



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	1045

73486 7590 11/16/2015
Barnes & Thornburg LLP (Intel)
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER

LE, THANH T

ART UNIT	PAPER NUMBER
----------	--------------

2495

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

11/16/2015

ELECTRONIC

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

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

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

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

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 06/24/2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 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 06/24/2013 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 07/26/2013, 09/20/2013, 05/27/2014 and 08/18/2014.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 4) ☐ Other: _____.

Art Unit: 2495

DETAILED ACTIONS

Notice of Pre-AIA status

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

Priority

2. Acknowledgement is made of applicant's claim of 371 of PCT /US11/65069 12/15/2011.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 07/26/2013, 09/20/2013, 05/27/2014 and 08/18/2014 have been considered by the examiner.

Drawing Objection

4. Fig. 2 recites: "RSA Key Exchange" which should be a typo.
Appropriate correction is required.

Claim Rejections- 35 U.S.C. § 112 Second Paragraph

5. The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 2 recites the limitations "the response message". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 U.S.C. § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 64-71 are rejected under 35 U.S.C. §101.

Regarding claim 64, it recites “One or more machine-readable storage media comprising...” which can be interpreted as a signal or a carrier wave. This does not fall under one of the four statutory categories. Applicant can overcome this rejection by instead reciting a "***non-transitory*** machine-readable storage media ", which would explicitly exclude signals per se.

- Claims 65-71 depend on claim 71 and they do not limit independent claim 64 or themselves to statutory subject matter; therefore, they are also rejected under 35 USC 101.

Claim Rejections - 35 U.S.C. § 103

7. 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 negated by the manner in which the invention was made.

Art Unit: 2495

8. Claims 48-50, 56-58 and 64-66 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 Goss (US application No. 2005/0213766) hereinafter "Goss".

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, 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);

store the 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.

However, in the field of cryptography, Goss discloses a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine (Abstract: a system-on-a-chip (SoC) has a secure execution environment (SEE) comprising secure memory containing cryptographic key. Fig. 1 and associated text: SoC comprises secure memory. The system on the chip can be interpreted as a security engine).

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

Art Unit: 2495

system on a chip that contains a secure memory to store session key as taught by Goss. The motivation to do so would be to achieve a higher encryption or decryption throughput in SoC than uses a cryptographic accelerator without compromising key or process security as taught by Goss (paragraphs [0006-0008]).

Regarding claim 49, Chou and Goss disclose the system-on-a-chip apparatus of claim 48, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (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 and is the designer's choice to store data for later retrieving. Combining with Goss' 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 Goss disclose the system-on-a-chip apparatus of claim 48, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server (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. Goss, Abstract: secure memory stores cryptographic key. The combination of Chou and Goss' teaching makes it obvious that the server's public key could be stored

Art Unit: 2495

in the secure memory; therefore, the server's public key is a security key of the security engine).

Claims 56-58 and 64-66 are s 48-50 respectively.

9. Claims 51, 52, 59-61 and 67-69 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 Goss (US application No. 2005/0213766), hereinafter "Goss", and further in view of Weisman et al. (US application No. 2009/0280905), hereinafter "Weisman".

Regarding claim 51, Chou and Goss disclose the system-on-a-chip apparatus of claim 50, wherein the security engine to wrap the pre-master key using a server public key (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. Goss, Abstract: secure memory stores cryptographic key).

Chou and Goss do not **explicitly** disclose the **wrapped** pre-master key is stored in the secure storage.

However, in the field of system-on-the-chip, Weisman discloses encrypted key is stored in secure memory (paragraph [0076]: system-on-the-chip product comprises CPU 300. Paragraph [0078]: data stored in `secure` memory may instead be encrypted such that a key known to the CPU 300 is used to decrypted the information strictly inside of registers of CPU 300").

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 Goss' 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 with Weisman's invention of storing encrypted key in secure memory. The motivation to do so would be to provide extra protection to the key.

Regarding claim 52, Chou, Goss, and Weisman disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine 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).

Art Unit: 2495

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, and 70-71 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 Goss (US application No. 2005/0213766), hereinafter "Goss", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho".

Regarding claim 53, Chou and Goss 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 Goss 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-

Art Unit: 2495

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 PK_A 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 Goss' 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 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, Goss, 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).

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

Regarding claim 63, Chou and Goss disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 8 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. Goss, Abstract: secure memory stores cryptographic key. The combination of Chou and Goss' teaching makes it obvious that

Art Unit: 2495

the server's public key could be stored in the secure memory; therefore, the server's public key is a security key of the security engine and it is obvious that the hash code could be signed using a security key stored in a secure memory of the security engine).

Chou and Goss 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 Goss' 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 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.

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 Goss

(US application No. 2005/0213766), hereinafter "Goss", 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 Goss disclose the system-on-a-chip apparatus of claim 48. Chou also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou and Goss 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 Goss' 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 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, Goss, 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, Goss, 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 store session key 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. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-F 6:00 am- 2:30pm.

Art Unit: 2495

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

Art Unit: 2495