys, signing and sending data and with Ho's invention of generating Diffie-Hellman keys by sender. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Regarding claim 54, Chou, Ali, Kumar, Stallings and Ho disclose the system-on-a-chip apparatus of claim 53. Ho further discloses wherein the security engine to receive a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A) and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key (step 5a and associated text: DHkey-session key- is computed based on Private key of device A –client- and public key of Device B-server).

9. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf), hereinafter, "Stallings".

Regarding claim 55, Chou, Ali and Kumar disclose the system-on-a-chip apparatus of claim 48. Kumar also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou, Ali and Kumar do not explicitly disclose wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server.

However, receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server are well-known in the art and Stallings' teaching is an example (page 541: "Anonymous Diffie-Hellman: The message content consists of the two global Diffie-Hellman values (a prime number and a primitive root of that number) plus the server's public Diffie-Hellman key.")

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server. The motivation to do so would be to provide web security for client and server.

Regarding claim 63, Chou, Ali, and Kumar disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 9 above). Chou further disclose:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each

hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Chou, Ali, and Kumar do not explicitly disclose signing the hash code using a security key stored in a secure memory of the security engine and sending a client certificate verification message to the server, the client certificate verification message including the signed hash code. However, signing hash code and sending a client certificate verification message are well-known in the art and Stallings' teaching is an example (page 540: "Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key." Page 542: "the client may send a certificate_verify message to provide explicit verification of a client certificate… This message signs a hash code based on the preceding messages, defined as follows:

```
CertificateVerify.signature.md5_hash
```

```
MD5(master_secret || pad_2 || MD5(handshake_messages ||
master_secret || pad_1));
Certificate.signature.sha_hash
SHA(master_secret || pad_2 || SHA(handshake_messages ||
      master_secret || pad_1));)
```

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of signing and sending signed data. The motivation to do so would be to provide authentication and to ensure secure communication for involved parties.

Claims 62 and 70 are rejected because they disclose similar subject matter to the combination of claims 53 and 54.

Claim 71 is rejected because it discloses similar subject matter to claim 63.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH T. LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-Th 8:30 am- 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. 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.

/THANH T. LE/

Examiner, Art Unit 2495

/FARID HOMAYOUNMEHR/

Supervisory Patent Examiner, Art Unit 2495

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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-2004/0158715 A1	08-2004	Peyravian, Mohammad	H04L9/3013	713/171
*	B	US-2005/0213766 A1	09-2005	Goss, Steven C.	G06F21/72	380/277
*	C	US-2006/0041938 A1	02-2006	Ali; Asad Mahboob	G06Q20/341	726/14
*	D	US-2006/0117177 A1	06-2006	Buer; Mark L.	G06F21/606	713/155
*	E	US-7,382,882 B1	06-2008	Immonen; Olli	H04L63/0428	380/247
*	F	US-2010/0042824 A1	02-2010	Lee; Ruby B.	G06F21/6218	713/2
*	G	US-2010/0042839 A1	02-2010	Ho; Jin-Meng	H04L9/3226	713/169
*	H	US-7,966,646 B2	06-2011	Chou; Randy	H04L63/166	726/2
*	I	US-2011/0302638 A1	12-2011	Cha; Inhyok	G06F21/57	726/6
*	J	US-2012/0137126 A1	05-2012	MATSUOKA; Kazunari	H04L9/0838	713/156
*	K	US-8,364,975 B2	01-2013	Kumar; Mohan J.	G06F21/57	380/277
*	L	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
*	M	US-9,317,708 B2	04-2016	Lee; Ruby B.	G06F21/6218	1/1

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	http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf. Pages 317-327 and 528-549 (Book was published November 16, 2005).
	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.

Petitioner Samsung Ex-1004, 0652

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.T.L/	1	20050213766	A1	2005-09-29	Goss	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/T.T.L/	1	WO00/02358	WO	A1	2000-01-13	Nokia Mobile Phones Limited		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0653

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

/T.T.L/		First Office Action for Chinese Application No. 201180075550.4, dated June 1, 2016, 5 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/THANH T LE/	Date Considered	01/03/2017

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2016-08-11
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Petitioner Samsung Ex-1004, 0656

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016	01/11/2017						
	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	-	-	-						

Petitioner Samsung Ex-1004, 0657

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016	01/11/2017						
	37	-	-	-						
	38	-	-	-						
	39	-	-	-						
	40	-	-	-						
	41	-	-	-						
	42	-	-	-						
	43	-	-	-						
	44	-	-	-						
	45	-	-	-						
	46	-	-	-						
	47	-	-	-						
	48	✓	✓	✓						
	49	✓	✓	✓						
	50	✓	✓	✓						
	51	✓	✓	✓						
	52	✓	✓	✓						
	53	✓	✓	✓						
	54	✓	✓	✓						
	55	✓	✓	✓						
	56	✓	✓	✓						
	57	✓	✓	✓						
	58	✓	✓	✓						
	59	✓	✓	✓						
	60	✓	✓	✓						
	61	✓	✓	✓						
	62	✓	✓	✓						
	63	✓	✓	✓						
	64	✓	✓	✓						
	65	✓	✓	✓						
	66	✓	✓	✓						
	67	✓	✓	✓						
	68	✓	✓	✓						
	69	✓	✓	✓						
	70	✓	✓	✓						
	71	✓	✓	✓						

Petitioner Samsung Ex-1004, 0658

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S90	2	("7382882").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/01/04 08:16
S91	0	(2004/0158715).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/01/04 09:08
S92	7	2004/0158715	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 09:09
S93	2	("20040158715").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/01/04 09:09
S94	200	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory) and ((key with exchang$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 11:30
S95	194	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory) and ((key near4 exchang$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 11:31
S96	138	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory) and ((key near4 exchang$3) (session adj key)) and (random with (nonce number))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 11:33
S97	1669	(@pd<"20111215" @ad<"20111215") and	US-PGPUB;	OR	ON	2017/01/04

Petitioner Samsung Ex-1004, 0659

		((system$1on$1a$1chip SOC) with key)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			12:37
S98	14	(@pd<"20111215" @ad<"20111215") and ((system$1on$1a$1chip SOC) with key) and (key with secure with memory) and ((key near4 exchang$3) (session adj key)) and (random with (nonce number))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 12:37
S99	5	(@pd<"20111215" @ad<"20111215") and ((system$1on$1a$1chip SOC) with key) and (key with secure with memory) and ((key near4 exchang$3) (session adj key)) and (nonce)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/04 21:13
S100	2	("7382882").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/01/05 12:23
S101	400	("5657390").URPN.	USPAT	OR	ON	2017/01/05 15:01
S102	1543	(@pd<"20111215" @ad<"20111215") and ((transport adj layer adj security) (secure adj sockets adj layer) SSL TLS) and (Diffie$1Hellman)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 16:19
S103	213	(@pd<"20111215" @ad<"20111215") and ((transport adj layer adj security) (secure adj sockets adj layer) SSL TLS) and (Diffie$1Hellman) and ((secure adj memory) system$1on$1the$1chip (tamper adj resistant) (secure adj chip))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 16:23
S104	38	(US-20050005093-$ or US-20100205443-$ or US-20060041938-$ or US-20100042839-$ or US-20050213766-$ or US-20110235806-$ or US-20140270166-$ or US-20110231923-$ or US-20040158715-$ or US-20080244267-$ or US-20120257757-$ or US-20110161370-$ or US-20090235090-$ or US-20060174110-$ or US-20120137126-$ or US-20110302638-$ or US-20060117177-$ or US-20100042824-$).did. or (US-8627440-$ or US-7966646-$ or US-5657390-$ or US-7096352-$ or US-6449720-$ or US-8571221-$ or US-8549297-$ or US-8364975-$ or US-8296581-$ or US-7366306-$ or US-6385597-$ or US-9317708-$ or US-7382882-$).did. or (US-20050005093-$ or US-20100042839-$ or US-20050213766-$	US-PGPUB; USPAT; DERWENT	OR	ON	2017/01/06 16:23

Petitioner Samsung Ex-1004, 0660

		or US-20110113244-$ or US-20100299525-$ or US-20100100953-$ or US-20140270166-$).did.				
S105	211	S103 not S104	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 16:24
S106	126	S105 and manufacture	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 16:31
S107	93	S105 and ((key secret) with manufacture)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 16:43
S108	3	elgamal.in. and handshak$3 and session adj key and Diffie$1hellman	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/01/06 17:38

EAST Search History (Interference)

<This search history is empty>

1/11/2017 7:55:33 PM
C:\Users\tle22\Documents\EAST\Workspaces\13997412.wsp

Petitioner Samsung Ex-1004, 0661

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

CPC- SEARCHED		
Symbol	Date	Examiner
H04L9/0838 H04L9/0841 H04L9/0861 with text	8/14/2015	T.L

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and assignee search with text	8/14/2015	T.L
Interference search with text	8/14/2015	T.L
International and foreign search	8/14/2015	T.L
713/171 with text	8/14/2015	T.L
text based search of claim keywords and synonyms	8/14/2015	T.L
NPL search in IP.com	8/14/2015	T.L
Update Search	4/27/2016	T.L
Update search	1/4/2017	T.L

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

Petitioner Samsung Ex-1004, 0662

BARNES & THORNBURG LLP
11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	2495
Examiner:	Le, Thanh T.
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	April 3, 2014
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

APRIL 24, 2017

RESPONSE TO NON-FINAL OFFICE ACTION

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

Sir:

In response to the Non-Final Office Action dated January 23, 2017, please consider the following:

Listing of the Claims, which begin on page **2**; and

Remarks, which begin on page **9**.

Petitioner Samsung Ex-1004, 0663

LISTING OF THE CLAIMS

1-47. (Canceled)

48. (Previously Presented) A system-on-a-chip apparatus comprising:

a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to:

generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce;

perform a cryptographic key exchange with the remote server;

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the symmetric session key based on the security key; and

store the encrypted session key in the secure memory,

the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key.

49. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory.

50. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server.

Petitioner Samsung Ex-1004, 0664

51. (Previously Presented) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory.

52. (Previously Presented) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to:

generate the session key as a function of the pre-master key; and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

53. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using the security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

54. (Previously Presented) The system-on-a-chip apparatus of claim 53, wherein the security engine is further to receive a public Diffie-Hellman server key from the remote server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

55. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the remote server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure memory.

Petitioner Samsung Ex-1004, 0665

56. (Previously Presented) A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

initiating, using the client device, a request for a secure communication session with a remote server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server;

generate a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypting the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

storing the encrypted session key in the secure memory of the security engine of the system-on-a-chip; and

establishing, using the client device, the secure communication session with the remote server using the session key.

57. (Previously Presented) The method of claim 56, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the remote server; and further comprising:

receiving a ServerHello message from the remote server, the ServerHello message including a server nonce; and

storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

58. (Previously Presented) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating a pre-master key in the security engine;

encrypting the pre-master key using the security key of the security engine; and

sending the encrypted pre-master key to the remote server.

Petitioner Samsung Ex-1004, 0666

59. (Previously Presented) The method of claim 58, further comprising:

wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and

storing the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

60. (Previously Presented) The method of claim 58, wherein performing the cryptographic key exchange with the remote server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

61. (Previously Presented) The method of claim 60, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

62. (Previously Presented) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

signing the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

sending the signed public Diffie-Hellman key to the remote server;

receiving a public Diffie-Hellman server key from the remote server; and

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

Petitioner Samsung Ex-1004, 0667

63. (Previously Presented) The method of claim 56, further comprising:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the remote server;

signing the hash code using the security key stored in the secure memory of the security engine; and

sending a client certificate verification message to the remote server, the client certificate verification message including the signed hash code.

64. (Previously Presented) One or more non-transitory machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to:

generate a random nonce in a security engine of a system-on-a-chip of the computing device;

initiate a request for a secure communication session with a remote server over a network, the request including the random nonce;

perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server;

generate, based on the cryptographic key exchange, a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

store the session key in the secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the remote server using the session key.

Petitioner Samsung Ex-1004, 0668

65. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to initiate a request for a secure communication session comprises to send a ClientHello message, including the nonce, to the remote server; and

wherein the plurality of instructions further cause the computing device to: receive a ServerHello message from the remote server, the ServerHello message including a server nonce; and

store the server nonce in the secure memory of the security engine of the system-on-a-chip.

66. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate a pre-master key in the security engine;

encrypt the pre-master key using the security key of the security engine; and

send the encrypted pre-master key to the remote server.

67. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 66, wherein the plurality of instructions further cause the computing device to:

wrap the pre-master key in the security engine of the system-on-a-chip with a server public key, and

store the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

68. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the remote server comprises to generate the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

Petitioner Samsung Ex-1004, 0669

69. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 68, wherein to generate the session key in the security engine comprises to calculate, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

70. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

sign the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

send the signed public Diffie-Hellman key to the remote server;

receive a public Diffie-Hellman server key from the remote server; and

generate, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

71. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein the plurality of instructions further cause the computing device to:

generate, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the remote server;

sign the hash code using the security key stored in the secure memory of the security engine; and

send a client certificate verification message to the remote server, the client certificate verification message including the signed hash code.

Petitioner Samsung Ex-1004, 0670

REMARKS

Applicant thanks the Examiner for consideration of the present application. Applicant has carefully reviewed the Office Action dated January 23, 2017 (hereinafter "the Office Action"). Claims 48-71 are pending in this application. Applicant respectfully requests reconsideration of the present application in light of the remarks presented below.

I. CLAIM LISTING

Although none of the pending claims 48-71 has been amended by the present Response, Applicant has included the above Claim Listing for the convenience of the Examiner.

II. 35 U.S.C. § 103 REJECTIONS

Each of claims 48-52, 56-61, and 64-69 stands rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 7,966,646 of Chou et al. (hereinafter "Chou") in view of U.S. Patent Application No. 2006/0041938 of Asad Mahboob Ali (hereinafter "Ali") and further in view of U.S. Patent No. 8,364,975 of Kumar et al. (hereinafter "Kumar"). Further, each of claims 53, 54, 62, 63, 70, and 71 stands rejected under 35 U.S.C. § 103 as being unpatentable over Chou in view of Ali and Kumar and in view of "Stallings Cryptography and Network Security" by William Stallings (herein after "Stallings") and further in view of U.S. Patent Application No. 2010/0042839 of Ho (hereinafter "Ho"). Additionally, claim 55 stands rejected under Chou in view of Ali, Kumar, and Stallings. It is well settled that the analysis required under 35 U.S.C. § 103(a) must be resolved on the basis of the factual inquiries outlined in *Graham v. John Deere, Co.*, 383 U.S. 1, 148 USPQ 459 (1966); *see KSR v. Teleflex*, 127 S.Ct. at 1740. The *Graham* Court stated that as part of any analysis under Section 103,

> the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

148 USPQ at 467. The analysis of obviousness therefore requires an inquiry into the scope and content of the prior art and, more particularly, an inquiry into whether the prior art discloses all of the elements of the claimed invention.

Petitioner Samsung Ex-1004, 0671

A. Independent Claim 48

In support of the 35 U.S.C. § 103 rejection of independent claim 48, the Office Action asserts that a combination of Chou, Ali, and Kumar describes or suggests every feature of independent claim 48. Applicant disagrees and submits that the proposed combination of references fails to disclose a security engine to "encrypt the symmetric session key based on the security key," which is "encoded in the secure memory during a manufacturing process of the system-on-a-chip" as recited in independent claim 48.

Indeed, the Office Action acknowledged on page 6 that Chou and Ali do not disclose:

> a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory.

To remedy this shortcoming of Chou and Ali, the Office Action relied on Kumar. In support of the proposition that Kumar discloses such features, the Office Action asserted on page 6 that:

> Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: It is obvious that Processor 22 could also be a secure processor-TPM/system-on-a chip-with Proc. Unit 30 is a secure nonvolatile and the Proc. Unit 30 is the execution engine. Col. 2, lines 17-19: In a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM) that was encoded in the secure memory during a manufacturing process of the system-on-a-chip (Fig. 1: Proc. Unit 30 has PUK 70. Col. 3, lines 2-7: a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form),

The Office Action indicated that the TPM 44 is the system-on-a-chip. However, contrary

Petitioner Samsung Ex-1004, 0672

to the Office Action's assertions, the TPM 44 does not comprise a security engine that has a secure memory that includes a security key that was encoded in the secure memory during a manufacturing process of the TPM 44 as recite in claim 48. Instead, Kumar discloses in col. 3, ll. 2-7 that "a processing unit key or PUK [of the processing unit 30, and not the TPM 44] is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form."

It seems that the Office Action is asserting that the TPM 44 may be incorporated into the processing unit 30 and function as a single component. However, Kumar states in col. 8, ll. 49-59 that:

> [P]rocessing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44. Processing unit 30 and TPM 44 may then use SK 74 to create a protected channel, as shown at block 230. That protected channel may traverse multiple system buses 24 and zero or more components of chipset 34. TPM 44 and processing unit 30 may then use SK 74 to encrypt communications, as indicated at block 232. In alternative embodiments, multiple session keys may be used for protecting communications between processing unit 30 and TPM 44.

In other words, the processing unit 30 and the trusted platform module (TPM) 44 are separate components within the same processing system (i.e., within the same computer) that communicates with one another other. As such, the assertion that the processor 22 that includes the processing unit 30 "could also be a secure processor-TPM/system-on-a-chip-with" the processing unit 30 is not supported by Kumar. Accordingly, Kumar fails to disclose or teach at least "a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip" as recited in claim 48.

Moreover, the Office Action asserted on page 6 that Kumar discloses that:

> the session key is encrypted based on the security key and is stored in the secure memory (Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker.

Petitioner Samsung Ex-1004, 0673

> Therefore, it is obvious that PKU is also used to encrypt SK to protect SK from attacker.)

Applicant respectfully submits that the Office Action's assertion that "it is obvious that PKU is also used to encrypt SK to protect SK from attacker" is unsupported by Kumar. As quoted above, Kumar discloses in col. 8, lines 49-52 that "processing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44." In other words, Kumar teaches that the session key (SK) 74 is *created* using the third party key (3PK) 72, and that the 3PK may be encrypted based on the PUK. *See* Kumar, col. 8, ll. 49-52 and col. 2, ln. 67 - col. 3, ll. 1. This is in contrast to *encrypting* a session key generated from a cryptographic key exchange, wherein the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture, in accordance with claim 48. As such, Kumar fails to disclose at least that feature of claim 48.

For at least the reasons discussed above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar does not render claim 48 obvious and Applicant respectfully requests withdrawal of the Section 103 rejection of claim 48.

B. Independent Claim 56

The Office Action also rejected claim 56 under Section 103 as being rendered obvious by Chou, Ali, and Kumar, using similar rational as set forth in the rejection of claim 48. Though different in scope, claim 56 includes features similar to those discussed above with reference to claim 48. Accordingly, Applicant respectfully disagrees with the rejection for at least the reasons provided above in regard to the rejection of independent claim 48. As such, all of the arguments presented above in regard to the rejection of independent claim 48 apply with equal force to the rejection of independent claim 56 and are incorporated into this section by reference.

Accordingly, for at least the reasons provided above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar fails to disclose every feature of independent claim 56. As such, that proposed combination fails to render independent claim 56 obvious. Applicant, therefore, respectfully submits that independent claim 56 is in condition for allowance and such action is respectfully requested.

Petitioner Samsung Ex-1004, 0674

C. Independent Claim 64

The Office Action also rejected claim 64 under Section 103 as being rendered obvious by Chou, Ali, and Kumar, using similar rational as set forth in the rejection of claim 48. Though different in scope, claim 64 includes features similar to those of claim 48, discussed above. As such, Applicant respectfully disagrees with the rejection for at least the reasons provided above in regard to the rejection of independent claim 48. Accordingly, all of the arguments presented above in regard to the rejection of independent claim 48 apply with equal force to the rejection of independent claim 64 and are incorporated into this section by reference.

For at least the reasons provided above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar fails to disclose every feature of independent claim 64. As such, that proposed combination fails to render independent claim 64 obvious. Applicant, therefore, respectfully submits that independent claim 64 is in condition for allowance and such action is respectfully requested.

D. Dependent Claims 49-55, 57-63, and 65-71

Each of claims 49-55 includes independent claim 48 as a base claim; each of claims 57-63 includes independent claim 56 as a base claim; and each of clams 65-71 includes independent claim 64 as a base claim. Stallings and Ho do not cure the deficiencies of Chou, Ali, and Kumar with respect to independent claims 48, 56, and 64. Accordingly, Applicant respectfully requests withdrawal of the Section 103 rejection of claims 49-55, 57-63, and 65-71. Any arguments specific to claims 49-55, 57-63, and 65-71 are held in abeyance without prejudice or admission to any assertion made in the Office Action in order to expedite prosecution.

III. CONCLUSION

In view of the foregoing, it is submitted that this application is in a condition for allowance. Action to that end is hereby solicited. If there are any questions or comments that would expedite prosecution of this application, the Examiner is invited to call the undersigned at (317) 231-7307.

Petitioner Samsung Ex-1004, 0675

It is respectfully requested that, if necessary to effect a timely response, this paper be considered as a Petition for an Extension of Time sufficient to effect a timely response. The Commissioner is hereby authorized to charge the fee for such Petition, if needed, and any shortage of fees, and credit any overpayment of fees, to the Account of Barnes & Thornburg, Deposit Account No. 10-0435 with reference to file P41624US/45631-225521.

Respectfully submitted,

/Scott R Powell/

Scott R. Powell
Registration No. 58,378
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-7307

DMS 4950792v1

Petitioner Samsung Ex-1004, 0676

Electronic Acknowledgement Receipt

EFS ID:	29002093
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/kim tyree
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	24-APR-2017
Filing Date:	03-APR-2014
Time Stamp:	10:49:04
Application Type:	U.S. National Stage under 35 USC 371

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	Amendment/Req. Reconsideration-After Non-Final Reject	P41624_RNFOA.pdf	71112 bbf87048563e41b5391826bd6a68fe7612825466	no	14

Warnings:

Information:	
Total Files Size (in bytes):	71112

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/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 13/997,412	Filing Date 04/03/2014	☐ 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 **04/24/2017**

	(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))	* 24	Minus	** 24	= 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
JACKIE WHITE

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101251879	CN	B	2010-10-13	Intel Corporation		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0680

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

	1	Chinese Office Action for Patent Application No. 201180075550.4, dated March 6, 2017,

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Petitioner Samsung Ex-1004, 0681

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2017-04-27
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0682

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 record s.

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.

Petitioner Samsung Ex-1004, 0683

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101251879 B
(45)授权公告日 2010.10.13

(21)申请号 200710307356.X

(22)申请日 2007.12.28

(30)优先权数据
11/648,472 2006.12.29 US

(73)专利权人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 M·J·库玛 S·格隆

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌

(51)Int.Cl.
G06F 21/00(2006.01)

审查员 崔哲

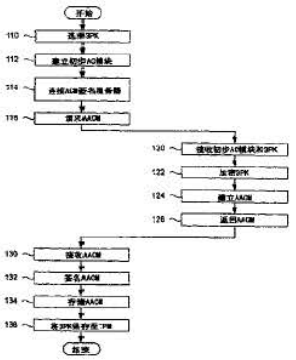
权利要求书 2 页 说明书 8 页 附图 5 页

(54)发明名称

用于保护数据的方法和装置

(57)摘要

一种扩充的引导代码模块包括在引导过程期间由处理单元执行的指令。该扩充的引导代码模块还包括可由无论处理单元重置与否仍保留在该处理单元内的密钥所解密的密钥的加密版本。在一个实施例中，处理单元可以解密该密钥的加密版本并在随后使用解密的密钥建立与诸如可信平台模块(TPM)的安全处理器之间的受保护的通信通道。也描述并要求保护了其他的实施例。



CN 101251879 B

Petitioner Samsung Ex-1004, 0684

1. 一种用于保护数据的方法，所述方法包括：

把来自处理系统的非易失性存储器的密钥的加密版本检索入所述处理系统的处理单元，所述密钥用于在所述处理单元与所述处理系统的安全协处理器之间建立受保护的通信通道；

解密所述密钥的所述加密版本；

在所述处理单元的受保护部分内存储所述解密的密钥；以及

使用所述解密的密钥来在所述处理系统的所述处理单元和安全协处理器之间建立受保护的通信通道。

2. 如权利要求 1 所述的方法，其特征在于，包括：

在有关所述处理系统的引导过程期间，检索来自所述非易失性存储器的所述密钥的所述加密版本。

3. 如权利要求 1 所述的方法，其特征在于，所述检索来自非易失性存储器的所述密钥的所述加密版本的操作包括：

在有关所述处理系统的引导过程期间，检索来自所述处理系统的引导存储器的代码模块；以及

从所述代码模块中提取所述密钥。

4. 如权利要求 1 所述的方法，其特征在于，还包括：

还利用存储在所述安全协处理器内的所述解密的密钥的一个示例来在所述处理单元和所述安全协处理器之间建立所述受保护的通信通道。

5. 如权利要求 1 所述的方法，其特征在于，所述在所述处理单元的受保护部分内存储所述解密的密钥的操作包括：

在所述处理单元无法通过监听通信耦合至所述处理单元的处理系统总线来访问的那一部分内存储所述解密的密钥。

6. 如权利要求 1 所述的方法，其特征在于，还包括：

使用处理单元密钥解密所述密钥的所述加密版本。

7. 如权利要求 6 所述的方法，其特征在于：

所述密钥包括第三方密钥；以及

所述处理单元密钥包括无论所述处理单元重置与否仍保留在所述处理单元内的密钥。

8. 一种用于保护数据的方法，包括：

将第一密钥保存至处理系统的安全协处理器，所述第一密钥被用于在所述处理系统的处理单元和安全协处理器之间建立受保护的通信通道；

将所述第一密钥发送给远程处理系统；

接收来自所述远程处理系统的所述第一密钥的加密版本；以及

将代码模块保存至所述处理系统内的引导存储，其中所述代码模块包括用户数据、所述第一密钥的所述加密版本、以及用第二密钥生成的签名。

9. 如权利要求 8 所述的方法，其特征在于，还包括：

以初步代码模块将所述代码模块的所述用户数据发送给所述远程处理系统；以及

以所述代码模块接收来自所述远程处理系统的所述第一密钥的所述加密版本。

10. 如权利要求 8 所述的方法，其特征在于：

Petitioner Samsung Ex-1004, 0685

所述将所述第一密钥发送给远程处理系统的操作包括将所述第一密钥发送给扩充的鉴别代码模块发生器；以及

所述接收来自所述远程处理系统的所述第一密钥的所述加密版本的操作包括接收来自所述鉴别代码模块发生器的鉴别代码模块，其中所述鉴别代码模块包括所述第一密钥的所述加密版本。

11. 如权利要求 8 所述的方法，其特征在于：

用于生成所述代码模块的所述签名的所述第二密钥包括私钥；以及

所述方法包括将对应于所述私钥的公钥载入所述代码模块。

12. 一种用于保护数据的处理系统，包括：

处理单元；

与所述处理单元通信的非易失性存储器，所述非易失性存储器存储密钥的加密版本，所述处理单元能用处理单元密钥解密所述密钥的所述加密版本；以及

与所述处理单元通信的安全协处理器，

其中所述安全协处理器通过在所述处理单元与所述安全协处理器之间建立的受保护的通信通道与所述处理单元通信，所述受保护的通信通道通过使用所解密的密钥来建立。

13. 如权利要求 12 所述的处理系统，其特征在于，在所述处理单元的受保护存储无法通过监听通信耦合至所述处理单元的处理系统总线来访问。

14. 如权利要求 12 所述的处理系统，其特征在于：

所述密钥包括第三方密钥。

Petitioner Samsung Ex-1004, 0686

用于保护数据的方法和装置

发明领域

[0001] 本公开一般涉及数据处理领域，尤其涉及用于保护数据的方法和相关的装置。

背景技术

[0002] 处理系统可以包括硬件资源，诸如中央处理单元 (CPU)、随机存取存储器 (RAM) 和非易失性存储器。处理系统还可以包括软件资源，诸如基本输入输出系统 (BIOS)、虚拟机监控程序 (VMM)、以及在 VMM 上运行的一个或多个客户机操作系统 (OS)。当计算机系统被启动或重置时，它可以载入 BIOS，并在随后载入 VMM。VMM 随后可以创建一个或多个虚拟机，并且这些虚拟机可以引导不同的 OS 或相同 OS 的不同示例。

[0003] 除了 RAM 和一个或多个 CPU 之外，处理系统还可以包括安全协处理器，诸如可信平台模块 (TPM)。TPM 是位于处理系统内的硬件组件，并提供了用于增强处理系统的安全性的各种设备和服务。例如，TPM 可以被实现为集成电路 (IC) 或半导体芯片，并且它可用于保护数据并证明一平台的配置。TPM 可以依照包括诸如设计原理、TPM 结构和 TPM 命令等部分的规范，诸如于 2003 年 10 月 2 日发布的 Trusted Computing Group(TCG) TPM Specification Version 1.2(可信计算小组 (TCG) TPM 规范版本 1.2)(下称“TPM 规范”) 来实现。该 TPM 规范由 TCG 公布并可从网址 www.trustedcomputinqqroup.org/home 处获取。

[0004] TPM 的子组件可以包括执行引擎和安全非易失性 (NV) 存储器或存储。安全 NV 存储器用于存储诸如加密密钥之类的敏感信息，而执行引擎则根据由 TPM 的控制逻辑指定的安全策略来保护这些敏感信息。

[0005] 一般而言，遵从 TCG 的 TPM 基于平台特性提供诸如证明身份和 / 或平台完整性等安全服务。TPM 通常考虑的平台特性包括平台的硬件组件，诸如处理器和芯片组，以及驻留在平台内的软件，诸如固件和 OS。TPM 还可以支持软件进程的审查和日志记录，平台引导完整性、文件完整性以及软件许可的验证。因此就可认为 TPM 是针对平台的信任根。

发明内容

[0006] 本发明提供了一种用于保护数据的方法，所述方法包括：把来自处理系统的非易失性存储器的密钥的加密版本检索入所述处理系统的处理单元；解密所述密钥的所述加密版本；在所述处理单元的受保护部分内存储所述解密的密钥；以及使用所述解密的密钥来在所述处理系统的所述处理单元和安全协处理器之间建立受保护的通信通道。

[0007] 根据本发明的另一方面，提供了一种用于保护数据的方法，包括：将第一密钥保存至处理系统的安全协处理器，所述第一密钥被用于在所述处理系统的处理单元和安全协处理器之间建立受保护的通信通道；将所述第一密钥发送给远程处理系统；接收来自所述远程处理系统的所述第一密钥的加密版本；以及将代码模块保存至所述处理系统内的引导存储，其中所述代码模块包括用户数据、所述第一密钥的所述加密版本、以及用第二密钥生成的签名。

[0008] 根据本发明的又一方面，提供了一种处理系统，包括：处理单元；与所述处理单元

Petitioner Samsung Ex-1004, 0687

通信的非易失性存储器；以及与所述处理单元通信的安全协处理器；其中所述处理单元被配置用于：把来自处理系统的非易失性存储器的密钥的加密版本检索入所述处理系统的处理单元；用处理单元密钥解密所述密钥的所述加密版本；在所述处理单元的受保护部分内存储所解密的密钥；以及使用所解密的密钥来在所述处理系统的所述处理单元和安全协处理器之间建立受保护的通信通道。

附图说明

[0009] 本发明的特征和优点将从所附权利要求书、以下对一个或多个示例实施例的详细描述以及相应的附图中变得显而易见，附图中：

[0010] 图 1 是描绘了在其中可以实现本发明一个示例实施例的某些方面的合适数据处理系统的框图；

[0011] 图 2 是描绘了涉及图 1 的数据处理系统的示例性数据处理环境的框图；

[0012] 图 3 是根据本发明一个示例实施例的用于向图 1 的处理系统供给第三方密钥的过程的流程图；

[0013] 图 4 是根据本发明一个示例实施例的扩充的鉴别代码模块的框图；以及

[0014] 图 5 是根据本发明一个示例实施例的用于在处理单元和安全协处理器之间建立受保护的通信通道的过程的流程图。

具体实施方式

[0015] 在带有 TPM 的平台内，可以使用平台测量和加密来将敏感信息或秘密密封至 TPM。例如，在带 VMM 的处理系统中，可以使用 VMM 和其他平台组件的测量来将秘密密封至 TPM。TPM 可以避免秘密在随后被泄漏或者从 TPM 开封，除非 VMM 和其他平台测量被验证与用于密封的测量匹配。然而，当秘密被开封时，它会在 TPM 和 CPU 之间在处理系统内经由通信通道以纯文本（即，未加密）传送。

[0016] 本发明公开描述了用于在安全协处理器（例如，TPM）和处理单元（例如，CPU）之间以加密格式通信秘密的机制和过程。因此，即使攻击者监听处理系统内的内部总线，攻击者也无法截取纯文本秘密。

[0017] 描述的机制和过程适于为例如有关数字权限管理 (DRM) 的高价值内容提供增强的保护。如下将进一步详述的那样，在一个实施例中，在 TPM 和 CPU 之间的通信通道上的数据使用每会话密钥来加密。此外，CPU 和 TPM 被预先供给密钥（在此被称为“第三方密钥”或“3PK”），用来鉴别会话结束点并创建每会话密钥。

[0018] 为了本公开的目的，对于处理单元并对于包括处理单元的处理系统而言，“第一方”是处理器的制造商，而“第三方”是与该处理单元或处理系统相关联的任何其他实体。例如，处理系统的制造商和处理系统的所有者都被认为是“第三方”。

[0019] 再次参考第三方密钥，CPU 的制造商没有必要将 3PK 载入 CPU 或 TPM。的确，因为 TPM 与平台相关联，所以若是 CPU 制造商并未装配平台，那么 CPU 制造商可能没有机会将 3PK 载入 TPM。相反地，3PK 以及将其载入处理系统的过程可以主要由某些其他方控制，诸如处理系统的制造商。例如，如下将进一步详述的那样，当建立处理系统时，原始设备制造商 (OEM) 可以获取已被扩充成包含要被安装在该处理系统的 CPU 内的第三方密钥的鉴别码

Petitioner Samsung Ex-1004, 0688

(AC) 模块。如下面进一步详述的那样，在扩充的 AC 模块 (AACM) 内，3PK 可由基于处理单元密钥 (PUK) 的加密所保护。AACM 还可用签名保护。出于本公开的目的，处理单元密钥或 PUK 是在制造处理器时存储在该处理器内的密钥，并且以非易失性的形式保留在处理器内。例如，处理器可以保留该密钥，而不考虑该处理器的功率循环或重置。

[0020] AACM 可以被存储在引导存储（例如，通常含有 BIOS 代码的闪存）内。平台建造者也可在平台制造期间将 3PK 安装入该平台的 TPM。随后，在重置时，CPU 可以查找并运行该 AACM。因此，AC 模块以及已用加密的 3PK 扩充的类似类型的模块就可被认为是扩充的引导代码模块。在一个实施例中，CPU 可以使用固件接口表 (FIT) 作为用于查找和运行 AACM 的标准机制。有关 FIT 的额外信息在日期为 2003 年 12 月的**Intel® Itanium®** Processor Family System Abstraction LayerSpecification（**Intel® Itanium®**处理器家族系统抽象层规范）中提供，这可以从因特网 download.intel.com/design/Itanium/Downloads/24535907.pdf 获取。当运行时，AACM 可以将 3PK 安装至仅可由特权代码修改的 CPU 寄存器。于是，一平台可以使用在此描述的方法而将 OEM 密钥输入 BIOS 存储器并且在每次导入时将其安全地安装入处理器。

[0021] AACM 还可以初始化 TPM 并创建会话密钥，该密钥将由处理器和 TPM 用来加密在这两个组件之间交换的数据。例如，一旦 3PK 已经被安装入处理器和 TPM，这些密钥又可使用标准加密方案用于生成一个或多个会话密钥。该会话随后可用于保护在处理器和 TPM 之间的通信。

[0022] 描述的解决方案允许在 CPU 和诸如 TPM 之类的安全处理器之间的安全通信，由此就能反抗哪怕是拥有高级监听硬件和对机器进行物理访问的攻击者，从而确保安全交换。例如，根据本公开的平台可以确保用于保护数据内容的密钥（例如，用于保护运动图像专家组 (MPEG) 影片的密钥、用于保护信用卡信息数据库的密钥等）免受基于目标内探针 (ITP) 的攻击。

[0023] 此外，本公开描述了一种灵活便利的方式来向平台供给密钥以建立受保护通信通道。密钥可由第三方选择并由该第三方安装入平台。3PK 密钥无需内建于处理器。处理器制造商因此无需知晓 3PK。此外，如果要将处理器返回给制造商，也可以在不危及 3PK 的安全的情况下重新使用该处理器。如果需要则可以由可信代理改变该 3PK，并且 3PK 可以仅在处理器存在于平台内时被系至该处理器。

[0024] 图 1 是描绘了在其中可以实现本发明一个示例实施例的某些方面的合适数据处理系统 20 的框图。数据处理系统 20 具有经由一个或多个系统总线 24 或其他通信路径或介质与各种其他组件通信耦合的各种硬件组件 82，诸如中央处理单元 (CPU) 22。本公开使用术语“总线”来指代共享的通信路径以及点对点路径。CPU 22 可以包括两个或多个处理单元，诸如处理单元 30 和处理单元 32。可选地，处理系统可以包括带有一个处理单元的 CPU，或者各自具有至少一个处理单元的多个处理器。处理单元可由超线程 (HT) 技术或由用于同时或大致同时执行多线程的任何其他合适技术来实现为处理核。

[0025] 正如在此使用的，术语“处理系统”和“数据处理系统”旨在广泛地包含单个机器，或者通信上耦合的共同工作的机器或设备的系统。示例性处理系统包括但不限于：分布式计算系统、超级计算机、高性能计算系统、计算集群、大型计算机、微型计算机、客户机 - 服务器系统、个人计算机、工作站、服务器、便携式计算机、膝上型计算机、图形输入板、电话

Petitioner Samsung Ex-1004, 0689

机、个人数字助理 (PDA)、手持式设备、诸如音频和 / 或视频设备等娱乐设备、以及用于处理或传输信息的其他设备。

[0026] 处理系统 20 可至少部分地通过来自诸如键盘、鼠标等的常规输入设备的输入，和 / 或通过接收自另一台机器、生物测定反馈、或其他输入源或信号的指示来控制。处理系统 20 可以利用对一个或多个远程数据处理系统的一个或多个连接，诸如通过网络接口控制器 (NIC)40、调制解调器或其他的通信端口或耦合。处理系统可以通过诸如局域网 (LAN)、广域网 (WAN)、内联网、因特网之类的物理和 / 或逻辑网络的方式互连。涉及网络的通信可以利用各种有线和 / 或无线近程或远程载体和协议，包括射频 (RF)、卫星、微波、电气和电子工程师协会 (IEEE)802.11、802.16、802.20、蓝牙、光学、红外线、电缆、激光等等。有关 802.11 的协议也被称为无线高保真 (WiFi) 协议。有关 802.16 的协议也被称为 WiMAX 或无线城域网协议，有关这些协议的信息当前可从 grouper.ieee.org/groups/802/16/published.html 获得。

[0027] 图 2 是描绘了涉及图 1 的处理系统 20 的一个示例性数据处理环境 12 的框图。更具体地，数据处理环境 12 包括作为本地处理系统的处理系统 20，以及被称为 AACM 发生器 80 的远程处理系统。处理系统 20 和 AACM 发生器 80 可以经由网络 90 通信。例如，处理系统 20 可位于 OEM 装配厂 102 内，并且当 OEM 正装配或配置处理系统 20 时，OEM 可以使得处理系统 20 与 AACM 发生器 80 通信以向处理系统 20 供给该 OEM 专用的 3PK，这在以下将参考图 3 更为详尽地描述。更具体地，如下所述，OEM 可以使得 AACM 发生器 80 在初步 AC 模块中嵌入 3PK 72，由此将其转换成该 OEM 专用的 AACM。

[0028] 再次参考图 1，在处理系统 20 中，处理器 22 可以通信耦合至一个或多个易失性或非易失性数据存储设备，诸如 RAM 26、只读存储器 (ROM)42、诸如硬盘驱动器的大容量存储设备 36、和 / 或诸如软盘、光学存储、磁带、闪存、记忆棒、数字视频盘等的其他设备或介质。为了本公开的目的，术语“ROM”通常用于指代诸如可擦除可编程 ROM(EPROM)、电可擦除可编程 ROM(EEPROM)、闪速 ROM、闪存等的非易失性存储器设备。处理器 22 还可以通信耦合至另外的组件，诸如视频控制器、集成驱动器电子电路 (IDE) 控制器、小型计算机系统接口 (SCSI) 控制器、通用串行总线 (USB) 控制器、输入 / 输出 (I/O) 端口、输入设备、诸如显示器之类的输出设备等等。

[0029] 在图 1 的实施例中，处理系统 20 还包括 TPM 44。在其它实施例中，也可以使用其他类型的安全协处理器。处理器 22、RAM 26、TPM 44 和其他组件可以连接至芯片组 34。芯片组 34 可包括用于通信耦合系统组件以及其他逻辑和存储组件的一个或多个桥或集线器。

[0030] 诸如视频控制器等某些组件例如可以被实现为用来与总线通信的带接口 (例如，PCI 连接器) 的适配器卡。在一个实施例中，一个或多个设备可以被实现为使用诸如可编程或不可编程逻辑器件或阵列、专用集成电路 (ASIC)、嵌入式计算机、智能卡等组件的嵌入式控制器。

[0031] 本发明在此可以参考诸如指令、函数、过程、数据结构、应用程序、配置设置等的数据来描述。当这些数据被机器访问时，会使该机器通过执行定义抽象数据类型或低级硬件上下文的任务，和 / 或执行诸如将在以下更为详细地描述的其他操作来响应。该数据可以被存储在易失性和 / 或非易失性数据存储中。为此公开的目的，术语“程序”覆盖广义范围的软件组件和构造，包括应用程序、驱动程序、过程、例程、方法、模块和子程序。术语“程序”

Petitioner Samsung Ex-1004, 0690

可用于指代一完整编译单位（即，可被独立编译的一组指令）、编译单位的集合或者编译单位的一部分。于是，术语“程序”可用于指代在由处理系统执行时会执行期望的一个或多个操作的任何指令的集合。在处理系统 20 内的程序可被认为是软件环境 84 的组件。

[0032] 例如，当处理系统 20 导入时，BIOS 50 和 VMM 52 可被载入 RAM 26 并在软件环境 84 内执行。BIOS 50 例如可以根据日期为 2006 年 1 月 31 日的 Version 2.0 ofthe Unified Extensible Firmware Interface Specification（统一可扩展固件接口规范版本 2.0）来实现。ROM 42 还可以包括诸如扩充的 AC 模块 (AACM) 60 之类的模块，这在如下将进一步详述。

[0033] 图 3 是根据本发明一个示例实施例用于向处理系统 20 供给 3PK 的过程的流程图。示出的过程与由 OEM 管理的装配或配置操作有关，该过程在 OEM 选择要向其供给 3PK 的处理系统 20 之后开始。在框 110，OEM 选择要供给的 3PK。

[0034] 在框 112，OEM 准备初步的 AC 模块。在该示例性的实施例中，OEM 为该 AC 模块使用诸如在日期为 2006 年 9 月的 LaGrande Technology PreliminaryArchitecture Specification（拉格朗日技术初步架构规范，其后称为“LTPA 规范”）描述的格式。该 LTPA 规范当前可从因特网 www.intel.com/technology/security/downloads/LT_spec_0906.pdf 获取。

[0035] 图 1 的示例性处理系统使用被称为更安全模式扩展 (SMX) 的功能来提供发射和控制接口。有关 SMX 的额外信息可从 LTPA 规范获取。该 LTPA 规范还描述了如何鉴别并执行 AC 模块。例如，第 11 和 12 页提供了下列解释：

[0036] •为支持受保护环境的建立，SMX 启用鉴别代码执行模式的能力。这提供了用于将被称为鉴别代码模块（AC 模块）的特定代码模块载入处理器的内部 RAM（被称为鉴别代码执行区）的能力。该 AC 模块首先被鉴别并在随后使用抗篡改方法执行。

[0037] • 鉴别是通过使用在 AC 模块头内的数字签名来实现的。处理器计算 AC 模块的散列并使用该结果来使签名有效。使用 SMX，处理器将仅初始化处理器状态或在其通过鉴别的情况下执行 AC 代码模式。因为鉴别代码模块被保持在处理器的内部 RAM 内，所以该模块的执行能够与外部存储器的内容或外部处理器总线上的活动隔离地进行。

[0038] 再次回到框 112，为了准备初步 AC 模块，OEM 可以将用户代码 / 数据载入初步 AC 模块的用户区。在此，初步 AC 模块用作需要被嵌入扩充的 AC 模块的 OEM 内容的格式化输入。处理系统 20 还可以填充该初步 AC 模块的其他部分，诸如大小字段。

[0039] 如框 114 所示，处理系统 20 随后连接至 AACM 发生器 80。在此示例性实施例中，处理系统 20 和 AACM 发生器 80 建立用于通信加密数据的安全通道。可以使用任何合适的技术来建立这条安全通道。如框 116 所示，处理系统 20 随后可以将信息或请求 84 发送给 AACM 发生器 80。如图 2 所示，请求 84 可以包括初步 AC 模块以及期望的 3PK。在此示例性实施例中，初步 AC 模块将含有 OEM 或第三方制造商填充用以指示寻找该 AACM 的处理器家族的字段。如框 120 和 122 所示，AACM 发生器 80 可以从处理系统 20 接收初步 AC 模块和 3PK，并可以在随后加密 3PK。

[0040] 在图 2 的实施例中，AACM 发生器 80 由处理器 22 的制造商管理，并且 AACM 发生器 80 使用预定的处理器制造密钥 (PMK) 71 来加密 3PK。在图 2 的实施例中，PMK 71 是私钥，并且处理单元 30 包括作为相应公钥的 PUK 70。在另一个实施例中，PMK 和 PUK 可以是相同

Petitioner Samsung Ex-1004, 0691

的密钥（即，它们可以具有相同的值）。

[0041] 在图 1 的实施例中，PUK 70 可由处理器 22 的制造商在制造过程中，在将处理器 22 发送给诸如 OEM 的买方之前永久性地烧入处理单元 30。处理器 22 的制造商可以把 PMK 71 保密，以使得没有其他实体能知晓该 PMK 71 的值。另外，处理器制造商可以安排个别可信实体来管理 AACM 发生器 80。虽然 PUK 70 可被认为是“公”钥，但是它可以被保密，以使得它的值从不被处理单元 30 泄漏。

[0042] 再次回到图 3，如框 124 所示，AACM 发生器 80 随后建立包括加密的 3PK(E3PK)72A 的 AACM 60。更具体地，再回到图 2，当建立 AACM 60 时，AACM 发生器 80 可以将 E3PK 附至初步 AC 模块的用户数据，并且更新该模块大小字段。另外，AACM 60 可以包括用以保持加密 3PK 的预定义字段。包括 3PK 加密版本的 AACM 也可被称为加密的 AC 模块。

[0043] 再次参考图 3，如框 126 所示，AACM 发生器 80 随后将 AACM 60 发送给处理系统 20。在框 130，处理系统 20 可以接收来自 AACM 发生器 80 的 AACM 60。随后如框 132 所示，处理系统 20 可以签名 AACM 60。例如，OEM 可以选择一个 AC 模块密钥对，诸如里维斯特 - 沙米尔 - 阿德尔曼 (Rivest,Shamir,Adelman(RSA)) 公钥 / 私钥对，并在随后将来自该对的公钥载入 AACM 60 的头部。OEM 很可能基于用户区的散列或可能是 AACM 60 的其他部分而使用来自该对的私钥生成用于该 AACM 60 的 RSA 签名。OEM 随后可以在 AACM 60 的头部内存储该 RSA 签名。

[0044] 于是，OEM（或其他第三方）可以为 AC 模块选择 3PK 以及 RSA 公钥。随后，为了区别这些密钥，RSA 公钥被称为主模块密钥，而 3PK 则被称为辅模块密钥。

[0045] 如框 134 所示，处理系统 20 随后可在 ROM 42 内存储 AACM 60，如图 1 所示。在图 1 的实施例中，处理单元 30 被配置用作自举处理器 (BSP)，而处理系统 20 则被配置成将 ROM 42 用作引导存储（即，非易失性存储，处理单元 30 在上电或重置时从其获取指令用以初始化并配置处理系统 20）。

[0046] 如框 136 所示，处理系统 20 随后将 3PK 72 保存入 TPM 44。例如，处理系统 20 可以在每次引导期间将 3PK 72 安全地安装入 TPM 44。可选地，OEM 可以在处理系统制造期间将 3PK 72 供给至 TPM 44 内。

[0047] 图 4 是图 1 的 AACM 60 的框图，其中示出了模块头部内的 RSA 公钥 76 和 RSA 签名 78、头部之后的擦除区、以及擦除区之后的用户区，该用户区在来自初步 AC 模块的用户代码和用户数据之后还带有附至模块末尾处或附近的加密的 3PK72A。另外，AC 模块可用独立字段构造，以便可能在该模块的头部内保持一加密的 3PK。

[0048] 于是，OEM 或执行系统配置的其他实体可以在 ROM 42 内安装密钥（例如，E3PK 72A）。此外，因为该密钥本身被加密，所以即使攻击者能够从 ROM 42 中提取该 E3PK 72A，攻击者仍然无法解密并使用 E3PK 72A。

[0049] 图 5 是根据本发明一个示例实施例用于建立处理单元和 TPM 之间受保护通信通道的过程的流程图。图 1 在总线 24 和芯片组 34 上使用了粗线以描绘如根据图 5 过程建立在处理单元 30 和 TPM 44 之间的这一安全通道的一个示例。该过程可根据诸如上述的过程，在带有 E3PK 72A 的 AACM 60 已被存储在 ROM 42 之后开始。

[0050] 更具体地，图 5 的过程可以响应于处理系统 20 正被开机或重置而开始，从而引起处理单元 30 内的微码检查 ROM 42 内的预定位置以判定 ROM 42 是否含有 AC 模块。如果找

Petitioner Samsung Ex-1004, 0692

到了 AC 模块，处理单元 30 就可以将 AC 模块载入处理单元 30 内受保护的内部 RAM。接收该 AC 模块的受保护的内部 RAM 也可被称为鉴别代码执行区 (ACEA)38。

[0051] 出于示例的目的，可以假设处理单元 30 在 ROM 42 内找到 AACM 60。如框 220 所示，处理单元 30 随后可以根据以上 LTPA 规范的摘录判定 AACM 60 是否可信。例如，处理单元 30 可以 (a) 计算 AACM 60 某些部分的散列，(b) 使用 RSA 公钥 76 来解密签名 78，以及 (c) 将解密的签名与散列相比较以判定 AACM 60 是否与 OEM 最初用相应的 RSA 私钥的签名相匹配。处理单元 30 还可以相对于有效公钥的预定列表来验证 RSA 公钥 76。例如，处理单元可以从 RSA 公钥 76 中导出散列值，并将该值与处理系统 20 内受保护存储中的有效散列值列表相比较。如果 RSA 公钥 76 验证良好，并且 AACM 60 的散列与解密的 RSA 签名匹配，处理单元 30 就可以推断 AACM 60 可信。

[0052] 如果处理单元 30 无法找出 AC 模块，或者如果处理单元 30 找出 AC 模块但判定其不可信，则如框 240 所示，处理单元 30 就把适当的差错消息记入日志。随后如框 250 所示，处理单元 30 检查处理系统 20 内的配置设置以判定处理系统 20 是否应被允许使用非 ACM 引导过程。如果非 ACM 引导被允许，则如框 252 所示，处理单元 30 就执行该非 ACM 引导。如果非 ACM 引导未被允许，则过程结束而不引导处理系统 20。

[0053] 再次参考框 220，如果处理单元 30 判定 AACM 60 可信，随后就如框 222 所示，处理单元 30 从 AACM 60 中提取 E3PK 72A。处理单元 30 例如可以在一个或多个处理器寄存器或其他内部存储中临时存储 E3PK 72A。

[0054] 如框 224 和 226 所示，处理单元 32 随后解密 E3PK 72A 并在处理单元 32 内的受保护存储中保存该结果 (即，3PK 72)。在图 1 的实施例中，该受保护的存储被实现为一个或多个寄存器，上述存储器 (a) 仅可由特权代码修改；(b) 无法由非特权代码读取、写入或调试；以及 (c) 无法由 ITP 访问。在此上下文中，特权代码是可以在处理器外部被携带的代码，但是在其由处理器运行之前要求特定的鉴别，随后在清洁环境中运行于处理器内，以使得特权代码的执行无法被恶意方观察或操纵。在图 1 的实施例中，处理单元 30 使用 PUK 70 来解密 E3PK 72A。

[0055] 如框 228 所示，处理单元 30 和 TPM 44 随后可使用 3PK 72 来创建用以保护处理单元 30 和 TPM 44 之间通信的会话密钥 (SK)74。随后如框 230 所示，处理单元 30 和 TPM 44 使用 SK 74 创建一受保护的通道。该受保护的通道穿过多条系统总线 24 以及芯片组 34 的零个或更多的组件。随后如框 232 所示，TPM 44 和处理单元 30 使用 SK 74 加密通信。在可选实施例中，可以使用多个会话密钥来保护处理单元 30 和 TPM 44 之间的通信。

[0056] 受保护的通道例如可用于将来自 TPM 44 的密钥或其他受保护的信息载入处理单元 30。同样地，受保护的通道可用于将来自处理单元 30 的密钥或其他敏感的信息载入 TPM 44。受保护的通道由此确保该通道的任何观察者都无法判定通信的内容，从而保护传输中的数据免受修改。此外，用于初始化该通道的过程可以鉴别终点以免于越权存取、免于重放和 TPM 交换攻击。

[0057] 鉴于在此描述并示出的原理和示例实施例，应该认识到，可以在不背离上述原理的情况下对所示的实施例的安排和细节做出修改。同样，虽然前述讨论关注了某些特定实施例，但是仍然可以构想其他配置。更具体地，即使在此使用了诸如“在一个实施例中”、“在另一个实施例中”之类的表达，但这些短语意味着一般参考实施例的可能性，而不旨在将本

Petitioner Samsung Ex-1004, 0693

发明限于某些特定的实施例配置。如此处所使用的，这些术语可以参考可并入其他实施例的相同或不同的实施例。

[0058] 类似地，虽然已关于以特定顺序执行的特定操作描述了示例过程，但是可以对这些过程应用各种修改以导出本发明的多个替换实施例。例如，替换实施例可以包括使用少于全部公开的操作的过程、使用附加操作的过程、使用顺序不同的相同操作的过程以及其中组合、细分或另外改变了在此公开的各个操作的过程。

[0059] 本发明的替换实施例还包括用于执行本发明的各操作的机器可访问介质编码指令。这些实施例还可被称为程序产品。这些机器可访问介质包括但不限于存储介质，诸如软盘、硬盘、CD-ROM、ROM 和 RAM；以及由机器或设备制造或形成的部分的其他可检测的装置。指令还可在分布式环境中使用并被本地和 / 或远程存储以供单或多处理器机器访问。

[0060] 应该理解，在此描述的硬件和软件组件表示合理自持以便各自都能被充分彼此独立地设计、构造或更新的功能元件。在替换实施例中，许多组件都可被实现为硬件、软件或硬件和软件的组合以提供在此描述并示出的功能。

[0061] 考虑到能从在此描述的示例实施例中轻易导出的各种有用的变化，该详细描述仅出于示意性的目的，而不应被理解为限制本发明的范围。因此，本发明所要求保护的是落入所附权利要求书的范围和精神内的全部实现以及这些实现的所有等效技术方案。

Petitioner Samsung Ex-1004, 0694

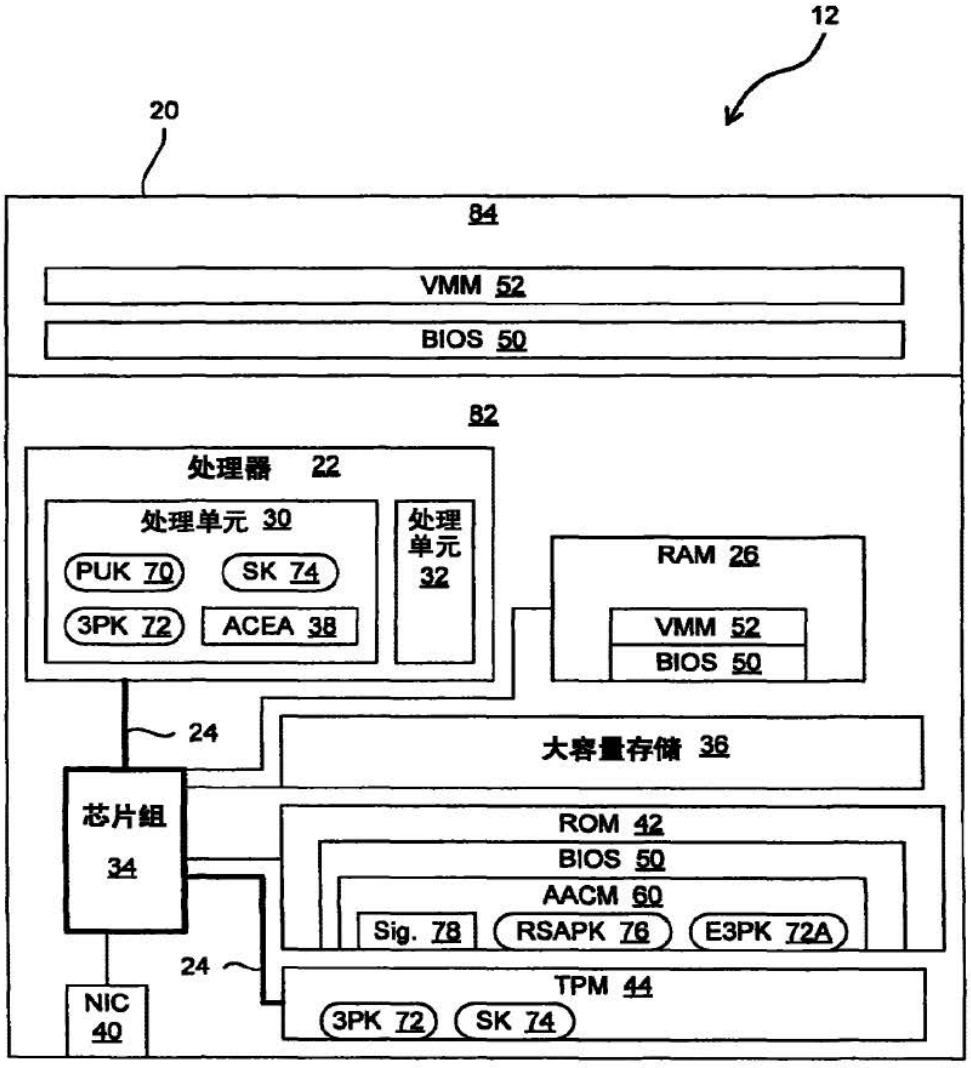


图 1

Petitioner Samsung Ex-1004, 0695

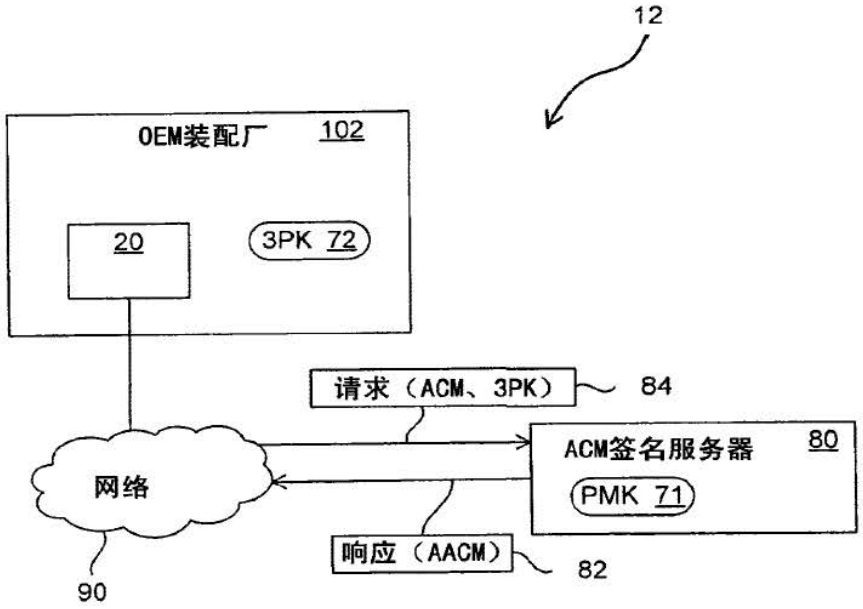


图 2

Petitioner Samsung Ex-1004, 0696

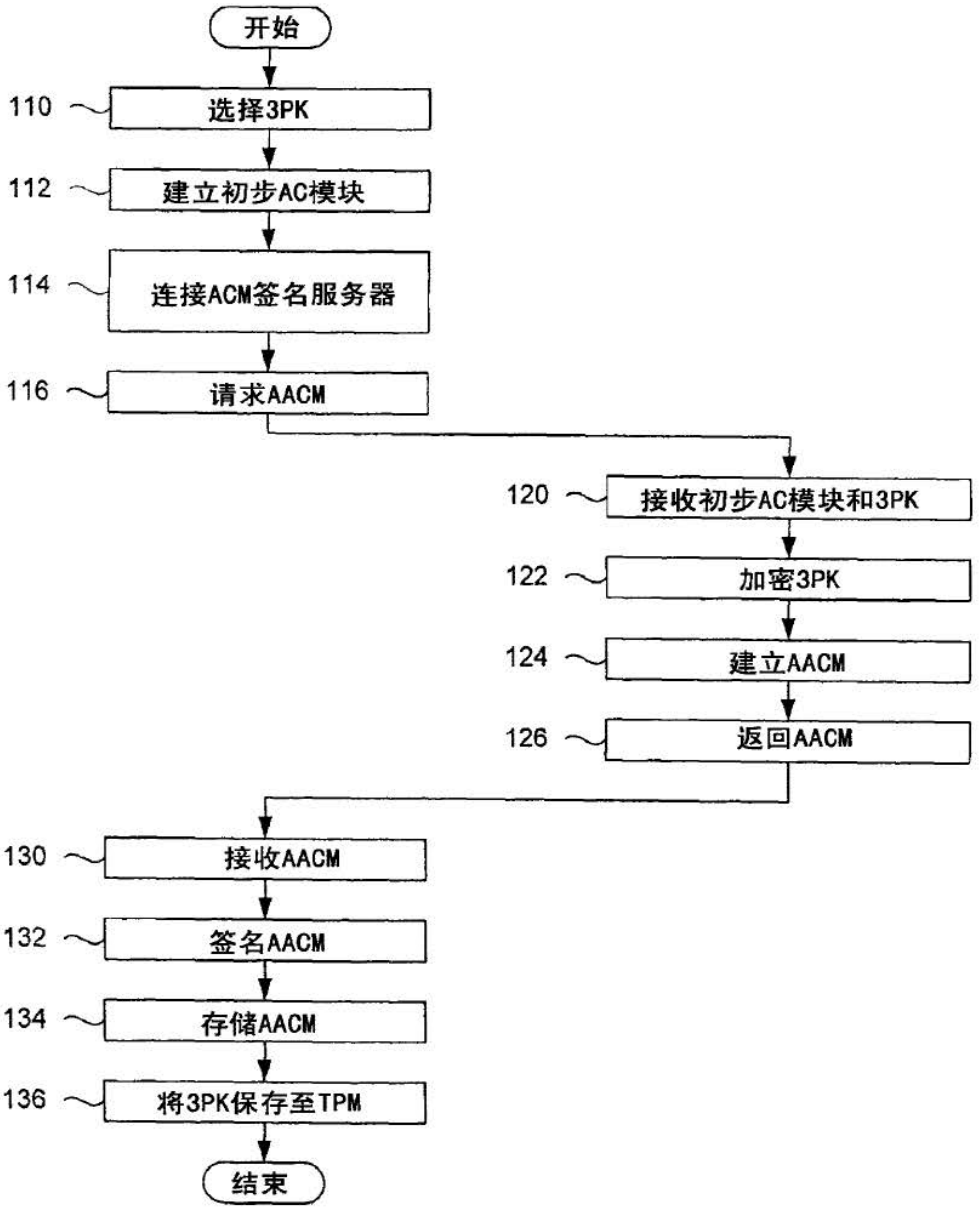


图 3

Petitioner Samsung Ex-1004, 0697

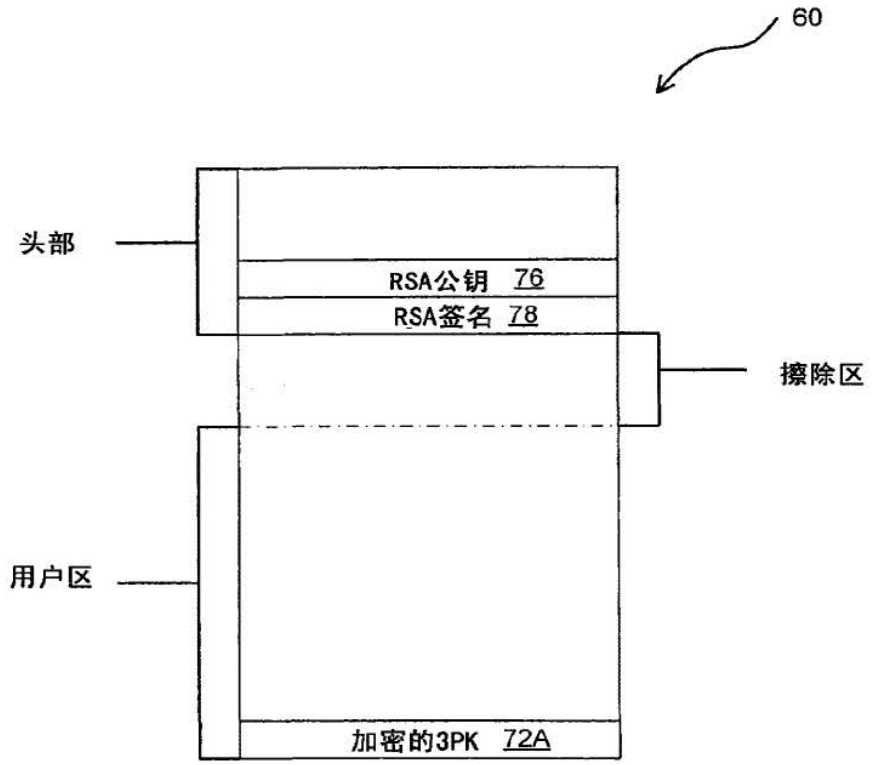


图 4

Petitioner Samsung Ex-1004, 0698

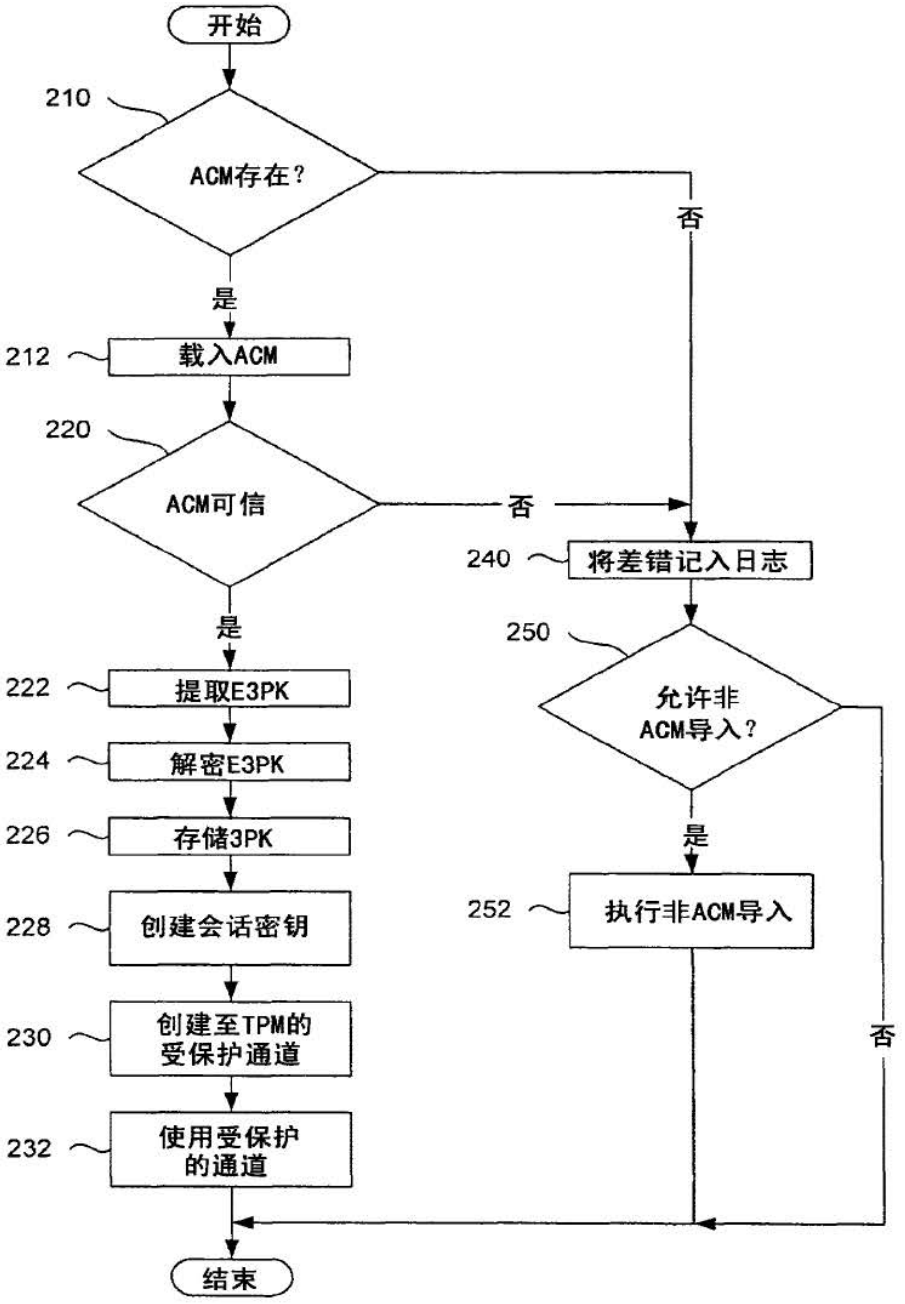


图 5

Petitioner Samsung Ex-1004, 0699

Electronic Acknowledgement Receipt

EFS ID:	29053437
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Glen Madison Kellett/Stacy Tebo
Filer Authorized By:	Glen Madison Kellett
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	27-APR-2017
Filing Date:	03-APR-2014
Time Stamp:	17:43:14
Application Type:	U.S. National Stage under 35 USC 371

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	Information Disclosure Statement (IDS) Form (SB08)	updated_IDS.pdf	1035039 cfb3c9216d77b6a7c9f908104819b97bccdc2339	no	4

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Foreign Reference	CN101251879B.PDF	856240 3a5d96e790b88ce5d941de75a0edf3ade5677 8a6	no	16
Warnings:					
Information:					
3	Non Patent Literature	P41624CN_OA2.pdf	281923 037f7205efdd5e91fec646fc015628e6b52c8c60	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	2173202		

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 06/09/2017

Barnes & Thornburg LLP (Intel)
11 S. Meridian Street
Indianapolis, IN 46204

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
06/09/2017	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Petitioner Samsung Ex-1004, 0702

Office Action Summary	Application No. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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 *04/24/2017*.

☐ 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) *48-71* 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) *48-71* 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 *01/19/2017 and 04/27/2017*.

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

4) ☐ Other: _____.

Petitioner Samsung Ex-1004, 0703

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 01/19/2017 and 04/27/2017 have been considered by the Examiner.

Status of Claims

3. This Office Action is issued in response to the Amendment filed on 04/24/2017.

Claims 1-47 are cancelled.

Claims 48-71 are pending in this Office Action.

Response to Arguments

4. Independent claim 48

Applicant states: “The Office Action indicated that the TPM 44 is the system-on-a-chip. However, contrary to the Office Action’s assertions, the TPM 44 does not comprise a security engine that has a secure memory that includes a security key that was encoded in the secure memory during a manufacturing process of the TPM 44 as recite in claim 48. Instead, Kumar discloses in col. 3, 11. 2-7 that “a processing unit key or PUK [of the processing unit 30, and not the TPM 44] is a cryptographic key that is

stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form."

It seems that the Office Action is asserting that the TPM 44 may be incorporated into the processing unit 30 and function as a single component. However, Kumar states in col. 8, 11. 49-59 that:

[Processing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44. Processing unit 30 and TPM 44 may then use SK 74 to create a protected channel, as shown at block 230. That protected channel may traverse multiple system buses 24 and zero or more components of chipset 34. TPM 44 and processing unit 30 may then use SK 74 to encrypt communications, as indicated at block 232. In alternative embodiments, multiple session keys may be used for protecting communications between processing unit 30 and TPM 44.

In other words, the processing unit 30 and the trusted platform module (TPM) 44 are separate components within the same processing system (i.e., within the same computer) that communicates with one another other. As such, the assertion that the processor 22 that includes the processing unit 30 "could also be a secure processor-TPM/system-on-a-chip-with" the processing unit 30 is not supported by Kumar. Accordingly, Kumar fails to disclose or teach at least "a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure

memory during a manufacturing process of the system-on-a-chip" as recited in claim 48."

In response, Kumar is brought in to show the obviousness of the limitation "a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory."

Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys, and the execution engine protects the sensitive information according to the security policies dictated by the TPM's control logic). Kumar also discloses "in a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM" and in Fig. 1, Processor 22 which has Proc. Unit 30-stores keys and Proc. Unit 32. Therefore, it is obvious to apply TPM to Processor 22 with Proc. Unit 32 as an execution engine and Proc. Unit 30 as secure nonvolatile (NV) memory or storage to protect data of Processor 22.

Applicant states: "Applicant respectfully submits that the Office Action's assertion that "it is obvious that PKU is also used to encrypt SK to protect SK from attacker" is

unsupported by Kumar. As quoted above, Kumar discloses in col. 8, lines 49-52 that "processing unit 30 and TPM 44 may then use 3PK 72 to create a session key (SK) 74 to be used for protecting communications between processing unit 30 and TPM 44." In other words, Kumar teaches that the session key (SK) 74 is created using the third party key (3PK) 72, and that the 3PK may be encrypted based on the PUK. See Kumar, col. 8, 11. 49-52 and col. 2, ln. 67 - col. 3, 11. 1. This is in contrast to encrypting a session key generated from a cryptographic key exchange, wherein the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture, in accordance with claim 48. As such, Kumar fails to disclose at least that feature of claim 48."

In response, Kumar teaches the concept of security key is encoded at the time of manufacture (Col. 3, lines 2-7: "a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form." Col. 3, lines 9-11: "The platform builder may also install the 3PK into the TPM of the platform during platform manufacturing."), the concept of encrypting key (Col. 7, lines 44-47: encrypted key is protected from attacker), and the concept of encryption using key that is encoded at the time of manufacture (Col. 6, lines 43-50: PKU is used to encrypt 3KP.) The combination of these concepts makes it obvious to have the encryption of the session key is performed using a security key that was encoded in the secure memory at the time of manufacture.

In conclusion, it is the combination of Kumar's teachings of TPM, key is encoded at the time of manufacture, and encryption using key that is encoded at the time of

manufacture that makes the limitation “a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory” obvious. Therefore, Applicant’s arguments regarding Kumar are not persuasive and previous 35 U.S.C. § 103 rejections are maintained.

Applicant’s arguments regarding independent claims 56, 64 and dependent claims 49-55, 57-63, and 65-71 are moot because they depend on Applicant’s arguments of claim 48 which is found non-persuasive.

Claim Rejections - 35 U.S.C. § 103

5. The following is a quotation of pre-AIA 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.

6. Claims 48-52, 56-61, 64-69 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter “Ali” and further in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar”.

Regarding claim 48, Chou discloses system-on-a-chip apparatus comprising:

[a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to]:

generate a random nonce for initiating a request for a secure communication session with a [remote] server over a network using the nonce (Fig. 1 and associated text: Client hello message 150 is sent from first network device-client- to second network device-server. Fig. 2A and associated text: Client hello message 150 includes first random number-random nonce. Col. 7, lines 22-23: “the first random number generated by the first network device”);

perform a cryptographic key exchange with the [remote] server (Fig. 1, step 180 and associated text: client key exchange message is sent to second network device-server);

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the [remote] server and decrypt messages received from the [remote] server during the secure communication session (Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120);

[encrypt the symmetric session key based on the security key]; and

store the encrypted session key in the [secure memory] (Chou does not explicitly disclose about storing the session key; however, in order for using the key to communicate between the two device in a period of time-a session of communication-, it is obvious that the key must be stored), [the system-on-a-chip] to establish the secure communication session with the remote server over the network using the session key (Col. 4, lines 60-63: Client Hello message 150 is a message that provides second network device 120 with information that is used to establish secured communications between network devices 110 and 120. Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120).

Chou does not explicitly disclose the secure communication session is with a ***remote*** server. However, generating session key for secure communication with a remote server is known in the art and Ali's teaching is an example (Paragraph [0039]: "Client applications on the Internet, such as standard web browsers, can connect to the web server on the smart card using HTTPS protocol. The TLS client side implementation allows the smart card to initiate a secure HTTPS connection to a remote web server on the Internet."

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou's invention of establishing a secure communication session with the server over the network using a session key with Ali's invention of secure communication session is with a remote server. The motivation to

do so would be enable secure communications end-to-end between the resource-constrained device and the remote node as taught by Ali (paragraph [0007]).

Chou and Ali do not explicitly disclose **a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key** and is stored **in the secure memory**.

However, in the field of protecting data, Kumar discloses a system-on-a-chip (Col. 1, lines 26-32: TPM is a system on a chip) comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key (Col. 1, lines 41-46: The sub-components of a TPM may include an execution engine and secure nonvolatile (NV) memory or storage. The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: It is obvious that Processor 22 could also be a secure processor-TPM/system-on-a chip-with Proc. Unit 30 is a secure nonvolatile and the Proc. Unit 30 is the execution engine. Col. 2, lines 17-19: In a platform with a TPM, platform measurements and encryption can be used to seal sensitive information or secrets to the TPM) that was encoded in the secure memory during a manufacturing process of the system-on-a-chip (Fig. 1: Proc. Unit 30 has PUK 70. Col. 3, lines 2-7: a processing unit key or PUK is a cryptographic key that is stored in a processor when the processor is manufactured, and that remains in the processor in nonvolatile form), the session key is encrypted

based on the security key and is stored in the secure memory (Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, it is obvious that PKU is also used to encrypt SK to protect SK from attacker.)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Ali's invention of establishing a secure communication session with the remote server over the network using a session key with a system on a chip that contains a secure memory to store session key and the session is encrypted using a key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip as taught by Kumar. The motivation to do so would be to protect data and to seal sensitive information or secrets to a secure area as taught by Kumar (Col. 1, line 8 and Col. 2, lines 17-19).

Regarding claim 49, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (Chou, Figs. 1, 2B and associated text: server hello message 160-response message- includes random number 260. Col. 4, lines 43-57: previously required and stored elements are used for second phase of authentication. It is obvious that server nonce is saved for using in second phase authentication. Combining with Kumar's teaching of secure memory as in claim 48 above, it is obvious

to have the server's nonce stored in the secure memory to protect the nonce from being compromised).

Regarding claim 50, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server (Chou, Col. 5, lines 50-61: first network device generates Pre-Master key. Pre-master key is encrypted with the public key of second network device and is sent to second network device-server. Kumar, Col. 3, lines 27-34: 3PKs are used to generate session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. The combination of Chou and Kumar's teaching makes it obvious that pre-master key is generated and encrypted using the security key of the security engine).

Regarding claim 51, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Kumar, Col. 1, lines 41-46: The secure NV memory is used to store sensitive information, such as encryption keys. Fig. 1: Proc. Unit 30 stores PUK, 3PK, and SK-session key. Col. 6, lines 43-50: PKU is used to encrypt 3KP. Col. 7, lines 44-47: encrypted key is protected from attacker. Therefore, the combination of Chou and Kumar's teachings make it

obvious that PKU is also used to encrypt pre-master key and store it in the secure memory to protect it from attacker.)

Regarding claim 52, Chou and Kumar disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine is further to:

generate the session key as a function of the pre-master key (Col. 5, lines 61-65: a master key is produced from the pre-master key); and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Claims 56-58 and 64-66 are rejected because they disclose similar subject matter to claims 48-50 respectively.

Claims 59 and 67 are rejected because they disclose similar subject matter to claim 48.

Claims 60-61 and 68-69 are rejected because they disclose similar subject matter to claim 52.

7. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (*http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf*), *hereinafter, "Stallings", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho"..*

Regarding claim 53, Chou, Ali, and Kumar disclose the system-on-a-chip apparatus of claim 48. Chou further discloses that client hello message includes list of cryptographic algorithms supported by first network device 110 such as Ephemeral Diffie-Hellman (DHE). Chou also discloses data is encrypted with server's public key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server).

Chou, Ali, and Kumar do not explicitly disclose wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie- Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

However, using Diffie-Hellman public and private keys in handshake process, signing and sending data are well-known in the art and Stallings' teaching is an example (page 540: "Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key.")

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of using Diffie-Hellman keys, signing and sending data. The motivation to do so would be to provide authentication.

Chou, Ali, Kumar and Stallings do not explicitly disclose that the security engine ***generate*** the Diffie-Hellman keys itself. However, generating Diffie-Hellman keys by sender is known in the art and Ho's teaching is an example ((Fig. 3, step 0a and associated text: a secret (private) key is chosen and a public key is computed. Paragraph [0038]: public key generated initiating device A-client- is used for Diffie-Hellman key exchange).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, Kumar and Stallings' inventions

of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information with using Diffie-Hellman keys, signing and sending data and with Ho's invention of generating Diffie-Hellman keys by sender. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Regarding claim 54, Chou, Ali, Kumar, Stallings and Ho disclose the system-on-a-chip apparatus of claim 53. Ho further discloses wherein the security engine to receive a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A) and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key (step 5a and associated text: DHkey-session key- is computed based on Private key of device A –client- and public key of Device B-server).

8. Claims 53, 54, 62, 63, 70, and 71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Asad Mahboob Ali (US Application No. 2006/0041938), hereinafter "Ali", in view of Kumar et al. (US Patent No. 8364975), hereinafter "Kumar", in view of William Stallings (http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf), hereinafter, "Stallings".

Regarding claim 55, Chou, Ali and Kumar disclose the system-on-a-chip apparatus of claim 48. Kumar also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou, Ali and Kumar do not explicitly disclose wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server.

However, receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server are well-known in the art and Stallings' teaching is an example (page 541: "Anonymous Diffie-Hellman: The message content consists of the two global Diffie-Hellman values (a prime number and a primitive root of that number) plus the server's public Diffie-Hellman key.")

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using

a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server. The motivation to do so would be to provide web security for client and server.

Regarding claim 63, Chou, Ali, and Kumar disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 9 above). Chou further disclose:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Chou, Ali, and Kumar do not explicitly disclose signing the hash code using a security key stored in a secure memory of the security engine and sending a client certificate verification message to the server, the client certificate verification message

including the signed hash code. However, signing hash code and sending a client certificate verification message are well-known in the art and Stallings' teaching is an example (page 540: "Ephemeral Diffie-Hellman: This technique is used to create ephemeral (temporary, one-time) secret keys. In this case, the Diffie-Hellman public keys are exchanged, signed using the sender's private RSA or DSS key. The receiver can use the corresponding public key to verify the signature. Certificates are used to authenticate the public keys. This would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key." Page 542: "the client may send a certificate_verify message to provide explicit verification of a client certificate… This message signs a hash code based on the preceding messages, defined as follows:

```
CertificateVerify.signature.md5_hash
MD5(master_secret || pad_2 || MD5(handshake_messages ||
master_secret || pad_1));
Certificate.signature.sha_hash
SHA(master_secret || pad_2 || SHA(handshake_messages ||
      master_secret || pad_1));)
```

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Ali, and Kumar's inventions of establishing a secure communication session with remote server over the network using a session key with a system on a chip that contains a secure memory to store sensitive information and with Stallings' invention of signing and sending signed data. The motivation to do so would be to provide authentication and to ensure secure communication for involved parties.

Claims 62 and 70 are rejected because they disclose similar subject matter to the combination of claims 53 and 54.

Claim 71 is rejected because it discloses similar subject matter to claim 63.

Conclusion

9. 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 THANH T. LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-Th 8:30 am- 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. 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.

/THANH T. LE/

Examiner, Art Unit 2495

/FARID HOMAYOUNMEHR/

Supervisory Patent Examiner, Art Unit 2495

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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-2004/0158715 A1	08-2004	Peyravian, Mohammad	H04L9/3013	713/171
*	B	US-2005/0213766 A1	09-2005	Goss, Steven C.	G06F21/72	380/277
*	C	US-2006/0041938 A1	02-2006	Ali; Asad Mahboob	G06Q20/341	726/14
*	D	US-2006/0117177 A1	06-2006	Buer; Mark L.	G06F21/606	713/155
*	E	US-7,382,882 B1	06-2008	Immonen; Olli	H04L63/0428	380/247
*	F	US-2010/0042824 A1	02-2010	Lee; Ruby B.	G06F21/6218	713/2
*	G	US-2010/0042839 A1	02-2010	Ho; Jin-Meng	H04L9/3226	713/169
*	H	US-7,966,646 B2	06-2011	Chou; Randy	H04L63/166	726/2
*	I	US-2011/0302638 A1	12-2011	Cha; Inhyok	G06F21/57	726/6
*	J	US-2012/0137126 A1	05-2012	MATSUOKA; Kazunari	H04L9/0838	713/156
*	K	US-8,364,975 B2	01-2013	Kumar; Mohan J.	G06F21/57	380/277
*	L	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
*	M	US-9,317,708 B2	04-2016	Lee; Ruby B.	G06F21/6218	1/1

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.

Petitioner Samsung Ex-1004, 0723

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/T.T.L/	1	101251879	CN	B	2010-10-13	Intel Corporation		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0724

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

/T.T.L/	Chinese Office Action for Patent Application No. 201180075550.4, dated March 6, 2017,	

If you wish to add additional non-patent literature document citation information please click the Add button [Add]

EXAMINER SIGNATURE

Examiner Signature	/THANH T LE/	Date Considered	05/30/2017

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2017-04-27
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0726

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 record s.

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.

Petitioner Samsung Ex-1004, 0727

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2014-04-03
First Named Inventor	Hormuzd M. Khosravi
Art Unit	2495
Examiner Name	LE, THANH T.
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.T.L/	1	20040158715	A1	2004-08-12	Peyravian et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/T.T.L/	1	201008309	TW	A	2010-02-16	Silver Spring Networks Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Samsung Ex-1004, 0728

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

/T.T.L/	1	Office Action, Search Report, and English Translation of R.O.C. Patent Application No. 101147511, dated October 24, 2016, 11 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/THANH T. LE/	Date Considered	05/30/2017

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13997412
	Filing Date	2014-04-03
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	2495
	Examiner Name	LE, THANH T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the 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 the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/GLEN M. KELLETT/	Date (YYYY-MM-DD)	2017-01-19
Name/Print	GLEN M. KELLETT	Registration Number	60202

This collection of information is required by 37 CFR 1.97 and 1.98. 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 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Petitioner Samsung Ex-1004, 0730

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 record s.

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.

Petitioner Samsung Ex-1004, 0731

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016	01/11/2017	05/31/2017					
	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	-	-	-	-					

Petitioner Samsung Ex-1004, 0732

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

✓	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	11/05/2015	04/29/2016	01/11/2017	05/31/2017					
	37	-	-	-	-					
	38	-	-	-	-					
	39	-	-	-	-					
	40	-	-	-	-					
	41	-	-	-	-					
	42	-	-	-	-					
	43	-	-	-	-					
	44	-	-	-	-					
	45	-	-	-	-					
	46	-	-	-	-					
	47	-	-	-	-					
	48	✓	✓	✓	✓					
	49	✓	✓	✓	✓					
	50	✓	✓	✓	✓					
	51	✓	✓	✓	✓					
	52	✓	✓	✓	✓					
	53	✓	✓	✓	✓					
	54	✓	✓	✓	✓					
	55	✓	✓	✓	✓					
	56	✓	✓	✓	✓					
	57	✓	✓	✓	✓					
	58	✓	✓	✓	✓					
	59	✓	✓	✓	✓					
	60	✓	✓	✓	✓					
	61	✓	✓	✓	✓					
	62	✓	✓	✓	✓					
	63	✓	✓	✓	✓					
	64	✓	✓	✓	✓					
	65	✓	✓	✓	✓					
	66	✓	✓	✓	✓					
	67	✓	✓	✓	✓					
	68	✓	✓	✓	✓					
	69	✓	✓	✓	✓					
	70	✓	✓	✓	✓					
	71	✓	✓	✓	✓					

Petitioner Samsung Ex-1004, 0733

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S109	6	(("20050213766") or ("20080159541") or ("20050213768")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/30 13:29
S110	309	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory) and (key with manufactur$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 18:54
S111	146	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory) and (key with manufactur$3) and ((key with exchang$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 18:55
S112	39	(US-20050005093-$ or US-20100205443-$ or US-20060041938-$ or US-20100042839-$ or US-20050213766-$ or US-20110235806-$ or US-20140270166-$ or US-20110231923-$ or US-20040158715-$ or US-20080244267-$ or US-20120257757-$ or US-20110161370-$ or US-20090235090-$ or US-20060174110-$ or US-20120137126-$ or US-20110302638-$ or US-20060117177-$ or US-20100042824-$).did. or (US-8627440-$ or US-7966646-$ or US-5657390-$ or US-7096352-$ or US-6449720-$ or US-8571221-$ or US-8549297-$ or US-8364975-$ or US-8296581-$ or US-7366306-$ or US-6385597-$ or US-9317708-$ or US-7382882-$ or US-7987356-$).did. or (US-20050005093-$ or US-20100042839-$ or US-20050213766-$ or US-20110113244-$ or US-20100299525-$ or US-20100100953-$ or US-20140270166-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2017/05/31 18:55
S113	143	S111 not S112	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 18:56

Petitioner Samsung Ex-1004, 0734

S114	0	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) same (key with secure with memory) same (key with manufactur$3) same ((key with exchang$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 18:56
S115	21	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (key with secure with memory with key with manufactur$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 18:58
S116	221	(@pd<"20111215" @ad<"20111215") and (key with secure with memory with key with manufactur$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 19:25
S117	27	(@pd<"20111215" @ad<"20111215") and (key with (secure adj memory) with (key near3 manufactur$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/31 19:26

EAST Search History (Interference)

< This search history is empty>

5/ 31/ 2017 10:04:25 PM
C:\ Users\ tle22\ Documents\ EAST\ Workspaces\ 13997412.wsp

Petitioner Samsung Ex-1004, 0735

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

CPC- SEARCHED		
Symbol	Date	Examiner
H04L9/0838 H04L9/0841 H04L9/0861 with text	8/14/2015	T.L

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and assignee search with text	8/14/2015	T.L
Interference search with text	8/14/2015	T.L
International and foreign search	8/14/2015	T.L
713/171 with text	8/14/2015	T.L
text based search of claim keywords and synonyms	8/14/2015	T.L
NPL search in IP.com	8/14/2015	T.L
Update Search	4/27/2016	T.L
Update search	1/4/2017	T.L
Update search	5/31/2017	T.L

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

Petitioner Samsung Ex-1004, 0736

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
P41624US/45631-225521	13/997,412	April 3, 2014
First Named Inventor:	**Title:**	
Hormuzd M. Khosravi	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
   - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
   - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
     - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
     - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
       - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
       - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/Scott Rylan Powell/	July 26, 2017
Name (Print/Typed) Scott Rylan Powell	**Practitioner Registration No.** 58378

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☐ * Total of 1 forms are submitted.

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.

BARNES & THORNBURG LLP
11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	2495
Examiner:	Le, Thanh T.
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	April 3, 2014
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

July 26, 2017

RESPONSE TO FINAL OFFICE ACTION

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

In response to the Final Office Action dated June 9, 2017, and contemporaneously with the filing of a request under the After Final Consideration Program ("AFCP 2.0"), please consider the following:

Listing of the Claims, which begin on page **2**; and

Remarks, which begin on page **9**.

AMENDMENTS TO THE CLAIMS

1-47. (Canceled)

48. (Currently Amended) A system-on-a-chip apparatus comprising:

a system-on-a-chip comprising a security engine that is separate from a processor core of the system-on-a-chip and has ~~having~~ a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to:

generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce;

perform a cryptographic key exchange with the remote server;

generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the symmetric session key based on the security key; and

store the encrypted session key in the secure memory,

the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key.

49. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the remote server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory.

50. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using the security key of the security engine, and send the encrypted pre-master key to the remote server.

Petitioner Samsung Ex-1004, 0740

51. (Previously Presented) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure memory.

52. (Previously Presented) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to:

generate the session key as a function of the pre-master key; and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

53. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using the security key of the security engine, and send the signed public Diffie-Hellman key to the remote server.

54. (Previously Presented) The system-on-a-chip apparatus of claim 53, wherein the security engine is further to receive a public Diffie-Hellman server key from the remote server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

55. (Previously Presented) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the remote server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure memory.

Petitioner Samsung Ex-1004, 0741

56. (Currently Amended) A method comprising:

generating a random nonce in a security engine that is separate from a processor core of a system-on-a-chip of a client device;

initiating, using the client device, a request for a secure communication session with a remote server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server;

generate a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypting the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

storing the encrypted session key in the secure memory of the security engine of the system-on-a-chip; and

establishing, using the client device, the secure communication session with the remote server using the session key.

57. (Previously Presented) The method of claim 56, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the remote server; and further comprising:

receiving a ServerHello message from the remote server, the ServerHello message including a server nonce; and

storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

58. (Previously Presented) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating a pre-master key in the security engine;

encrypting the pre-master key using the security key of the security engine; and

sending the encrypted pre-master key to the remote server.

Petitioner Samsung Ex-1004, 0742

59. (Previously Presented) The method of claim 58, further comprising:

wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and

storing the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

60. (Previously Presented) The method of claim 58, wherein performing the cryptographic key exchange with the remote server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

61. (Previously Presented) The method of claim 60, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

62. (Previously Presented) The method of claim 56, wherein performing the cryptographic key exchange with the remote server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

signing the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

sending the signed public Diffie-Hellman key to the remote server;

receiving a public Diffie-Hellman server key from the remote server; and

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

Petitioner Samsung Ex-1004, 0743

63. (Previously Presented) The method of claim 56, further comprising:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the remote server;

signing the hash code using the security key stored in the secure memory of the security engine; and

sending a client certificate verification message to the remote server, the client certificate verification message including the signed hash code.

64. (Currently Amended) One or more non-transitory machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to:

generate a random nonce in a security engine that is separate from a processor core of a system-on-a-chip of the computing device;

initiate a request for a secure communication session with a remote server over a network, the request including the random nonce;

perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server;

generate, based on the cryptographic key exchange, a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

encrypt the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

store the session key in the secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the remote server using the session key.

65. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to initiate a request for a secure communication session comprises to send a ClientHello message, including the nonce, to the remote server; and

Petitioner Samsung Ex-1004, 0744

wherein the plurality of instructions further cause the computing device to:

receive a ServerHello message from the remote server, the ServerHello message including a server nonce; and

store the server nonce in the secure memory of the security engine of the system-on-a-chip.

66. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate a pre-master key in the security engine;

encrypt the pre-master key using the security key of the security engine; and

send the encrypted pre-master key to the remote server.

67. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 66, wherein the plurality of instructions further cause the computing device to:

wrap the pre-master key in the security engine of the system-on-a-chip with a server public key, and

store the wrapped pre-master key in the secure memory of the security engine of the system-on-a-chip.

68. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the remote server comprises to generate the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

Petitioner Samsung Ex-1004, 0745

69. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 68, wherein to generate the session key in the security engine comprises to calculate, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the remote server.

70. (Previously Presented) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the remote server comprises to:

generate, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

sign the public Diffie-Hellman client key using the security key of the security engine of the system-on-a-chip;

send the signed public Diffie-Hellman key to the remote server;

receive a public Diffie-Hellman server key from the remote server; and

generate, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

71. (Canceled)

72. (New) The system-on-a-chip apparatus of claim 48, wherein the security engine is communicatively coupled to the processor core through an interconnect of the system-on-a-chip.

Petitioner Samsung Ex-1004, 0746

REMARKS

Applicant thanks the Examiner for consideration of the present application. Applicant has carefully reviewed the Final Office Action dated June 9, 2017 (hereinafter "the Office Action"). Claims 48-71 stand rejected. In this amendment, claims 48, 56, 64 have been amended, claim 71 has been canceled, and claim 72 is new. Applicant respectfully requests reconsideration of the present application in light of the remarks presented below.

I. 35 U.S.C. § 103 REJECTIONS

Each of claims 48-52, 56-61, and 64-69 stands rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 7,966,646 of Chou et al. (hereinafter "Chou") in view of U.S. Patent Application No. 2006/0041938 of Asad Mahboob Ali (hereinafter "Ali") and further in view of U.S. Patent No. 8,364,975 of Kumar et al. (hereinafter "Kumar"). Further, each of claims 53, 54, 62, 63, 70, and 71 stands rejected under 35 U.S.C. § 103 as being unpatentable over Chou in view of Ali and Kumar and in view of "Stallings Cryptography and Network Security" by William Stallings (herein after "Stallings") and further in view of U.S. Patent Application No. 2010/0042839 of Ho (hereinafter "Ho"). Additionally, claim 55 stands rejected under Chou in view of Ali, Kumar, and Stallings. It is well settled that the analysis required under 35 U.S.C. § 103(a) must be resolved on the basis of the factual inquiries outlined in *Graham v. John Deere, Co.*, 383 U.S. 1, 148 USPQ 459 (1966); *see KSR v. Teleflex*, 127 S.Ct. at 1740. The *Graham* Court stated that as part of any analysis under Section 103,

> the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

148 USPQ at 467. The analysis of obviousness therefore requires an inquiry into the scope and content of the prior art and, more particularly, an inquiry into whether the prior art discloses all of the elements of the claimed invention.

A. Independent Claim 48

In support of the 35 U.S.C. § 103 rejection of independent claim 48, the Office Action asserts that a combination of Chou, Ali, and Kumar describes or suggests every feature of independent claim 48. Applicant disagrees. However, solely in the interest of expediting

Petitioner Samsung Ex-1004, 0747

prosecution, Applicant has amended claim 48 to clarify that the security engine that performs the steps of the method (e.g., generating a random nonce, performing a cryptographic key exchange, generating a symmetric session key, etc.) is *separate* from a processor core of the system-on-a-chip. In particular, claim 48 has been amended to recite: "a system-on-a-chip comprising a security engine that is separate from a processor core of the system-on-a-chip and has a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to . . . generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce . . . perform a cryptographic key exchange with the remote server . . . generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session . . . encrypt the symmetric session key based on the security key . . . store the encrypted session key in the secure memory . . . the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key."

This feature is described in paragraph [0014] of the present application, which is reproduced below:

> The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes the security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

Petitioner Samsung Ex-1004, 0748

By contrast, the Office Action, on page 9, cited a general purpose processor 22 in Kumar as allegedly being a security engine. As such, the art of record does not teach a security engine that is *separate* from a processor core of a system on a chip.

Furthermore, and with reference to page 10 of the Office Action, Applicant respectfully submits that Kumar does not disclose a security engine encrypting a session key that was generated from a key exchange with a remote server. Rather, Kumar discloses an AACM Generator 80, which is a remote system used in the assembly of the processor 22, that encrypts a third party key (3PK) that is later stored in the memory of the processor 22.

Chou and Ali do not cure these deficiencies of Kumar. Indeed, the Office Action acknowledged on page 9 that Chou and Ali do not disclose:

> a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the session key is encrypted based on the security key and is stored in the secure memory.

For at least the reasons discussed above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar does not render claim 48 obvious and Applicant respectfully requests withdrawal of the Section 103 rejection of claim 48.

B. Independent Claim 56

The Office Action also rejected claim 56 under Section 103 as being rendered obvious by Chou, Ali, and Kumar, using similar rational as set forth in the rejection of claim 48. Solely in the interest of expediting prosecution, Applicant has amended claim 56 in a manner similar to claim 48. In particular, claim 48 has been amended to recite: "generating a random nonce in a security engine that is separate from a processor core of a system-on-a-chip of a client device . . . initiating, using the client device, a request for a secure communication session with a remote server over a network, the request including the random nonce . . . performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server . . . generate a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session . . . encrypting the session key based on a security key that was encoded in a secure memory of the

Petitioner Samsung Ex-1004, 0749

security engine during a manufacturing process of the system-on-a-chip . . . storing the encrypted session key in the secure memory of the security engine of the system-on-a-chip . . . establishing, using the client device, the secure communication session with the remote server using the session key."

As such, all of the arguments presented above in regard to the rejection of independent claim 48 apply with equal force to the rejection of independent claim 56 and are incorporated into this section by reference. Accordingly, for at least the reasons provided above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar fails to disclose every feature of amended independent claim 56. As such, that proposed combination fails to render independent claim 56 obvious. Applicant, therefore, respectfully submits that independent claim 56 is in condition for allowance and such action is respectfully requested.

C. Independent Claim 64

The Office Action also rejected claim 64 under Section 103 as being rendered obvious by Chou, Ali, and Kumar, using similar rational as set forth in the rejection of claim 48. Applicant respectfully disagrees. However, solely in the interest of expediting prosecution, Applicant has amended claim 64 in a manner similar to claim 48. In particular, Applicant has amended claim 64 to recite: "One or more non-transitory machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to . . . generate a random nonce in a security engine that is separate from a processor core of a system-on-a-chip of the computing device . . . initiate a request for a secure communication session with a remote server over a network, the request including the random nonce . . . perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the remote server . . . generate, based on the cryptographic key exchange, a symmetric session key to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session . . . encrypt the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip . . . store the session key in the secure memory of the security engine of the system-on-a-chip . . . establish the secure communication session with the remote server using the session key."

Petitioner Samsung Ex-1004, 0750

Accordingly, all of the arguments presented above in regard to the rejection of independent claim 48 apply with equal force to the rejection of independent claim 64 and are incorporated into this section by reference. For at least the reasons provided above, Applicant respectfully submits that the proposed combination of Chou, Ali, and Kumar fails to disclose every feature of amended independent claim 64. As such, that proposed combination fails to render independent claim 64 obvious. Applicant, therefore, respectfully submits that independent claim 64 is in condition for allowance and such action is respectfully requested.

D. Dependent Claims 49-55, 57-63, and 65-71

Each of claims 49-55 includes independent claim 48 as a base claim; each of claims 57-63 includes independent claim 56 as a base claim; and each of clams 65-70 includes independent claim 64 as a base claim. Claim 71 has been canceled. Stallings and Ho do not cure the deficiencies of Chou, Ali, and Kumar with respect to independent claims 48, 56, and 64. Accordingly, Applicant respectfully requests withdrawal of the Section 103 rejection of claims 49-55, 57-63, and 65-70. Any arguments specific to claims 49-55, 57-63, and 65-70 are held in abeyance without prejudice or admission to any assertion made in the Office Action in order to expedite prosecution.

II. NEW CLAIM

Claim 72 is new and is supported by the present application at least at paragraph [0013]. Further, claim 72 depends from and thereby incorporates the features of claim 48, which has been shown to be patentable. As such, Applicant submits that claim 72 likewise is patentable.

III. CONCLUSION

In view of the foregoing, it is submitted that this application is in a condition for allowance. Action to that end is hereby solicited. If there are any questions or comments that would expedite prosecution of this application, the Examiner is invited to call the undersigned at (317) 231-7307.

Petitioner Samsung Ex-1004, 0751

It is respectfully requested that, if necessary to effect a timely response, this paper be considered as a Petition for an Extension of Time sufficient to effect a timely response. The Commissioner is hereby authorized to charge the fee for such Petition, if needed, and any shortage of fees, and credit any overpayment of fees, to the Account of Barnes & Thornburg, Deposit Account No. 10-0435 with reference to file P41624US/45631-225521.

Respectfully submitted,

/Scott R Powell/

Scott R. Powell
Registration No. 58,378
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-7307

DMS 4950792v1

Petitioner Samsung Ex-1004, 0752

Electronic Acknowledgement Receipt

EFS ID:	29892934
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/kim tyree
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	26-JUL-2017
Filing Date:	03-APR-2014
Time Stamp:	12:08:53
Application Type:	U.S. National Stage under 35 USC 371

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	After Final Consideration Program Request	P41624US_AFCP.pdf	226486 b94d30d00077c00266a379194a9e69f0193 4a1ef	no	2

Warnings:

Information:					
2	Response After Final Action	P41624US_RFOA.pdf	93242 a38839b0ecf704dc2f2a9299eeedcf625b329e01	no	14
Warnings:					
Information:					
			Total Files Size (in bytes):	319728	

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/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 13/997,412	Filing Date 04/03/2014	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	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	07/26/2017	(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))	* 24	Minus	** 24	= 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
JAMES MASON

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.

Petitioner Samsung Ex-1004, 0755

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 08/11/2017

Barnes & Thornburg LLP (Intel)
11 S. Meridian Street
Indianapolis, IN 46204

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
08/11/2017	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):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Petitioner Samsung Ex-1004, 0756

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *13/997,412*	**Applicant(s)** KHOSRAVI ET AL.	
	Examiner THANH T. LE	**Art Unit** 2495	**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 26 July 2017 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 _____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): _____.
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: _____.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☒ Other: PTO 2323 is attached.

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: 48-70, 72.
    Claim(s) withdrawn from consideration: .

/Jason K. Gee/ Primary Examiner AU 2495	/THANH T LE/ Examiner, Art Unit 2495

Petitioner Samsung Ex-1004, 0757

Continuation of 12: Applicant's request for AFCP 2.0 is acknowledged. However, the request is denied because the amended limitations cannot be reviewed and updated search cannot be conducted in the limited amount of time authorized for this pilot program. Therefore, the response is being reviewed under pre-pilot practice.
The request for reconsideration has been considered, but does not place the application in condition for allowance because amended limitations would require further consideration and/or search.

Petitioner Samsung Ex-1004, 0758

AFCP 2.0 Decision	Application No.	Applicant(s)
	13/997,412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T. LE	2495

This is in response to the After Final Consideration Pilot request filed 26 July 2017.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.

   ☐ Other:

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☒ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action. See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☐ 5. Other:

   Examiner Note: Please attach an interview summary when necessary as described above.

Petitioner Samsung Ex-1004, 0759

DO NOT ENTER: /T.T.L/

08/04/2017

Doc Code: A.NE.AFCP

Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
P41624US/45631-225521	13/997,412	April 3, 2014

First Named Inventor:	Title:
Hormuzd M. Khosravi	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
    - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
    - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
        - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
        - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
            - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
            - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/Scott Rylan Powell/	July 26, 2017
Name (Print/Typed) Scott Rylan Powell	Practitioner Registration No. 58378

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☐ * Total of 1 forms are submitted.

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.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
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.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13997412	Filing Date	2014-04-03	Docket Number (if applicable)	P41624US/45631-225521	Art Unit	2495
First Named Inventor	Hormuzd M. Khosravi			Examiner Name	LE, THANH T.		

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, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

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).

☒ 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.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other Response to Final Office Action filed July 26, 2017

☐ Enclosed

- ☐ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ 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)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 100435

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

EFS - Web 2.1.15

PTO/SB/30EFS (07-14)
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.

Signature of Registered U.S. Patent Practitioner			
Signature	/Scott R. Powell/	Date (YYYY-MM-DD)	2017-09-11
Name	Scott R. Powell	Registration Number	58378

This collection of information is required by 37 CFR 1.114. 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.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Petitioner Samsung Ex-1004, 0763

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.

Petitioner Samsung Ex-1004, 0764

Electronic Patent Application Fee Transmittal

Application Number:	13997412
Filing Date:	03-Apr-2014
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Filer:	Scott Rylan Powell/kim tyree
Attorney Docket Number:	P41624US/45631-225521

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

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($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1700	1700
		Total in USD ($)		**1700**

Electronic Acknowledgement Receipt

EFS ID:	30318784
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/kim tyree
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	11-SEP-2017
Filing Date:	03-APR-2014
Time Stamp:	10:59:05
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1700
RAM confirmation Number	091117INTEFSW00010494100435
Deposit Account	100435
Authorized User	kim tyree
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.492 (National application filing, search, and examination fees)

37 CFR 1.492(a) (Basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	P41624US_RCE2.pdf	1349924 be42acb2926a6772085060e33aae53c4fca71a0e	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31198 1f221d9daa0c44b1a112ce13ff8f3716cc5cb8f6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1381122		

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/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 13/997,412	Filing Date 04/03/2014	☐ 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 **09/11/2017**

	(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))	* 24	Minus	** 24	= 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.

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

73486 7590 09/29/2017
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

EXAMINER
LE, THANH T

ART UNIT	PAPER NUMBER
2495	

DATE MAILED: 09/29/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

TITLE OF INVENTION: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

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	12/29/2017

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.

Petitioner Samsung Ex-1004, 0770

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)

73486 7590 09/29/2017
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

TITLE OF INVENTION: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

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	12/29/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THANH T	2495	713-171000

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

Petitioner Samsung Ex-1004, 0771

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

73486 7590 09/29/2017

Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

EXAMINER	
LE, THANH T	

ART UNIT	PAPER NUMBER
2495	

DATE MAILED: 09/29/2017

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.

Petitioner Samsung Ex-1004, 0772

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. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	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 *7/26/2017*.
   ☐ 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 *48-70 and 72*. 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 _____
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 _____.

/THANH T LE/
Examiner, Art Unit 2495

Petitioner Samsung Ex-1004, 0774

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Reasons for Allowance

2. Claims 48-70 and 72 are allowed.

The following is an Examiner's statement of Reasons for Allowance:

Applicant's arguments/amendments submitted on 07/26/2017 have been considered and are persuasive in light of the arguments and claim amendments. Also, please see prior Office actions. Therefore, the previously filed claim rejections have been withdrawn. The record is clear; therefore, no reason for allowance is necessary.

According to MPEP 1302.14 (I): "In most cases, the Examiner's actions and the applicant's replies make evident the reasons for allowance, satisfying the "record as a whole" provisio of the rule. This is particularly true when applicant fully complies with 37 CFR 1.111 (b) and (c) and 37 CFR 1.133(b). Thus, when the Examiner's actions clearly point out the reasons for rejection and the applicant's reply explicitly presents reasons why claims are patentable over the reference, the reasons for allowance are in all probability evident from the record and no statement should be necessary."

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."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH T. LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-Th 9:00 am- 2:00 pm and alt Fri 9 am- 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. 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.

/THANH T. LE/

Examiner, Art Unit 2495

/FARID HOMAYOUNMEHR/

Supervisory Patent Examiner, Art Unit 2495

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,657,390 A	08-1997	Elgamal; Taher	H04L29/06	713/151
*	B	US-6,385,597 B1	05-2002	Guenther; Stephan	G06K13/0825	705/402
*	C	US-6,449,720 B1	09-2002	Sprague; Steven K	G06F21/602	380/255
*	D	US-2004/0158715 A1	08-2004	Peyravian, Mohammad	H04L9/0844	713/171
*	E	US-2005/0005093 A1	01-2005	Bartels, Andrew	G06F21/606	713/150
*	F	US-2005/0213766 A1	09-2005	Goss, Steven C.	G06F21/72	380/277
*	G	US-2006/0041938 A1	02-2006	Ali; Asad Mahboob	G06Q20/341	726/14
*	H	US-2006/0117177 A1	06-2006	Buer; Mark L.	G06F21/606	713/155
*	I	US-2006/0174110 A1	08-2006	Strom; Clifford P.	G06F21/10	713/165
*	J	US-7,096,352 B2	08-2006	Kang; Kyoung Jin	H04L63/0428	380/270
*	K	US-7,356,671 B1	04-2008	Wei; David Dawei	G06F9/3851	712/35
*	L	US-7,366,306 B1	04-2008	Trimberger; Stephen M.	G06F12/1425	326/8
*	M	US-7,382,882 B1	06-2008	Immonen; Olli	H04L63/0428	380/247

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.

Petitioner Samsung Ex-1004, 0778

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0244267 A1	10-2008	Zimmer; Vincent J.	G06F21/572	713/171
*	B	US-2009/0235090 A1	09-2009	Chang; Chih-Chung	H04L9/0825	713/190
*	C	US-2010/0042839 A1	02-2010	Ho; Jin-Meng	H04L9/0841	713/169
*	D	US-2010/0042824 A1	02-2010	Lee; Ruby B.	G06F21/6218	713/2
*	E	US-2010/0205443 A1	08-2010	Zhao; Yunlei	H04L9/0841	713/171
*	F	US-7,966,646 B2	06-2011	Chou; Randy	H04L63/166	726/2
*	G	US-2011/0161370 A1	06-2011	Miyamae; Takeshi	G06F17/30067	707/783
*	H	US-2011/0235806 A1	09-2011	Fukuda; Naohiro	H04L9/0825	380/282
*	I	US-2011/0231923 A1	09-2011	Bollay; Benn Sapin	H04L63/166	726/9
*	J	US-2011/0289004 A1	11-2011	Prakash; Gyan	G06Q20/20	705/71
*	K	US-2011/0302638 A1	12-2011	Cha; Inhyok	G06F21/57	726/6
*	L	US-2012/0137126 A1	05-2012	MATSUOKA; Kazunari	H04L9/0838	713/156
*	M	US-8,296,581 B2	10-2012	Jennings; Gerard David	G06F9/3824	711/100

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	
	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.

Petitioner Samsung Ex-1004, 0779

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2012/0257757 A1	10-2012	Gessner; Jurgen	H04L63/061	380/282
*	B	US-8,364,975 B2	01-2013	Kumar; Mohan J.	G06F21/57	380/277
*	C	US-8,571,221 B2	10-2013	Little; Herbert A.	G06F21/72	380/255
*	D	US-8,549,297 B1	10-2013	Topham; Andrew	G06F21/80	380/278
*	E	US-8,627,440 B2	01-2014	Mowers; David R.	H04L63/0807	380/279
*	F	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
*	G	US-9,317,708 B2	04-2016	Lee; Ruby B.	G06F21/6218	1/1
	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	
	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.

Petitioner Samsung Ex-1004, 0780

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S126	76	(@pd<"20111215" @ad<"20111215") and (system$1on$1a$1chip SOC) and (processor near2 core) and (security adj (engine agent unit))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/18 12:00
S127	1	(@pd<"20111215" @ad<"20111215") and ((system$1on$1a$1chip SOC) with (processor near2 core) with (security adj (engine agent unit)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/18 12:06
S128	3	(@pd<"20111215" @ad<"20111215") and ((system$1on$1a$1chip SOC) same (processor near2 core) same (security adj (engine agent unit)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/18 12:08
S129	35	(@pd<"20111215" @ad<"20111215") and ((processor near2 core) with (security adj (engine agent unit)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/18 12:15
S130	34	S129 not S126	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/18 12:16

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S131	0	system$1on$1a$1chip with (security adj engine) with (security with memory) with (random adj nonce) with (cryptograph$3 near2 key near2 exchang$3) with (symmetric near2 session near2 key)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:52
S132	0	system$1on$1a$1chip with (security adj engine) with memory with (random adj nonce) with (cryptograph$3 near2 key near2 exchang$3) with (symmetric near2 session near2 key)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:53
S133	0	system$1on$1a$1chip with (security adj engine) with (security adj memory)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:54
S134	0	(security adj engine) with (security with memory) with (random adj nonce) with (cryptograph$3 near2 key near2 exchang$3) with (symmetric near2 session near2 key)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:54
S135	0	(security adj engine) with (security with memory) with (random adj nonce) with	US-PGPUB;	OR	ON	2017/09/21 09:54

Petitioner Samsung Ex-1004, 0781

		(cryptograph$3 near2 key near2 exchang$3)	USPAT			
S136	852	(security adj engine) with (security with memory)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:54
S137	1	(security adj engine) with (security with memory) with (cryptograph$3 near2 key near2 exchang$3)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:55
S138	1	(security adj engine) with (security with memory) with (cryptograph$3 near2 key near2 exchang$3).clm.	US-PGPUB; USPAT	OR	ON	2017/09/21 09:55
S139	110	((security adj engine) with (security with memory)).clm.	US-PGPUB; USPAT	OR	ON	2017/09/21 09:58
S140	6	((security adj engine) with (security with memory)).clm. and ((713/171).ccls. (H04L9/0838 H04L9/0841 H04L9/0861 H04L63/061).cpc.)	US-PGPUB; USPAT	OR	ON	2017/09/21 09:59

9/21/2017 10:00:50 AM
C:\Users\tle22\Documents\EAST\Workspaces\13997412.wsp

Petitioner Samsung Ex-1004, 0782

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	Art Unit
	THANH T LE	2495

CPC- SEARCHED		
Symbol	Date	Examiner
H04L9/0838 H04L9/0841 H04L9/0861 with text	8/14/2015	T.L

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
173	171	08/14/2015	T.L

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and assignee search with text	8/14/2015	T.L
Interference search with text	8/14/2015	T.L
International and foreign search	8/14/2015	T.L
713/171 with text	8/14/2015	T.L
text based search of claim keywords and synonyms	8/14/2015	T.L
NPL search in IP.com	8/14/2015	T.L
Update Search	4/27/2016	T.L
Update search	1/4/2017	T.L
Update search	5/31/2017	T.L
Update search	9/18/2017	T.L
Consult Farid Homayounmehr for allowance	9/20/2017	T.L
Update search	9/21/2017	T.L

INTERFERENCE SEARCH	

Petitioner Samsung Ex-1004, 0783

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
173	171	9/21/2017	T.L

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	**Art Unit**
	THANH T LE	2495

CPC						
Symbol					**Type**	**Version**
H04L		9	/	0838	F	2013-01-01
H04L		9	/	0841	I	2013-01-01
H04L		9	/	0861	I	2013-01-01
H04L		63	/	061	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

/THANH T LE/ Examiner.Art Unit 2495	9/21/2017	**Total Claims Allowed:**
(Assistant Examiner)	(Date)	24
/FARID HOMAYOUNMEHR/ Supervisory Patent Examiner, Art Unit 2495		O.G. Print Claim(s) / O.G. Print Figure
(Primary Examiner)	(Date)	1 / 1

Petitioner Samsung Ex-1004, 0785

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	**Art Unit**
	THANH T LE	2495

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION														
CLASS	SUBCLASS	CLAIMED						NON-CLAIMED								
713	171	H	0	4	L	9 / 0838										
CROSS REFERENCE(S)		H	0	4	L	9 / 0841										
		H	0	4	L	9 / 0861										
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)	H	0	4	L	63 / 061										

/THANH T LE/ Examiner.Art Unit 2495	9/21/2017	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	24	
/FARID HOMAYOUNMEHR/ Supervisory Patent Examiner, Art Unit 2495		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Petitioner Samsung Ex-1004, 0786

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13997412	KHOSRAVI ET AL.
	Examiner	**Art Unit**
	THANH T LE	2495

☐ 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	48	17	64												
2	49	18	65												
3	50	19	66												
4	51	20	67												
5	52	21	68												
6	53	22	69												
7	54	23	70												
8	55	-	71												
9	56	24	72												
10	57														
11	58														
12	59														
13	60														
14	61														
15	62														
16	63														

/THANH T LE/ Examiner.Art Unit 2495	9/21/2017	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	24	
/FARID HOMAYOUNMEHR/ Supervisory Patent Examiner, Art Unit 2495		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Petitioner Samsung Ex-1004, 0787

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. 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(c).

I hereby appoint:

☑ Practitioners associated with Customer Number: 73486

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 a ssigned only to the undersigned according to the USPTO assignment records or assignments docu ments attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☑ The address associated with Customer Number: 73486

OR

☐	Firm or Individual Name		
	Address		
	City		
	Country		
	Telephone		Email

Assignee Name and Address: INTEL CORPORATION
2200 MISSION COLLEGE BOULEVARD, SANTA CLARA, CA 95054

A copy of this form, together with a statement under 37 CFR 3.73(c) (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(c) may be completed by one of The practitioners appointed in this form, 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	Heather Adamson	Date	1/2/2013
Name	Heather Adamson	Telephone	503-613-0191
Title	Administrator of Patents		

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.

PTO/AIA/14 (03-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P41624US
	Application Number	13/997,412
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

⊗ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix
Intel Corporation				

Petitioner Samsung Ex-1004, 0789

PTO/AIA/14 (03-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P41624US
	Application Number	13/997,412
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

Mailing Address Information:			
Address 1	2200 Mission College Blvd.		
Address 2			
City	Santa Clara	**State/Province**	CA
Country i	US	Postal Code	95054
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section only if non-applicant assignee information is desired to be included on the patent application publication in accordance with 37 CFR 1.215(b). Do not include in this section an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest), as the patent application publication will include the name of the applicant(s).

Remove

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the Add button. Add

Petitioner Samsung Ex-1004, 0790

PTO/AIA/14 (03-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P41624US
	Application Number	13/997,412
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

2017-12-26

Signature	/Glen M. Kellett, Reg. No. 60202/ Scott Rylan Powell/			Date (YYYY-MM-DD)	2013-06-19
First Name	~~Glen M.~~ Scott	Last Name	~~Kellett~~ Powell	Registration Number	~~60202~~ 58378

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

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.

Petitioner Samsung Ex-1004, 0792

PTO/SB/47 (03-09)
Approved for use through 07/31/2018. OMB 0651-0016
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.

"FEE ADDRESS" INDICATION FORM

Address to:
Mail Stop M Correspondence
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

- OR -

Fax to:
571-273-6500

INSTRUCTIONS: The issue fee must have been paid for application(s) listed on this form. In addition, only an address represented by a Customer Number can be established as the fee address for maintenance fee purposes (hereafter, fee address). A fee address should be established when correspondence related to maintenance fees should be mailed to a different address than the correspondence address for the application. **When to check the first box below:** If you have a Customer Number to represent the fee address. **When to check the second box below:** If you have no Customer Number representing the desired fee address, in which case a completed Request for Customer Number (PTO/SB/125) must be attached to this form. For more information on Customer Numbers, see the Manual of Patent Examining Procedure (MPEP) § 403.

For the following listed application(s), please recognize as the "Fee Address" under the provisions of 37 CFR 1.363 the address associated with:

☒ Customer Number: 000197

OR

☐ The attached Request for Customer Number (PTO/SB/125) form.

PATENT NUMBER (if known)	APPLICATION NUMBER
	13/997,412

Completed by (check one):

☐ Applicant/Inventor

☒ Attorney or Agent of record 58378 (Reg. No.)

☐ Assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☐ Assignee recorded at Reel Frame

/Scott Rylan Powell/
Signature

Scott Rylan Powell
Typed or printed name

317-231-7307
Requester's telephone number

December 26, 2017
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more that one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.363. 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 5 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 COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Mail Stop M Correspondence, 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.

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: Hormuzd M. Khosravi et al.

Application No./Patent No.: 13/997,412 Filed/Issue Date: April 3, 2014

Titled: MEHTOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

Intel Corporation, 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: Hormuzd M. Khosravi and Edward C. Epp To: Intel Corporation

   The document was recorded in the United States Patent and Trademark Office at

   Reel 027820, Frame 0601, or for which a copy thereof is attached.

2. From: Farhana Kabir To: Intel Corporation

   The document was recorded in the United States Patent and Trademark Office at

   Reel 032595, Frame 0639, 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.

/Scott Rylan Powell/	December 26, 2017
Signature	Date
Scott Rylan Powell	58378
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.

Electronic Patent Application Fee Transmittal

Application Number:	13997412
Filing Date:	03-Apr-2014
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Filer:	Scott Rylan Powell/kim tyree
Attorney Docket Number:	P41624US/45631-225521

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

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**

Electronic Acknowledgement Receipt

EFS ID:	31334839
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/kim tyree
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	26-DEC-2017
Filing Date:	03-APR-2014
Time Stamp:	16:12:13
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$960
RAM confirmation Number	122717INTEFSW00001636100435
Deposit Account	100435
Authorized User	kim tyree
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.492 (National application filing, search, and examination fees)

37 CFR 1.492(a) (Basic national fee only)

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)	P41624US_issue_fee_transmittal.pdf	588822 fb1590c38fc1ad9a1886277493b71844bdf7e744	no	1
Warnings:					
Information:					
2	Power of Attorney	POST_AIA_POA_INTEL.pdf	59541 154e780f8b5b2ceaf641de4af534a74861f5db09	no	1
Warnings:					
Information:					
3	Application Data Sheet	P41624US_correctedADS.pdf	340587 15721813902e0800d09f0c270394e38ba367680b	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
4	Maintenance Fee Address Change	P41624US_fee_address.pdf	156590 bec209679fa00ac857bf25dde5ba47ff3320455c	no	2
Warnings:					
Information:					
5	Assignee showing of ownership per 37 CFR 3.73	P416241US_373_cert.pdf	119635 7d4c339a22ecaf9382643088948a1cafc384ea24	no	3
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	31078 0f62cc3a9ef2223d0623939155c141f07bf59191	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	1296253

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.

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)

73486 7590 09/29/2017
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

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.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US/45631-225521	1045

TITLE OF INVENTION: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

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	12/29/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THANH T	2495	713-171000

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 Barnes & Thornburg 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: Intel Corporation
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Santa Clara, CA

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 100435 (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 /Scott Rylan Powell/ Date December 26, 2017
Typed or printed name Scott Rylan Powell Registration No. 58378

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

Petitioner Samsung Ex-1004, 0803

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
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US

CONFIRMATION NO. 1045

73486
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

POA ACCEPTANCE LETTER

OC000000096332041

Date Mailed: 12/28/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/26/2017.

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**.

/bcrittenden/

Petitioner Samsung Ex-1004, 0804

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
13/997,412	04/03/2014	2495	1800	P41624US	24	3

CONFIRMATION NO. 1045

CORRECTED FILING RECEIPT

73486
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204



Date Mailed: 12/28/2017

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)

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

Applicant(s)

Intel Corporation, Santa Clara, CA;

Power of Attorney: The patent practitioners associated with Customer Number 73486

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/US11/65069 12/15/2011

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.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 10/23/2014

Petitioner Samsung Ex-1004, 0805

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/997,412**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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).

Petitioner Samsung Ex-1004, 0806

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.

Petitioner Samsung Ex-1004, 0807

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
13/997,412	04/03/2014	2495	1800	P41624US	24	3

CONFIRMATION NO. 1045

CORRECTED FILING RECEIPT

73486
Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204



Date Mailed: 01/10/2018

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)

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

Applicant(s)

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

Power of Attorney: The patent practitioners associated with Customer Number 73486

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/US11/65069 12/15/2011

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.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Petitioner Samsung Ex-1004, 0808

If Required, Foreign Filing License Granted: 10/23/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/997,412**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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).

Petitioner Samsung Ex-1004, 0809

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.

Petitioner Samsung Ex-1004, 0810

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.
13/997,412	02/06/2018	9887838	P41624US	1045

73486 7590 01/17/2018

Barnes & Thornburg LLP (Intel)
11 S. Meridian Steet
Indianapolis, IN 46204

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):

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

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.

Petitioner Samsung Ex-1004, 0811