Trials@uspto.gov
571-272-7822

Paper 10
Date: June 27, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. and
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

DAEDALUS PRIME LLC,
Patent Owner.

IPR2023-00659 (Patent 9,432,840 B2)
IPR2023-00660 (Patent 8,359,629 B2)
IPR2023-00661 (Patent 10,705,960 B2)
IPR2023-00727 (Patent 9,887,838 B2)
IPR2023-00753 (Patent 10,372,197 B2)

Before WILLIAM V. SAINDON, THOMAS L. GIANNETTI, ARTHUR M. PESLAK, and KRISTI L. R. SAWERT, *Administrative Patent Judges*.[1]

PER CURIAM.

DECISION
Settlement Prior to Institution of Trial
37 C.F.R. § 42.74

---

[1] This is not an expanded panel. The panel for IPR2023-00659 includes Judges Saindon, Peslak, and Sawert. The panel for IPR2023-00660 and -00753 includes Judges Giannetti, Peslak, and Sawert. The panel for IPR2023-00661 includes Judges Saindon, Giannetti, and Peslak. The panel for IPR2023-00727 includes Judges Saindon, Giannetti, and Sawert.

I. INTRODUCTION

With the Board's authorization, Petitioner and Patent Owner (collectively "the Parties") filed a Joint Motion to Terminate in each of the above-identified proceedings. Paper 10 ("Joint Motion").[2] In support of each Joint Motion, the Parties filed a copy of a Settlement Agreement (Ex. 1028) and a Joint Request to Treat the Settlement Agreement as Business Confidential Information (Paper 9 ("Joint Request")) pursuant to 37 C.F.R. § 42.74.

II. DISCUSSION

In the Joint Motions, the Parties represent that they have reached an agreement to jointly seek termination of the above-identified *inter partes* review proceedings, and that the filed copy of the Settlement Agreement is a true and complete copy. Paper 10; 37 C.F.R. § 42.74(b) (requiring a "true copy" of any agreement to be filed with the Board). The Parties state that "there are no other agreements, oral or written, between the Parties made in connection with, or in contemplation of, the termination of the proceeding[s]." Paper 10; 37 C.F.R. § 42.74(b) (requiring "*Any* agreement or understanding between the parties" to be filed with the Board) (emphasis added). The Settlement Agreement indicates that it resolves all currently

[2] This Decision cites to papers and exhibits in IPR2023-00659. Corresponding items were filed in IPR2023-00660, IPR2023-00661, IPR2023-00727, and IPR2023-00753.

pending proceedings between the Parties involving the above-identified patents at issue. Ex. 1028, 1–2.

These proceedings are at an early stage, and we have not yet decided whether to institute trial in any of the proceedings. In view of the early stage of the proceedings and the settlement between the Parties, which resolves all proceedings involving the Parties and the above-identified patents, we determine that good cause exists to terminate the proceedings with respect to the Parties.

The Parties also filed Joint Requests that the Settlement Agreement be treated as business confidential information and be kept separate from the files of the patents involved in these *inter partes* review proceedings. Paper 9. After reviewing the Settlement Agreement between Petitioner and Patent Owner, we find that the Settlement Agreement contains confidential business information regarding the terms of settlement. We determine that good cause exists to treat the Settlement Agreement between Petitioner and Patent Owner as business confidential information pursuant to 37 C.F.R. § 42.74(c).

This Order does not constitute a final written decision pursuant to 35 U.S.C. § 318(a).

III. ORDER

Accordingly, for the reasons discussed above, it is:

ORDERED that the Joint Motion to Terminate in each of the above-

identified proceedings is *granted*, and the proceedings are *terminated*; and

FURTHER ORDERED that the Joint Request to Treat the Settlement Agreement as Business Confidential Information in each of the above-identified proceedings is *granted*, and the Settlement Agreement shall be kept separate from the files of Patents 9,432,840 B2; 8,359,629 B2; 10,705,960 B2; 9,887,838 B2; and 10,372,197 B2 and made available only to Federal Government agencies on written request, or to any person on a showing of good cause, pursuant to 37 C.F.R. § 42.74(c).

FOR PETITIONER:

John Kappos
Benjamin M. Haber
Xin-Yi Zhou
Jeff Baxter
William M. Fink
O'MELVENY & MYERS LLP
jkappos@omm.com
bhaber@omm.com
vzhou@omm.com
jbaxter@omm.com
tfink@omm.com

FOR PATENT OWNER:

Robert S. Magee
BLUE PEAK LAW GROUP LLP
robert@bluepeak.law

Trials@uspto.gov
571-272-7822

Paper 10
Date: June 27, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. and
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

DAEDALUS PRIME LLC,
Patent Owner.

IPR2023-00659 (Patent 9,432,840 B2)
IPR2023-00660 (Patent 8,359,629 B2)
IPR2023-00661 (Patent 10,705,960 B2)
IPR2023-00727 (Patent 9,887,838 B2)
IPR2023-00753 (Patent 10,372,197 B2)

Before WILLIAM V. SAINDON, THOMAS L. GIANNETTI, ARTHUR M. PESLAK, and KRISTI L. R. SAWERT, *Administrative Patent Judges*.[1]

PER CURIAM.

DECISION
Settlement Prior to Institution of Trial
37 C.F.R. § 42.74

---

[1] This is not an expanded panel. The panel for IPR2023-00659 includes Judges Saindon, Peslak, and Sawert. The panel for IPR2023-00660 and -00753 includes Judges Giannetti, Peslak, and Sawert. The panel for IPR2023-00661 includes Judges Saindon, Giannetti, and Peslak. The panel for IPR2023-00727 includes Judges Saindon, Giannetti, and Sawert.

I. INTRODUCTION

With the Board's authorization, Petitioner and Patent Owner (collectively "the Parties") filed a Joint Motion to Terminate in each of the above-identified proceedings. Paper 10 ("Joint Motion").[2] In support of each Joint Motion, the Parties filed a copy of a Settlement Agreement (Ex. 1028) and a Joint Request to Treat the Settlement Agreement as Business Confidential Information (Paper 9 ("Joint Request")) pursuant to 37 C.F.R. § 42.74.

II. DISCUSSION

In the Joint Motions, the Parties represent that they have reached an agreement to jointly seek termination of the above-identified *inter partes* review proceedings, and that the filed copy of the Settlement Agreement is a true and complete copy. Paper 10; 37 C.F.R. § 42.74(b) (requiring a "true copy" of any agreement to be filed with the Board). The Parties state that "there are no other agreements, oral or written, between the Parties made in connection with, or in contemplation of, the termination of the proceeding[s]." Paper 10; 37 C.F.R. § 42.74(b) (requiring "*Any* agreement or understanding between the parties" to be filed with the Board) (emphasis added). The Settlement Agreement indicates that it resolves all currently

[2] This Decision cites to papers and exhibits in IPR2023-00659. Corresponding items were filed in IPR2023-00660, IPR2023-00661, IPR2023-00727, and IPR2023-00753.

pending proceedings between the Parties involving the above-identified patents at issue. Ex. 1028, 1–2.

These proceedings are at an early stage, and we have not yet decided whether to institute trial in any of the proceedings. In view of the early stage of the proceedings and the settlement between the Parties, which resolves all proceedings involving the Parties and the above-identified patents, we determine that good cause exists to terminate the proceedings with respect to the Parties.

The Parties also filed Joint Requests that the Settlement Agreement be treated as business confidential information and be kept separate from the files of the patents involved in these *inter partes* review proceedings. Paper 9. After reviewing the Settlement Agreement between Petitioner and Patent Owner, we find that the Settlement Agreement contains confidential business information regarding the terms of settlement. We determine that good cause exists to treat the Settlement Agreement between Petitioner and Patent Owner as business confidential information pursuant to 37 C.F.R. § 42.74(c).

This Order does not constitute a final written decision pursuant to 35 U.S.C. § 318(a).

III. ORDER

Accordingly, for the reasons discussed above, it is:

ORDERED that the Joint Motion to Terminate in each of the above-

identified proceedings is *granted*, and the proceedings are *terminated*; and

FURTHER ORDERED that the Joint Request to Treat the Settlement Agreement as Business Confidential Information in each of the above-identified proceedings is *granted*, and the Settlement Agreement shall be kept separate from the files of Patents 9,432,840 B2; 8,359,629 B2; 10,705,960 B2; 9,887,838 B2; and 10,372,197 B2 and made available only to Federal Government agencies on written request, or to any person on a showing of good cause, pursuant to 37 C.F.R. § 42.74(c).

FOR PETITIONER:

John Kappos
Benjamin M. Haber
Xin-Yi Zhou
Jeff Baxter
William M. Fink
O'MELVENY & MYERS LLP
jkappos@omm.com
bhaber@omm.com
vzhou@omm.com
jbaxter@omm.com
tfink@omm.com

FOR PATENT OWNER:

Robert S. Magee
BLUE PEAK LAW GROUP LLP
robert@bluepeak.law

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☐ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22cv354	9/12/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
Daedalus Prime LLC	Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., Samsung Semiconductor, Inc., and Samsung Austin Semiconductor, LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,996,135	6/12/2018	Daedalus Prime LLC
2	10,705,960	7/7/2020	Daedalus Prime LLC
3	10,372,197	8/6/2019	Daedalus Prime LLC
4	9,887,838	2/6/2018	Daedalus Prime LLC
5	8,359,629	1/22/2013	Daedalus Prime LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☐ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22cv354	9/12/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
Daedalus Prime LLC	Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., Samsung Semiconductor, Inc., and Samsung Austin Semiconductor, LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,432,840	8/30/2016	Daedalus Prime LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

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.

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.

MediaTek Exhibit 1012, Page 12 of 463

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).

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.

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

OC000000096332081

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

MediaTek Exhibit 1012, Page 15 of 463

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).

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.

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/

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	1/21/2013
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				

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

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

Signature	~~/Glen M. Kellett, Reg No. 60202/~~ /Scott Rylan Powell/			Date (YYYY-MM-DD)	~~2013-06-10~~ 2017-12-26
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.

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

Fax to:
571-273-6500

- OR -

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

MediaTek Exhibit 1012, Page 34 of 463

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.

PTOL-85 (Rev. 02/11)

MediaTek Exhibit 1012, Page 35 of 463

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

MediaTek Exhibit 1012, Page 36 of 463

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.

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

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.

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.

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.

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

		(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

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	

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

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

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

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.

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

☒ Patent Practitioner Signature

Applicant Signature

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.

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.

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.

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

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

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.

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.

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: 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.

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.

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.

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.

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

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.

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.

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

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.

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

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."

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.

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

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 b94d30d00077c00266a379194a9e69f01934a1ef	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

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 **07/26/2017**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	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	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.

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

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: _____.

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.

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]

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.**

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.

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]

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/		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.**

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.

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	-	-	-	-					

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	✓	✓	✓	✓					

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

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

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

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]

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.

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.**

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.

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 3a5d96e790b88ce5d941de75a0edf3ade56778a6	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.

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**.

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.

MediaTek Exhibit 1012, Page 128 of 463

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.

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.

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.

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.

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.

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.

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.

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

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.

MediaTek Exhibit 1012, Page 137 of 463

> 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.

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.

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

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.

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

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: _____.

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.

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]	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]

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.

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	-	-	-						

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	✓	✓	✓						

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

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]

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):

☒ 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.**

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.

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.

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

☒ 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)	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.

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.

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]

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.

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)	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.

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.

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

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

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.

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**.

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.

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;

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.

MediaTek Exhibit 1012, Page 202 of 463

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.

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.

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;

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.

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.

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

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

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

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 29d4a314f1bf163e600cd8c911bee0fae36552f4	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.

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 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 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

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: _____.

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.

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.

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

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	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

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	☒
/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	☐

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.

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.**

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.

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

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

			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

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	-	-							

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	✓	✓							

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
	1	8014530		2011-09-06	Ernest Brickell	
	2	7802085		2010-09-21	Gary L. Graunke	
	3	7747862		2010-06-29	Shlomo Ovadia	
	4	7350083		2008-03-25	Steven E. Wells	
	5	6948065		2005-09-20	David W. Grawrock	
	6	7600132		2009-10-06	Fadi A. Mahmoud	
	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

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
	1	20080244267		2008-10-02	Vincent J. Zimmer	
	2	20070138229		2007-06-21	Yasuyuki Fujimoto	
	3	20110154023		2011-06-23	Ned M. Smith	
	4	20060005011		2006-01-05	Masakazu Satoh	
	5	20070240200		2007-10-11	Hee-chul Han	
	6	20130297936		2013-11-07	Hormuzd M. Khosravi	
	7	20050144436		2005-06-30	Tse-Min Chen	
	8	20030236970		2003-12-25	Rodney Wendell Palmer	
	9	20090319804		2009-12-24	Zheng QI	
	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

	11	20070192611		2007-08-16	Shamanna M. Datta	
	12	20020112161		2002-08-15	Fred C. Thomas	
	13	20080077809		2008-03-27	Don L. Hayler	
	14	20110161645		2011-06-30	Jiang Zhang	
	15	20050213766		2005-09-29	Steven C. Goss	
	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]
	1	2011119985	WO		2011-09-29	Maxlinear, Inc.		
	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

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
	1	Taiwanese Office Action issued in connection with Taiwanese Application No. 101147203, completed December 29, 2014, 11 pages	☒
	2	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065072, mailed June 26, 2014, 6 pages.	☐
	3	International Search Report and Written Opinion received for International Application No. PCT/US2011/065072, Mailed July 18, 2012, 10 Pages	☐
	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)	☐
	5	Data Security Architure using Embedded Chip. Thomas et al. IJCSNS (May 2011)	☐
	6	Scalable Architectural Support for Trusted Software. Champagne et al. IEEE (2009)	☐
	7	Secure Memory Accesses on Networks-on Chip. Fiorin et al. IEEE (2009)	☐
	8	Extended European Search Report issued in connection with European Application No. 11877254.0 - 1853, dated July 17, 2015, 8 pages	☐
	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.	☐
	10	Intel Corp., Product Brief: Intel Atom Processor CE4100, 2009, Pg. 1-4	☐

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

	11	Digital Transmission License Administrator, Digital Transmission Content Protection Specification, March 19, 2010, Volume 1, Pg. 11, 26-29, and 36-38	☐
	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		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	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.**

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.

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/Priscilla York
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**

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:

FEBRUARY 15, 2016

RESPONSE TO OFFICE ACTION

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

Sir:

In response to the Office Action dated November 16, 2015, 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 server over a network using the nonce;

perform a cryptographic key exchange with the 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;

encrypt the 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 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 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 [[a]] the security key of the security engine, and send the encrypted pre-master key to the server.

MediaTek Exhibit 1012, Page 256 of 463

51. (Currently Amended) 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 ~~storage~~ 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 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 [[a]] the security key of the security engine, and send the signed public Diffie-Hellman key to the 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 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 server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure ~~storage~~ 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 server over a network, the request including the random nonce;

MediaTek Exhibit 1012, Page 257 of 463

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

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 [[a]] 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 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 server; and further comprising:

receiving a ServerHello message from the 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 server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

59. (Currently Amended) 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 ~~storage~~ 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 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 server.

62. (Currently Amended) The method of claim 56, wherein performing the cryptographic key exchange with the 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 [[a]] the security key of the security engine of the system-on-a-chip;

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

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

signing the hash code using [[a]] the security key stored in [[a]] the 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.

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 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 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;

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 [[a]] the secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the 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 server; and

wherein the plurality of instructions further cause the computing device to:
receive a ServerHello message from the 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. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate a pre-master key in the security engine;

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

send the encrypted pre-master key to the server.

67. (Currently Amended) 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 ~~storage~~ 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 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 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 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 [[a]] the security key of the security engine of the system-on-a-chip;

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

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

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

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

MediaTek Exhibit 1012, Page 262 of 463

REMARKS

Applicants thank the Examiner for consideration of the present application. Applicants have carefully reviewed the Office Action dated November 16, 2015 (hereinafter "the Office Action"). Claims 1-47 are pending in this application. In the present Response, Applicants have amended claims 48-56, 58, 59, and 62-71 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. DRAWING OBJECTION

The Office Action objected to FIG. 2, stating that FIG. 2 recites "RSA Key **Excange**" rather than "RSA Key **Exchange**". A replacement drawing is submitted herewith to address the typographical error. Accordingly, Applicants respectfully request withdrawal of the objection to the drawings.

II. CLAIM REJECTION – 35 U.S.C. § 112, Second Paragraph

The Office Action rejected claim 49 under 35 U.S.C. 112, Second Paragraph stating that there is insufficient antecedent basis for "the response message". Claim 49 has been amended to address the rejection. More specifically, claim 49 has been amended to recite "to receive a server nonce from the server in a response message . . . the response message including . . ." For at least this reason, Applicants respectfully request withdrawal of the Section 112, Second Paragraph rejection of claim 49.

I. 35 U.S.C. § 101 REJECTIONS

The Office Action rejected each of claims 64-71 as being directed to non-statutory subject matter. Specifically, the Office Action found that the metes and bounds of those claims to not positively limit the invention to non-transitory media. In the interest of expediting prosecution of the present application, Applicants have amended each of claims 64-71 to recite "one or more non-transitory machine-readable storage media." In so doing, Applicants respectfully submit that the term "non-transitory" excludes only the subject matter of a transitory signal *per se* in accordance with *In re Nuijten*, 500 F. 3d 1346 (Fed. Cir. 2007), and specifically includes machine-readable devices wherein data is stored in a temporary manner, such as volatile

memory devices or RAM. As such, Applicants respectfully submit that those amendments overcome the present Section 101 rejections.

II. 35 U.S.C. § 103(a) REJECTIONS

Each of claims 48-50, 56-58, and 64-66 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,966,646 of Chou et al. (hereinafter "Chou") in view of U.S. Patent Application Publication No. 2005/0213766 of Goss (hereinafter "Goss"). Additionally, each of claims 51, 52, 59-61, and 67-69 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and U.S. Patent Application Publication No. 2009/0280905 to Weisman et al. (hereinafter "Weisman"). Further, each of claims 53, 54, 62, 63, 70, and 71 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and U.S. Patent Application No. 2010/0042839 of Ho (hereinafter "Ho"). Additionally, claim 55 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and Ho, in further 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(a) rejection of independent claim 48, the Office Action asserts that Chou in view of Goss describes or suggests every feature of independent claim 48. Applicants disagree. However, in order to expedite prosecution of the present application, Applicants have amended independent claim 48 to recite that the secure memory includes a

security key that was encoded in the secure memory when the system-on-a-chip was manufactured and that the security key is used by the security engine to encrypt a session key. More specifically, claim 1 has been amended to recite: "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 . . . encrypt the session key based on the security key…."

No combination of Chou and Goss describes or suggests a system-on-a-chip that includes a security engine in which a secure memory of the security engine includes a security key that was encoded in the secure memory when the system-on-a-chip was manufactured. Further, no combination of Chou and Goss describes using such a security key to encrypt a session key. The Office Action acknowledges, on page 5, that Chou does not disclose a system-on-a-chip that includes a security engine. Rather, the Office Action cites Goss at the Abstract and FIG. 1 as allegedly describing a system-on-a-chip having a security engine that includes a secure memory that is accessible only by the security engine. In Goss, a cryptographic accelerator is used to perform encryption functions. The cryptographic accelerator has a key register that receives a key from a secure execution environment ("SEE") and performs cryptographic functions on behalf of the SEE. As described at paragraph [0024], the key in Goss is stored in RAM, which is a type of volatile memory. In other words, the key is unlike the security key recited in claim 48, which was encoded in the secure memory when the system-on-a-chip was manufactured. Accordingly, in Goss, any cryptographic functions are performed by a cryptographic accelerator that receives a temporary key into a key register from RAM, rather than using a security key that (i) was permanently encoded into a secure memory of a system-on-a-chip when the system-on-a-chip was manufactured and (ii) is accessible only to a security engine residing on the system-on-a-chip. For at least the reasons discussed above, Applicants respectfully submit that the proposed combination of Chou and Goss does not render claim 48 obvious and Applicants respectfully request withdrawal of the Section 103(a) rejection of claim 48.

B. Independent Claim 56

The Office Action also rejected claim 56 under Section 103(a) as being rendered obvious by Chou and Goss, 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 Goss does not render claim 56 obvious and Applicants respectfully request withdrawal of the Section 103(a) rejection of claim 56.

C. Independent Claim 64

The Office Action also rejected claim 64 under Section 103(a) as being rendered obvious by Chou and Goss, 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 Goss does not render claim 64 obvious and Applicants respectfully request withdrawal of the Section 103(a) 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. Weisman, Ho, and Peyravian do not cure the deficiencies of Chou and Goss with respect to independent claims 48, 56, and 64. Accordingly, Applicants respectfully request withdrawal of the Section 103(a) 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.

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

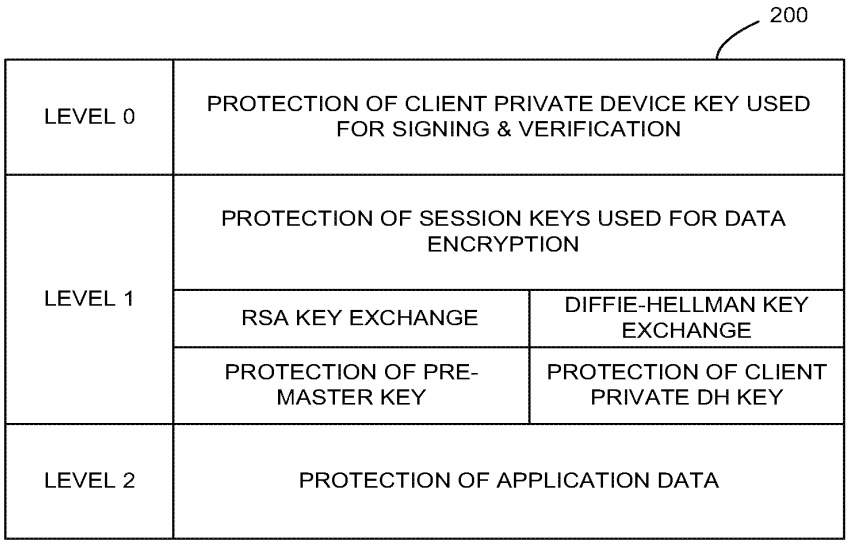

200
LEVEL 0
PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION
LEVEL 1
PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION
RSA KEY EXCHANGE
DIFFIE-HELLMAN KEY EXCHANGE
PROTECTION OF PRE-MASTER KEY
PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2
PROTECTION OF APPLICATION DATA

FIG. 2

Electronic Acknowledgement Receipt	
EFS ID:	24912659
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/Priscilla York
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	15-FEB-2016
Filing Date:	03-APR-2014
Time Stamp:	15:58:02
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	225521_Response_To_Office_Action.pdf	65979 85170e9b87fb3740145b3fbaf1f04bdb68398984	no	13

Warnings:
Information:

2	Drawings-only black and white line drawings	Replacement_FIG_2.pdf	19847 5527689954fa726d154890c6d5eb8237c8c34f07	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	85826	

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 **02/15/2016**

	(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
/TARA WITCHER/

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	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: _____.

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 ***Excange***" 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 negatived by the manner in which the invention was made.

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

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

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).

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-

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 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

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.

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 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-2011/0235806 A1	09-2011	Fukuda; Naohiro	H04L9/0825	380/282
*	M	US-2011/0231923 A1	09-2011	Bollay; Benn Sapin	H04L63/166	726/9

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.

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-8,615,787 B2	12-2013	Murray; Bruce	H04L63/0853	380/281
*	B	US-8,627,440 B2	01-2014	Mowers; David R.	H04L63/0807	380/279
*	C	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	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.

Receipt date: 08/18/2014

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
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	8645677	B2	2014-02-04	Khosravi et al.	

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.L./	1	20110023077	A1	2011-01-27	Simon	
/T.L./	2	20080177998	A1	2008-07-24	Apsangi et al.	
/T.L./	3	20060133604	A1	2006-06-22	Buer 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.L./	1	2014074127	WO	A1	2014-05-15	Intel Corporation		☐

Receipt date: 08/18/2014

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

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]
/T.L./	1	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065069, mailed June 26, 2014, 8 pages.	☐

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	08/20/2015

*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.

Receipt date: 08/18/2014

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-08-18
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	34	("20100299525" | "20020163522" | "20130275769" | "20060133604" | "20120079287" | "20080177998" | "20110231923" | "8295484" | "20050213768" | "20130297936" | "20140129827" | "8645677" | "20080037793" | "20070209072" | "20110023077").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 06:04
S2	1	13/997412	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 06:42
S3	22	(("8205238") or ("7813822") or ("6324288") or ("20120137137") or ("20110154061") or ("20130080764")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/14 06:54
S4	2	13/694221	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 08:50
S5	0	((hormuzd near2 khosravi) (edward near2 epp) (farhana near2 kabir)) .in. and (generat$3 with random with nonce with key with exchang$3 with session with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:12
S6	0	((hormuzd near2 khosravi) (edward near2 epp) (farhana near2 kabir)).in. and (generat$3 with random with nonce with key with exchang$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:12
S7	0	(intel).as. and (generat$3 with random with nonce with key with exchang$3 with session with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:13

S8	0	(intel).as. and (generat$3 with random with nonce with key with exchang$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:13
S9	1	(generat$3 with random with nonce with key with exchang$3 with session with key).clm. and (H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:14
S10	2	(generat$3 with random with nonce with key with exchang$3 with session with key) and (H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:19
S11	1	S10 not S9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:19
S12	1	(generat$3 with random with nonce with key with exchang$3 with session with key).clm. and (713/171).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:21
S13	4	(generat$3 with random with nonce with key with exchang$3 with session with key) and (713/171).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:23
S14	3	S13 not S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:23
S17	5	(("20080077809") or ("20110161645")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/21 08:17
S18	3	("20080037793").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2015/08/21 11:30

			DERWENT; IBM_TDB			
S19	15	(generat$3 with random with nonce with key with exchang$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:35
S20	19	(random with nonce with key with exchang$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:53
S21	4	S20 not S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:53
S22	94	(nonce with key with exchang$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:59
S23	75	S22 not (S19 S20)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:59
S24	763	(diffie-hellman with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:02
S25	41	(diffie-hellman with session with key) and (nonce with key with exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:02
S26	34	(@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) and (nonce with key with exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:05
S27	29	(("20060041938") or ("8627440") or ("8006090") or ("8392968") or ("5657390") or ("5825890") or	US-PGPUB; USPAT; USOCR;	OR	OFF	2015/08/24 11:28

		("7966646")).PN.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S28	11	S27 and (random nonce (key with exchang$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 11:58
S29	11	S27 and (random nonce (key with exchang$3) (session adj key) hash diffie-hellman)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 12:00
S30	75	(@pd<"20111215" @ad<"20111215") and (diffie-hellman with generat$3 with key) and ((random nonce) with key with exchang$3) and (hash with (random nonce))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 13:30
S31	9	(@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((TLS (transport adj layer adj security)) with (handshak$3 hello) with (random nonce)) and (key with exchang$3) and ((secret session) with key) and (hash with (nonce random))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 14:39
S32	0	(@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on-a-chip SOC) with secure with communication)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:45
S33	1596	(@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and (system-on-a-chip SOC)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:45
S34	26	(@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on-a-chip SOC) with (TLS (transport adj layer adj security)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:46
S35	26	(@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on-chip SOC) with (TLS (transport adj layer adj security)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:48
S36	8	(@pd<"20111215" @ad<"20111215") and	US-PGPUB;	OR	ON	2015/08/24

		(SSL (secure adj socket adj layer)).ti,bsum,ab. and ((system-on-chip SOC) with (SSL (secure adj socket adj layer)))	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:50
S37	155	(@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:53
S38	23	(@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag$3) with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:53
S39	168	(@pd<"20111215" @ad<"20111215") and (diffie-hellman with (generat$3 exchang$3) with key with stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 16:43
S40	48	(@pd<"20111215" @ad<"20111215") and (SSL (secure adj socket adj layer) TLS (transport adj layer adj security)) and (diffie-hellman with (generat$3 exchang$3) with key with stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 16:45
S41	2	("8788805").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/24 17:34
S42	30	("20010020274" | "6367009" | "20030120948" | "20050074126" | "6643774" | "20050074126" | "20030126464" | "6081900" | "20030005286" | "20010020274" | "5923756" | "6633979" | "6205482" | "7096352").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/26 11:41
S43	5	(("20080077809") or ("20110161645")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/02 08:37
S44	1	"13997406"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2015/11/02 09:06

			IBM_TDB			
S45	38	(US-20080037793-$ or US-20140129827-$ or US-20130297936-$ or US-20130275769-$ or US-20120079287-$ or US-20110231923-$ or US-20110023077-$ or US-20100299525-$ or US-20080177998-$ or US-20070209072-$ or US-20060133604-$ or US-20050213768-$ or US-20020163522-$ or US-20130080764-$ or US-20120137137-$ or US-20110154061-$).did. or (US-8205238-$ or US-7813822-$ or US-6324288-$).did. or (KR-20140129827-$ or KR-20120079287-$ or KR-20110023077-$ or KR-20080037793-$ or KR-20060133604-$).did. or (US-20140129827-$ or WO-2013089726-$ or WO-2013089728-$ or US-20130080764-$ or WO-2011116342-$ or WO-2011109780-$ or US-20100299525-$ or WO-2009073925-$ or US-20080177998-$ or EP-1826694-$ or US-20060133604-$ or US-20050213768-$ or EP-1484890-$ or US-20020163522-$).did.	US-PGPUB; USPAT; FPRS; DERWENT	OR	ON	2015/11/02 09:16
S46	30	S45 and (system-on-a-chip (random adj nonce) (key with exchang$3) (session adj key) (stor$3) hash Diffie-Hellman (Diffie near2 Hellman) d-h)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/02 09:16
S47	3	("7096352").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/02 12:56
S48	41	(("20050213766") or ("8615787") or ("20100299525") or ("7069352") or ("20050005093") or ("20110235806") or ("20080037793") or ("20140270166") or ("8627440") or ("20050289343") or ("20110231923") or ("7966646") or ("20100042839") or ("20110161645") or ("20080077809") or ("20060041938")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/03 07:56
S51	16	(US-20150039890-$ or US-20050005093-$ or US-20100205443-$ or US-20060041938-$ or US-20100042839-$ or US-20050289343-$ or US-20050213766-$ or US-20110235806-$ or US-20140270166-$ or US-20110231923-$).did. or (US-8627440-$ or US-7966646-$ or US-5657390-$ or US-7096352-$ or US-8615787-$ or US-7069352-$).did.	US-PGPUB; USPAT	OR	ON	2015/11/04 08:56
S52	16	S51 and (hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification)	US-PGPUB; USPAT	OR	ON	2015/11/04 09:01
S53	16	S51 and (sign$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification)	US-PGPUB; USPAT	OR	ON	2015/11/04 13:01

S54	16	S51 and (sign$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification verif$3)	US-PGPUB; USPAT	OR	ON	2015/11/04 13:06
S55	37	(@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag$3)) and (cryptograph$3 with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:37
S56	232	(@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) and ((global near3 value) prime primitive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:40
S57	31	(@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) same ((global near3 value) prime primitive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:40
S58	16	(US-20150039890-$ or US-20050005093-$ or US-20100205443-$ or US-20060041938-$ or US-20100042839-$ or US-20050289343-$ or US-20050213766-$ or US-20110235806-$ or US-20140270166-$ or US-20110231923-$).did. or (US-8627440-$ or US-7966646-$ or US-5657390-$ or US-7096352-$ or US-8615787-$ or US-7069352-$).did.	US-PGPUB; USPAT	OR	ON	2015/11/05 09:06
S59	16	S58 and (sign$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric stor$3 verification verif$4)	US-PGPUB; USPAT	OR	ON	2015/11/05 09:06
S60	16	S58 and (sign$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric stor$3 verification verif$4 encrypt$3 master)	US-PGPUB; USPAT	OR	ON	2015/11/05 09:08
S61	3291	(@pd<"20111215" @ad<"20111215") and ((encrypted adj key) with stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 09:51
S62	5	(@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag$3)) and ((encrypted adj key) with stor$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 09:53
S63	11	S58 and (Diffie-Hellman global prime primitive adj root)	US-PGPUB; USPAT	OR	ON	2015/11/05 12:24
S64	3	S58 and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT	OR	ON	2015/11/05 12:24

S65	0	(@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag$3)) and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:26
S66	409	(@pd<"20111215" @ad<"20111215") and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:26
S67	28	(@pd<"20111215" @ad<"20111215") and ((send$3 transmit$3) with (Diffie-Hellman with (global prime primitive adj root)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:27

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S15	3	(generat$3 with random with nonce with key with exchang$3 with session with key).clm.	US-PGPUB; USPAT	OR	ON	2015/08/14 11:29
S16	4	"8209533"	US-PGPUB; USPAT	OR	ON	2015/08/14 11:52

11/5/2015 2:29:05 PM
C:\Users\tle22\Documents\EAST\Workspaces\13997412.wsp

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

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	8295484	B2	2012-10-23	Buer et al.	
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.L./	1	20140129827	A1	2014-05-08	Khosravi et al.	
/T.L./	2	20130297936	A1	2013-11-07	Khosravi et al.	
/T.L./	3	20130275769	A1	2013-10-17	Khosravi et al.	US equivalent of TW 201340692 below.
/T.L./	4	20120079287	A1	2012-03-29	Leclercq	
/T.L./	5	20070209072	A1	2007-09-06	Chen	

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

/T.L./	6	20020163522	A1	2002-11-07	Porter 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.L./	1	201340692	TW	A	2013-10-01	Intel Corporation	Taiwanese equivalent of US 20130275769 above.	☒

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]
	1		☐

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	08/20/2015

*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	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-05-27
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
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.L./	1	20110231923	A1	2011-09-22	Bollay et al.	
/T.L./	2	20100299525	A1	2010-11-25	Shah et al.	
/T.L./	3	20080037793	A1	2008-02-14	Buer	
/T.L./	4	20050213768	A1	2005-09-29	Durham 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]

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

	1	2013089725	WO	A1	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

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]
/T.L./	1	International Search Report and Written Opinion received for International Application No. PCT/US2011/065069, mailed August 30, 2012, 11 pages.	☐
/T.L./	2	"Transport Layer Security," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=464220022], edited December 5, 2011, 19 pages.	☐
/T.L./	3	"HTTP Secure," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=HTTP_Secure&oldid=465003157], edited December 9, 2011, 6 pages.	☐

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	08/20/2015

*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	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-07-26
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

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

BIB DATA SHEET

CONFIRMATION NO. 1045

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/997,412	04/03/2014 RULE	713	2495	P41624US

APPLICANTS

INVENTORS

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/US11/65069 12/15/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

10/23/2014

Foreign Priority claimed	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☐	OR	4	24	3
35 USC 119(a-d) conditions met ☑ Yes ☐ No					
Verified and Acknowledged /THANH T LE/ Examiner's Signature	Initials				

ADDRESS

Barnes & Thornburg LLP (Intel)
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402
UNITED STATES

TITLE

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

FILING FEE RECEIVED		
1800	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

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

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

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								
	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	-								

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								
	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	✓								

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS

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	8205238	B2	2012-06-19	Blumenthal et al.	
/T.L./	2	7813822	B1	2010-10-12	Hoffberg	
/T.L./	3	6324288	B1	2001-11-27	Hoffman	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20130080764	A1	2013-03-28	Khosravi et al.	
/T.L./	2	20120137137	A1	2012-05-31	Brickell et al.	
/T.L./	3	20110154061	A1	2011-06-23	Chilukuri et al.	

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

/T.L./	4	20080229104	A1	2008-09-18	Ju et al.	
/T.L./	5	20080148061	A1	2008-06-19	Jin et al.	
/T.L./	6	20080022395	A1	2008-01-24	Holtzman et al.	
/T.L./	7	20070156987	A1	2007-07-05	Chen	
/T.L./	8	20050114687	A1	2005-05-26	Zimmer et al.	
/T.L./	9	20040243823	A1	2004-12-02	Moyer et al.	

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

FOREIGN PATENT DOCUMENTS

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	2013089728	WO	A1	2013-06-20	Intel Corporation		☐
/T.L./	2	2013089726	WO	A1	2013-06-20	Intel Corporation		☐

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

NON-PATENT LITERATURE DOCUMENTS

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	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.	T[5]
/T.L./	1	BAJIKAR, "Trusted Platform Module (TPM) based Security on Notebook PCs," White Paper, June 20, 2002, 20 pages.	☐
/T.L./	2	INTEL CORP., "Product Brief: Intel® Atom™ Processor CE4100," 2009, 4 pages.	☐
/T.L./	3	"Diffie-Hellman key exchange," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Diffie%E2%80%93Hellman_key_exchange&oldid=464229141>, accessed December 8, 2011, 9 pages.	☐
/T.L./	4	"Elliptic curve cryptography," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Elliptic_curve_cryptography&oldid=464634149>, accessed December 8, 2011, 8 pages.	☐
/T.L./	5	"Scrambler," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Scrambler&oldid=460036487>, accessed December 8, 2011, 4 pages.	☐
/T.L./	6	U.S. Patent Application Serial No. 13/694,221, filed November 8, 2012, 50 pages.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Thanh Le/	Date Considered	08/20/2015

*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	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-09-20
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

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)
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402

PUBLICATION NOTICE



Title:METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

Publication No.US-2015-0039890-A1
Publication Date:02/05/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/997,412	Hormuzd M. Khosravi	P41624US

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

INTERNATIONAL APPLICATION NO.	
PCT/US11/65069	
I.A. FILING DATE	PRIORITY DATE
12/15/2011	

CONFIRMATION NO. 1045
371 ACCEPTANCE LETTER

OC000000071507632

Date Mailed: 10/28/2014

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

04/03/2014	04/03/2014
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).*

The following items have been received:

- Copy of the International Application filed on 06/24/2013
- Copy of the International Search Report filed on 06/24/2013
- Preliminary Amendments filed on 06/24/2013
- Information Disclosure Statements filed on 07/26/2013
- Inventor's Oath or Declaration filed on 04/03/2014
- Request for Immediate Examination filed on 04/03/2014
- U.S. Basic National Fees filed on 06/24/2013
- Authorization to Permit Access filed on 06/24/2013

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

BRIAN A HARDEN

Telephone: (703) 756-1815

FORM PCT/DO/EO/903 (371 Acceptance Notice)

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		1800	P41624US	24	3

CONFIRMATION NO. 1045

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

FILING RECEIPT

OC000000071507631

Date Mailed: 10/28/2014

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 - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

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: 02/05/2015

MediaTek Exhibit 1012, Page 322 of 463

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

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).

MediaTek Exhibit 1012, Page 323 of 463

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/997,412

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	480
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20 =	* 4			OR	x 80 =	320
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00
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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1800

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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 found in the appropriate box in column 1.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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 M. Khosravi
Art Unit	UNK
Examiner Name	UNK
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	8645677	B2	2014-02-04	Khosravi et al.	

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	20110023077	A1	2011-01-27	Simon	
	2	20080177998	A1	2008-07-24	Apsangi et al.	
	3	20060133604	A1	2006-06-22	Buer 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	2014074127	WO	A1	2014-05-15	Intel Corporation		☐

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

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]
	1	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065069, mailed June 26, 2014, 8 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	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-08-18
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

Electronic Acknowledgement Receipt	
EFS ID:	19887003
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:	Christopher A. Singh/Stacy Tebo
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	18-AUG-2014
Filing Date:	
Time Stamp:	12:29:58
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)	P41624US_SupplDS.pdf	612385 a2fdaaabf3bd9a9bf654610997a6eba4c277b4cd	no	4

Warnings:
Information:

2	Foreign Reference	FR1.pdf	1836210 a34b6b8eb01301c62b15862a341138f3426272c5	no	41
Warnings:					
Information:					
3	Non Patent Literature	NPL1.pdf	260581 a372ced5356b790ffba386cd61954003cc76a0d3	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	2709176		

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

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

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	8295484	B2	2012-10-23	Buer et al.	
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	20140129827	A1	2014-05-08	Khosravi et al.	
	2	20130297936	A1	2013-11-07	Khosravi et al.	
	3	20130275769	A1	2013-10-17	Khosravi et al.	US equivalent of TW 201340692 below.
	4	20120079287	A1	2012-03-29	Leclercq	
	5	20070209072	A1	2007-09-06	Chen	

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 M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

	6	20020163522	A1	2002-11-07	Porter 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	201340692	TW	A	2013-10-01	Intel Corporation	Taiwanese equivalent of US 20130275769 above.	☒

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]
	1		☐

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	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

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	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-05-27
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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.

Electronic Acknowledgement Receipt	
EFS ID:	19136152
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:	Christopher A. Singh
Filer Authorized By:	
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	27-MAY-2014
Filing Date:	
Time Stamp:	17:12:25
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)	P41624US_SupplDS.pdf	612446 ed2cc37fbf7140f85726dd94bad22d1e00fdc73d	no	4

Warnings:
Information:

2	Foreign Reference	FR1.pdf	1293959 2e675262a929587dd0fa9667f25cfa754e55044f	no	37

Warnings:	
Information:	
Total Files Size (in bytes):	1906405

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

Int'l Application No.:	PCT/US2011/068279
Int'l Application Filing Date:	December 15, 2011
U.S. Application No.:	13/997,412
Confirmation No.:	1045
Art Unit:	Unknown
Examiner:	Unknown
Application Title:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor:	Hormuzd M. Khosravi
Filed:	June 24, 2013
Attorney Docket:	P41624US/45631-225521

ELECTRONICALLY SUBMITTED ON:

APRIL 3, 2014

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

MAIL STOP PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

In response to the Notification of Missing Requirements under 35 U.S.C. 371 dated July 23, 2013, Applicants respectfully submit herewith:

1. An executed Declaration signed by inventor Farhana Kabir identifying the present application by the International application number and international filing date; and

2. An executed Supplemental Declaration signed by inventor Hormuzd M. Khosravi and an executed Supplemental Declaration signed by inventor Edward C. Epp, each identifying the present application by the International application number and international filing date, and each being in compliance with 37 CFR 1.497(a) and (b).

Applicants believe this submission completes the requirements for acceptance under 35 U.S.C. 371. No fee is believed to be due with regard to this submission. However, the Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Deposit Account No. 50-4238 with reference to Docket No. P41624US.

Respectfully submitted,

/ Christopher A. Singh /

Christopher A. Singh
Registration No. 61,236
Barnes & Thornburg LLP
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-6458
Fax: (317) 231-7433

INDS02 1315889v1

Docket No.: P41624US
PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

the specification of which (check one):

___ is attached hereto.
X was filed on June 24, 2013 as
United States Application Number 13/997,412
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(e) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed?		Certified Copy Attached?	
___	___	___	___	___	___	___

Docket No.: P41624US
PATENT

(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No

I hereby appoint practitioners associated with the Customer Number: **73486**
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: **73486**

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

Full Name of Sole/First Inventor **Hormuzd M. KHOSRAVI**

Inventor's Signature _____ Date 3/14/2014

Residence Portland, OR (City, State) Citizenship ~~India~~ U.S.A (Country)

Post Office Address 4737 NW Rainier Ter

Portland, OR 97229

Full Name of Second/Joint Inventor **Edward C. EPP**

Inventor's Signature _____ Date _____

Residence Portland,OR (City, State) Citizenship United States of America (Country)

Post Office Address 3035 NE 23rd Av

Portland, OR 97212

Docket No.: P41624US
PATENT

Full Name of Third/Joint Inventor **Farhana KABIR**

Inventor's Signature _____ Date _____

Residence Camas, WA (City, State) Citizenship United States of America (Country)

Post Office Address 20021 SE 3rd Circle

Camas, WA 98607

Docket No.: P41624US
PATENT

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

(e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

(d)

Docket No.: P41624US
PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

the specification of which (check one):

__ is attached hereto.
X was filed on June 24, 2013 as
United States Application Number 13/997,412
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(e) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed?		Certified Copy Attached?	
_____	_____	_____	___	___	___	___

Docket No.: P41624US
PATENT

(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No

I hereby appoint practitioners associated with the Customer Number: **73486**
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: **73486**

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

Full Name of Sole/First Inventor **Hormuzd M. KHOSRAVI**

Inventor's Signature _____ Date _____

Residence Portland, OR (City, State) Citizenship India (Country)

Post Office Address 4737 NW Rainier Ter

Portland, OR 97229

Full Name of Second/Joint Inventor **Edward C. EPP**

Inventor's Signature _____ Date 3-19-19

Residence Portland,OR (City, State) Citizenship United States of America (Country)

Post Office Address 3035 NE 23rd Av

Portland, OR 97212

Docket No.: P41624US
PATENT

Full Name of Third/Joint Inventor **Farhana KABIR**

Inventor's Signature _____ Date _____

Residence Camas, WA (City, State) Citizenship United States of America (Country)

Post Office Address 20021 SE 3rd Circle

Camas, WA 98607

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

(e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

(d)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

the specification of which (check one):

___ is attached hereto.
X was filed on **June 24, 2013** as
United States Application Number **13/997,412**
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(c) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed?		Certified Copy Attached?	

(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No

I hereby appoint practitioners associated with the Customer Number: **73486**
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: **73486**

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

Full Name of Sole/First Inventor **Hormuzd M. KHOSRAVI**

Inventor's Signature _____ Date _____

Residence Portland, OR (City, State) Citizenship India (Country)

Post Office Address 4737 NW Rainier Ter

Portland, OR 97229

Full Name of Second/Joint Inventor **Edward C. EPP**

Inventor's Signature _____ Date _____

Residence Portland,OR (City, State) Citizenship United States of America (Country)

Post Office Address 3035 NE 23rd Av

Portland, OR 97212

Full Name of Third/Joint Inventor **Farhana KABIR**

Inventor's Signature Farhana M. Kabir Date 03/24/2014

Residence Camas, WA (City, State) Citizenship United States of America (Country)

Post Office Address 20021 SE 3rd Circle

Camas, WA 98607

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

(e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

(d)

Electronic Acknowledgement Receipt	
EFS ID:	18662321
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:	Christopher A. Singh/Ernest Carlson
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	03-APR-2014
Filing Date:	
Time Stamp:	13:13:21
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	Transmittal Letter	225521TransmittalLetter.pdf	134279 72745e44c03823e08f2316d84d2a795bc19594f5	no	3
Warnings:					
Information:					

2	Supplemental Response or Supplemental Amendment	P41624US_RespNotificationMissingReqs.pdf	113885 6baaacd09c4528e48dd6ff1ceafaef9e530fdada	no	2
Warnings:					
Information:					
3	Oath or Declaration filed	P41624US_Declarations.pdf	368819 a550d522852ece444ba01d13c071081d87a711aa	no	12
Warnings:					
Information:					
		Total Files Size (in bytes):	616983		

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-1390 (03-13)
Approved for use through 4/30/2013. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	U.S. Application No. (if known, see 37 CFR 1.5)
P41624US/45631-225521	13/997,412

International Application No.	International Filing Date	Priority Date Claimed
PCT/US2011/065069	15 December 2011 (15.12.11)	15 December 2011 (15.12.11)

Title of Invention
METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

First Named Inventor
KHOSRAVI, Hormuzd M., et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☑ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.
2. ☐ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☑ is attached.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☐ A preliminary amendment.
11. ☐ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☐ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
15. ☐ Assignment papers *(cover sheet and document(s))*. Name of Assignee: _____
16. ☐ 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

PTO-1390 (03-13)
Approved for use through 4/30/2013. OMB 0651-0021
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.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
13/997,412	PCT/US2011/065069	P41624US/45631-225521

17. ☑ Other items or information:

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following fees have been submitted.	CALCULATIONS	PTO USE ONLY
18. ☐ Basic national fee (37 CFR 1.492(a)) **$280**	$	
19. ☐ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** All other situations **$720**	$	
20. ☐ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$120** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB ..... **$480** All other situations **$600**	$	
TOTAL OF 18, 19, and 20 =	$ 0.00	
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$400**		

Total Sheets	Extra Sheets	Number of each addition 50 or fraction thereof (round **up** to a whole number)	RATE	
- 100 =	/ 50 =		x **$400**	$

Surcharge of **$140.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	- 20 =		x **$80**	$	
Independent claims	- 3 =		x **$420**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$780**	$	
Processing fee of **$140.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)).			**+**	$	
TOTAL OF ABOVE CALCULATIONS =				$ 0.00	
☑ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.					
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =				$ 0.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property.			**+**	$	
TOTAL FEES ENCLOSED =				$ 0.00	
				Amount to be refunded:	$
				Amount to be charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

c. ☑ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 50-4238 as follows:

i. ☐ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File)Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☑ The address associated with Customer Number: 73486 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country			Telephone		
Email					

Signature	/Christopher A. SINGH/	Date	2014-04-03
Name (Print/Type)	Christopher A. SINGH	Registration No. (Attorney/Agent)	61236

Electronic Acknowledgement Receipt	
EFS ID:	16431576
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:	Christopher A. Singh/Jenny Kathman
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	26-JUL-2013
Filing Date:	
Time Stamp:	17:34:18
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)	P41624US_IDS.pdf	612529 d1252053a2f5862f53cab17042ff94031ea243fa	no	4

Warnings:
Information:

2	Foreign Reference	FR1.pdf	1414117 2001cf96b8116eb778bdc2ed624e2199833dedb9	no	31
Warnings:					
Information:					
3	Non Patent Literature	NPL1.pdf	403207 55c54ca63faa05b6910359efa1077d8c913180d6	no	11
Warnings:					
Information:					
4	Non Patent Literature	NPL2.pdf	3104183 08aea302b1c155c2b18eeea6cca27818f8699a78	no	19
Warnings:					
Information:					
5	Non Patent Literature	NPL3.pdf	919669 0b6a539cc93664667a9281043edd26694e2e1922	no	6
Warnings:					
Information:					
		Total Files Size (in bytes):	6453705		

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/997,412	Hormuzd M. Khosravi	P41624US

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

INTERNATIONAL APPLICATION NO.	
PCT/US11/65069	
I.A. FILING DATE	PRIORITY DATE
12/15/2011	

CONFIRMATION NO. 1045
371 FORMALITIES LETTER

OC000000062743010

Date Mailed: 07/23/2013

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated Office (37 CFR 1.494):

- Copy of the International Application filed on 06/24/2013
- Copy of the International Search Report filed on 06/24/2013
- Oath or Declaration filed on 06/24/2013
- U.S. Basic National Fees filed on 06/24/2013

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
  - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
  - Inventor Kabir has not signed OATH

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

FORM PCT/DO/EO/905 (371 Formalities Notice)

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

BRIAN A HARDEN

Telephone: (703) 756-1815

FORM PCT/DO/EO/905 (371 Formalities Notice)

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/997,412

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	480
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20 =	* 4			OR	x 80 =	320
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00
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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1800

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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 found in the appropriate box in column 1.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET Substitute for Form PTO-1360 (For use with Form PTO/SB/06)	Application Number 13997412	Filing Date
	Applicant(s) Hormuzd Khosravi	
	* May be used for additional claims or amendments	

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		---	---		
2		1	---	---		
3		1	---	---		
4		1	---	---		
5		1	---	---		
6		1	---	---		
7		1	---	---		
8		1	---	---		
9		1	---	---		
10		1	---	---		
11		1	---	---		
12		1	---	---		
13		1	---	---		
14		1	---	---		
15		1	---	---		
16	1		---	---		
17		1	---	---		
18		1	---	---		
19		1	---	---		
20		1	---	---		
21		1	---	---		
22		1	---	---		
23		1	---	---		
24		1	---	---		
25		1	---	---		
26		1	---	---		
27		1	---	---		
28		1	---	---		
29		1	---	---		
30		1	---	---		
31		1	---	---		
32		1	---	---		
33		1	---	---		
34		1	---	---		
35		29	---	---		
36		29	---	---		
37	1		---	---		
38		1	---	---		
39		1	---	---		
40		1	---	---		
41		1	---	---		
42		1	---	---		
43		1	---	---		
44		1	---	---		
45		1	---	---		
46		9	---	---		
47		9	---	---		
48			1			
49				1		
50				1		
Total Indep	3		3		0	
Total Depend	116	↵	21	↵	0	↵
Total Claims	119		24		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51				1		
52				1		
53				1		
54				1		
55				1		
56			1			
57				1		
58				1		
59				1		
60				1		
61				1		
62				1		
63				1		
64			1			
65				1		
66				1		
67				1		
68				1		
69				1		
70				1		
71				1		
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

PTO-1390 (03-13)
Approved for use through 4/30/2013. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	U.S. Application No. (if known, see 37 CFR 1.5)
P41624US	New Application

International Application No.	International Filing Date	Priority Date Claimed
PCT/US2011/065069	December 15, 2011	December 15, 2011

Title of Invention
METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

First Named Inventor
Hormuzd M. Khosravi

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☑ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.
2. ☑ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☑ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☐ is attached.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☑ A preliminary amendment.
11. ☑ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☐ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
15. ☐ Assignment papers *(cover sheet and document(s))*. Name of Assignee: _____
16. ☐ 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

PTO-1390 (03-13)
Approved for use through 4/30/2013. OMB 0651-0021
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.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
New Application	PCT/US2011/065069	P41624US

17. ☑ Other items or information:

International Search Report and Written Opinion

The following fees have been submitted.	CALCULATIONS	PTO USE ONLY
18. ☑ Basic national fee (37 CFR 1.492(a)) **$280**	$ 280	
19. ☑ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** All other situations **$720**	720 $	
20. ☑ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$120** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB ..... **$480** All other situations **$600**	480 $	
TOTAL OF 18, 19, and 20 =	$ 1480	
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$400**	$	
Total Sheets: - 100 = / Extra Sheets: / 50 = / Number of each addition 50 or fraction thereof (round **up** to a whole number): / RATE: x **$400**	$	
Surcharge of **$140.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	24 - 20 =	4	x **$80**	$ 320	
Independent claims	3 - 3 =		x **$420**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$780**	$	
Processing fee of **$140.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). +				$	
TOTAL OF ABOVE CALCULATIONS =				$ 320	
☐ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.					
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =				$ 1800	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property. +				$	
TOTAL FEES ENCLOSED =				$ 1800	
				Amount to be refunded:	$
				Amount to be charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☑ Please charge my Deposit Account No. 504238 in the amount of $ 1800 to cover the above fees.

c. ☑ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 504238 as follows:

i. ☑ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File)Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☑ The address associated with Customer Number: 73486 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country			Telephone		
Email					

Signature	/Glen M. Kellett, Reg No. 60202/	Date	June 19, 2013
Name (Print/Type)	Glen M. Kellett	Registration No. (Attorney/Agent)	60,202

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.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	TBD
Applicant	:	Hormuzd M. Khosravi et al.
International Filing Date	:	December 15, 2011
TC/A.U.	:	TBD
Examiner	:	TBD

Docket No. : P41624US
Customer No. : 73486

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

PRELIMINARY AMENDMENT

SIR:

Please consider the above-identified application (the "Patent Application") in view of the following preliminary amendments and remarks.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claims 1-47 (Canceled)

48. (New) 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, 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;

perform a cryptographic key exchange with the 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;

store the session key in the secure memory,

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

49. (New) 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.

50. (New) 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.

MediaTek Exhibit 1012, Page 368 of 463

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

52. (New) The system-on-a-chip apparatus of claim 50, wherein the security engine 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 server.

53. (New) The system-on-a-chip apparatus of claim 48, 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.

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

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

56. (New) 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 server over a network, the request including the random nonce;

MediaTek Exhibit 1012, Page 369 of 463

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

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

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

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

receiving a ServerHello message from the 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. (New) The method of claim 56, wherein performing the cryptographic key exchange with the server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

59. (New) 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 storage of the security engine of the system-on-a-chip.

MediaTek Exhibit 1012, Page 370 of 463

60. (New) The method of claim 58, wherein performing the cryptographic key exchange with the 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. (New) 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 server.

62. (New) The method of claim 56, wherein performing the cryptographic key exchange with the 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 a security key of the security engine of the system-on-a-chip;

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

receiving a public Diffie-Hellman server key from the 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. (New) 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 server;

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.

MediaTek Exhibit 1012, Page 371 of 463

64. (New) One or more 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 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 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;

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

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

65. (New) The one or more 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 server; and wherein the plurality of instructions further cause the computing device to:

receive a ServerHello message from the 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. (New) The one or more machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate a pre-master key in the security engine;

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

send the encrypted pre-master key to the server.

MediaTek Exhibit 1012, Page 372 of 463

67. (New) The one or more 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 storage of the security engine of the system-on-a-chip.

68. (New) The one or more machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the 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. (New) The one or more 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 server.

70. (New) The one or more machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the 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 a security key of the security engine of the system-on-a-chip;

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

receive a public Diffie-Hellman server key from the 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.

MediaTek Exhibit 1012, Page 373 of 463

71. (New) The one or more 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 server;

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

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

MediaTek Exhibit 1012, Page 374 of 463

REMARKS

These amendments and remarks are set forth prior to examination. Claims 1-47 have been cancelled. Claims 48-71 new claims have been added. Favorable consideration and allowance of the pending claims are respectfully requested.

MediaTek Exhibit 1012, Page 375 of 463

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (317) 261-7959 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-4238.

Respectfully submitted,

Barnes & Thornburg LLP

CUSTOMER NO. 73486

/Glen M. Kellett, Reg No. 60202/

Date: June 20, 2013

Glen M. Kellett
Registration No. 60,202
Barnes & Thornburg LLP
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 261-7959
Fax: (317) 231-7433

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

BACKGROUND

Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

MediaTek Exhibit 1012, Page 377 of 463

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to "one embodiment," "an embodiment," "an example embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

MediaTek Exhibit 1012, Page 378 of 463

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages. Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

MediaTek Exhibit 1012, Page 379 of 463

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

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.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11standard), and/or other communication protocols or standards.

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104, and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

MediaTek Exhibit 1012, Page 383 of 463

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization, which acts as a third-party verifier of the authentication of the server 104. The server certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a "ServerHelloDone" message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the "master" key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

MediaTek Exhibit 1012, Page 388 of 463

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

In block 410, the client device 102 completes the server authentication and server key exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

MediaTek Exhibit 1012, Page 389 of 463

However, if the server 104 is successfully authenticated, the method 400 advances to bock 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device key.

In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to bock 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. 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, 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;

perform a cryptographic key exchange with the 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;

store the session key in the secure memory,

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

2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip to establish a Secure Sockets Layer communication session with the server over the network using the session key.

3. The system-on-a-chip apparatus of claim 1, 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.

4 The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.

5 The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.

6. The system-on-a-chip apparatus of claim 5, 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.

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.

8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.

11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.

12. The system-on-a-chip apparatus of claim 11, 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.

13. The system-on-a-chip apparatus of claim 12, wherein the security engine to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

14. The system-on-a-chip apparatus of claim 13, wherein the security engine to use the session key to encrypt a subsequent message sent from the client device to the server.

15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

16. 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 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 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;

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

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

17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.

18. The method of claim 16, further comprising:

receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and

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

19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:

receiving a ServerHello message from the 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.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.

21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

23. The method of claim 22, 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 storage of the security engine of the system-on-a-chip.

24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

25. The method of claim 24, 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 server.

26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

receiving a public Rivest-Shamir-Adleman server key from the server; and

storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

MediaTek Exhibit 1012, Page 395 of 463

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the 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 a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key exchange with the server comprises:

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

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.

30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, 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 server;

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.

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key; and

sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device performing the method of claims 16-34.

37. 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 Sockets Layer communication session with a 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 server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer communication session;

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

generating, in the security engine, a hash code as a function of the session key; and

sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

40. The method of claim 39, further comprising:

wrapping the pre-master key in the security engine using a server public key, and

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

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

42. The method of claim 41, 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 server.

43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the 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 a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

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

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.

46. A source device comprising:

a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

ABSTRACT OF THE DISCLOSURE

A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SLL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

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	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Hormuzd	M.	Khosravi	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Portland	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	4816 NW 166th Avenue		
Address 2			
City	Portland	State/Province	OR
Postal Code	97229	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Edward	C.	Epp	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Hillsboro	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	2111 NE 25th Avenue		
Address 2			
City	Portland	State/Province	OR
Postal Code	97124	Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Farhana		Kabir	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

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	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

City	Camas	State/Province	WA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	20021 SE 3rd Circle		
Address 2			
City	Camas	State/Province	WA
Postal Code	98607	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	73486		
Email Address	inteldocs@cpaglobal.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
Attorney Docket Number	P41624US	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)

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	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

Customer Number	73486

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/US2011/065069	2011-12-15

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

Authorization to Permit Access:

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	
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

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	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE	

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
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

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	
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					
Signature	/Glen M. Kellett, Reg No. 60202/			Date (YYYY-MM-DD)	2013-06-19
First Name	Glen M.	Last Name	Kellett	Registration Number	60202

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.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd Khosravi
Filer:	Glen Madison Kellett/Dannel Johnson
Attorney Docket Number:	P41624US

Filed as Large Entity

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
National Stage Fee	1631	1	280	280
Natl Stage Search Fee - Report provided	1642	1	480	480
National Stage Exam - all other cases	1633	1	720	720
Pages:				
Claims:				
Claims in excess of 20	1615	4	80	320
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		1800

Electronic Acknowledgement Receipt	
EFS ID:	16093266
Application Number:	13997412
International Application Number:	PCT/US11/65069
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 Khosravi
Customer Number:	73486
Filer:	Glen Madison Kellett/Dannel Johnson
Filer Authorized By:	Glen Madison Kellett
Attorney Docket Number:	P41624US
Receipt Date:	24-JUN-2013
Filing Date:	
Time Stamp:	14:27:46
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	$1800
RAM confirmation Number	753
Deposit Account	504238
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	P41624PCT_FIGS.pdf	48349 066ff196ae2b2be216e2877db1a79ae2be583a1a	no	4
Warnings:					
Information:					
2	Documents submitted with 371 Applications	P41624PCT_ISR.pdf	567205 d2d8afdc945eb595a9cabeec581af1f7a18c65c2	no	11
Warnings:					
Information:					
3	Transmittal of New Application	P41624US_1390.pdf	222264 eeb40af8b3adb7b887f299d2f6ec8bf8609d6c6c	no	4
Warnings:					
Information:					
4		P41624US_Preliminary_Amendment.pdf	35221 6ff8b5a23b35f42d1a9fad3fe4870a1a1242a656	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	8
Applicant Arguments/Remarks Made in an Amendment	9	10

Warnings:					
Information:					
5		P41624PCT_APPLN_Use.pdf	120430 434175b9358a0acc7296db74864c2f3934cf40be	yes	25

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	15
Claims	16	24

	Abstract		25	25	
Warnings:					
Information:					
6	Application Data Sheet	P41624US_ADS.pdf	1503119 b7b6e86a89c6ce56c7df8790ae51569e3da0d940	no	7
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	36958 d3fadccf2239f543a216daf67a214dd5a9ef5ad0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2533546		

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.

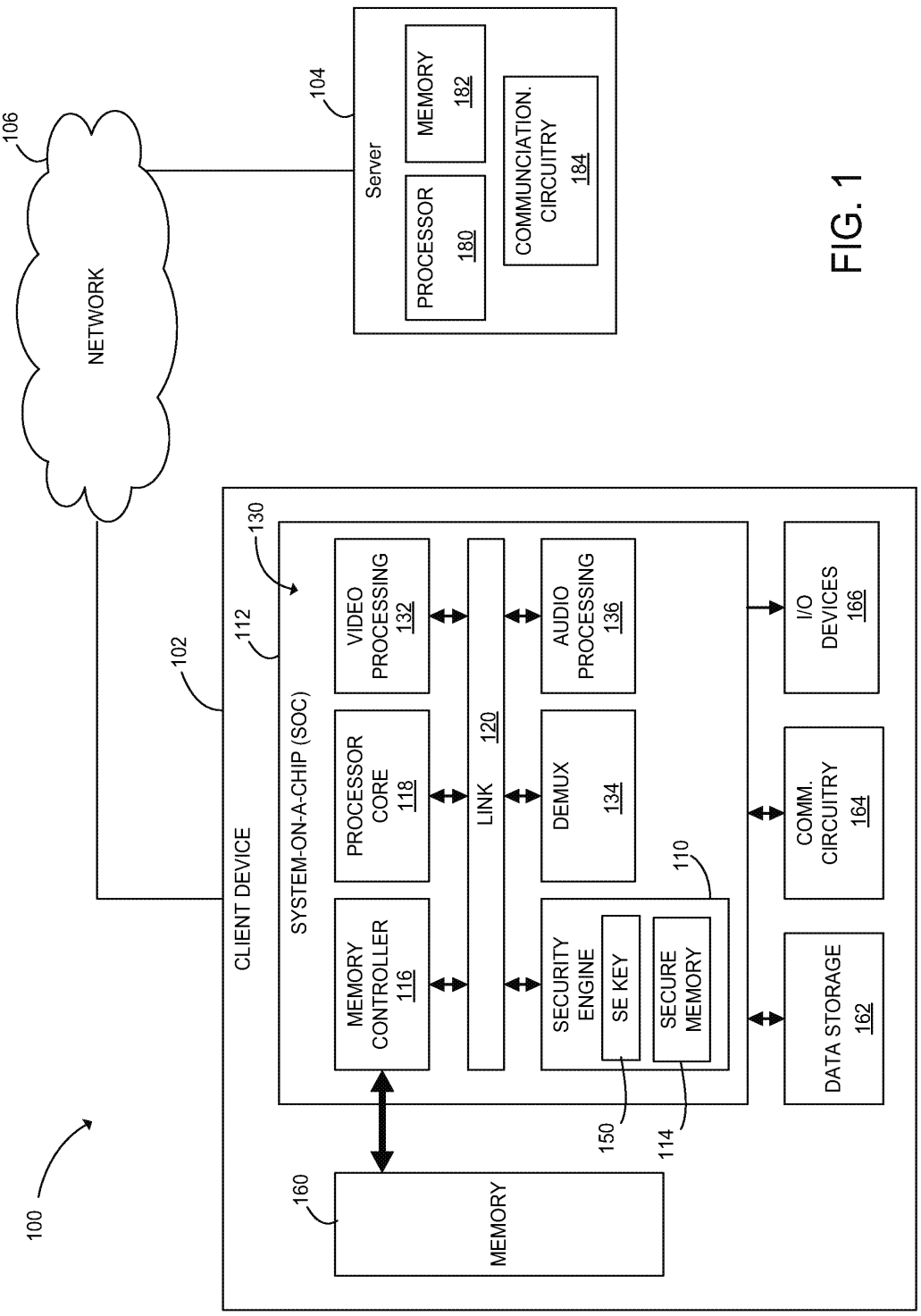

100
106
NETWORK
104
Server
MEMORY 182
PROCESSOR 180
COMMUNCIATION. CIRCUITRY 184
102
CLIENT DEVICE
112
SYSTEM-ON-A-CHIP (SOC)
130
VIDEO PROCESSING 132
AUDIO PROCESSING 136
PROCESSOR CORE 118
LINK 120
DEMUX 134
MEMORY CONTROLLER 116
SECURITY ENGINE
SE KEY
SECURE MEMORY
110
150
114
160
MEMORY
I/O DEVICES 166
COMM. CIRCUITRY 164
DATA STORAGE 162

FIG. 1

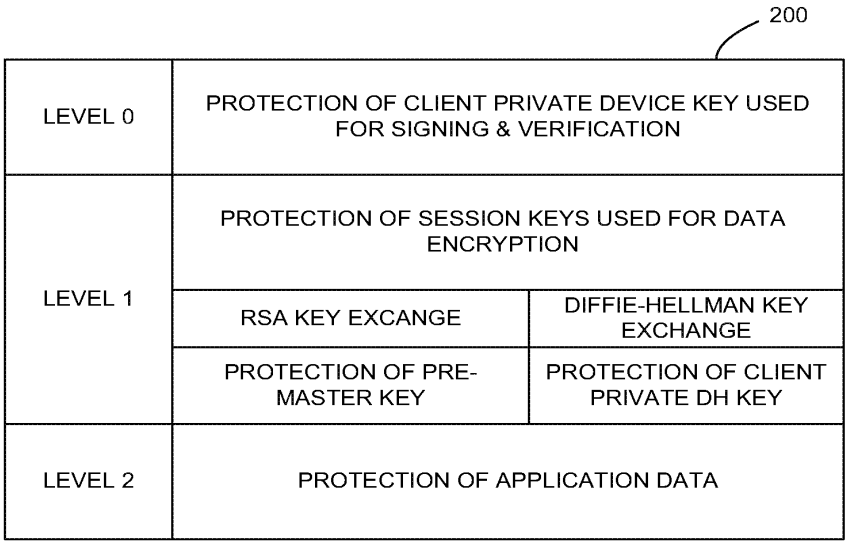

200
LEVEL 0
PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION
LEVEL 1
PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION
RSA KEY EXCANGE
DIFFIE-HELLMAN KEY EXCHANGE
PROTECTION OF PRE-MASTER KEY
PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2
PROTECTION OF APPLICATION DATA

FIG. 2

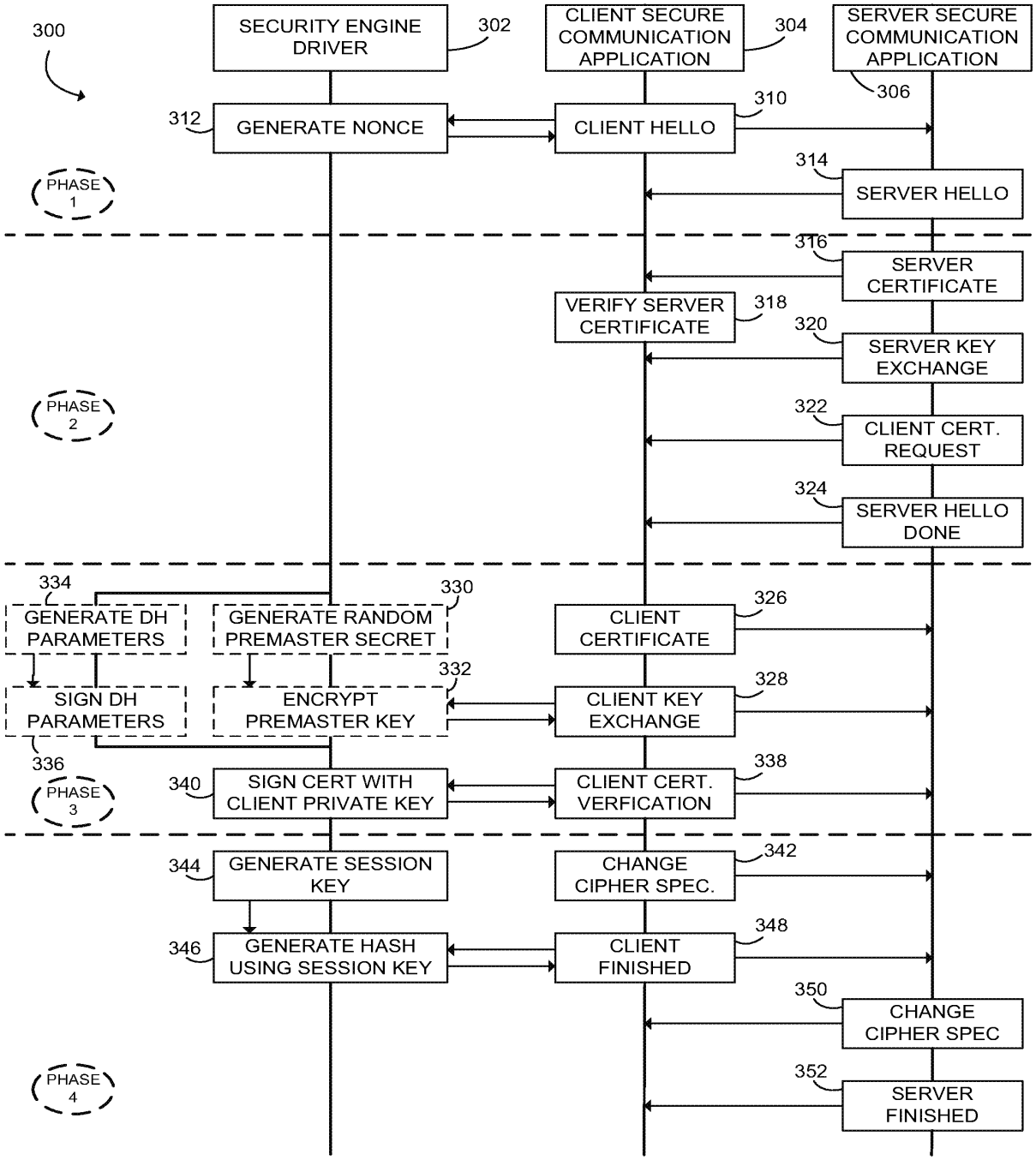

300
SECURITY ENGINE DRIVER
302
CLIENT SECURE COMMUNICATION APPLICATION
304
SERVER SECURE COMMUNICATION APPLICATION
306
312
GENERATE NONCE
CLIENT HELLO
310
314
SERVER HELLO
PHASE 1
316
SERVER CERTIFICATE
VERIFY SERVER CERTIFICATE
318
320
SERVER KEY EXCHANGE
PHASE 2
322
CLIENT CERT. REQUEST
324
SERVER HELLO DONE
334
GENERATE DH PARAMETERS
330
GENERATE RANDOM PREMASTER SECRET
CLIENT CERTIFICATE
326
332
SIGN DH PARAMETERS
ENCRYPT PREMASTER KEY
CLIENT KEY EXCHANGE
328
336
PHASE 3
340
SIGN CERT WITH CLIENT PRIVATE KEY
CLIENT CERT. VERFICATION
338
344
GENERATE SESSION KEY
CHANGE CIPHER SPEC.
342
346
GENERATE HASH USING SESSION KEY
CLIENT FINISHED
348
350
CHANGE CIPHER SPEC
PHASE 4
352
SERVER FINISHED

FIG. 3

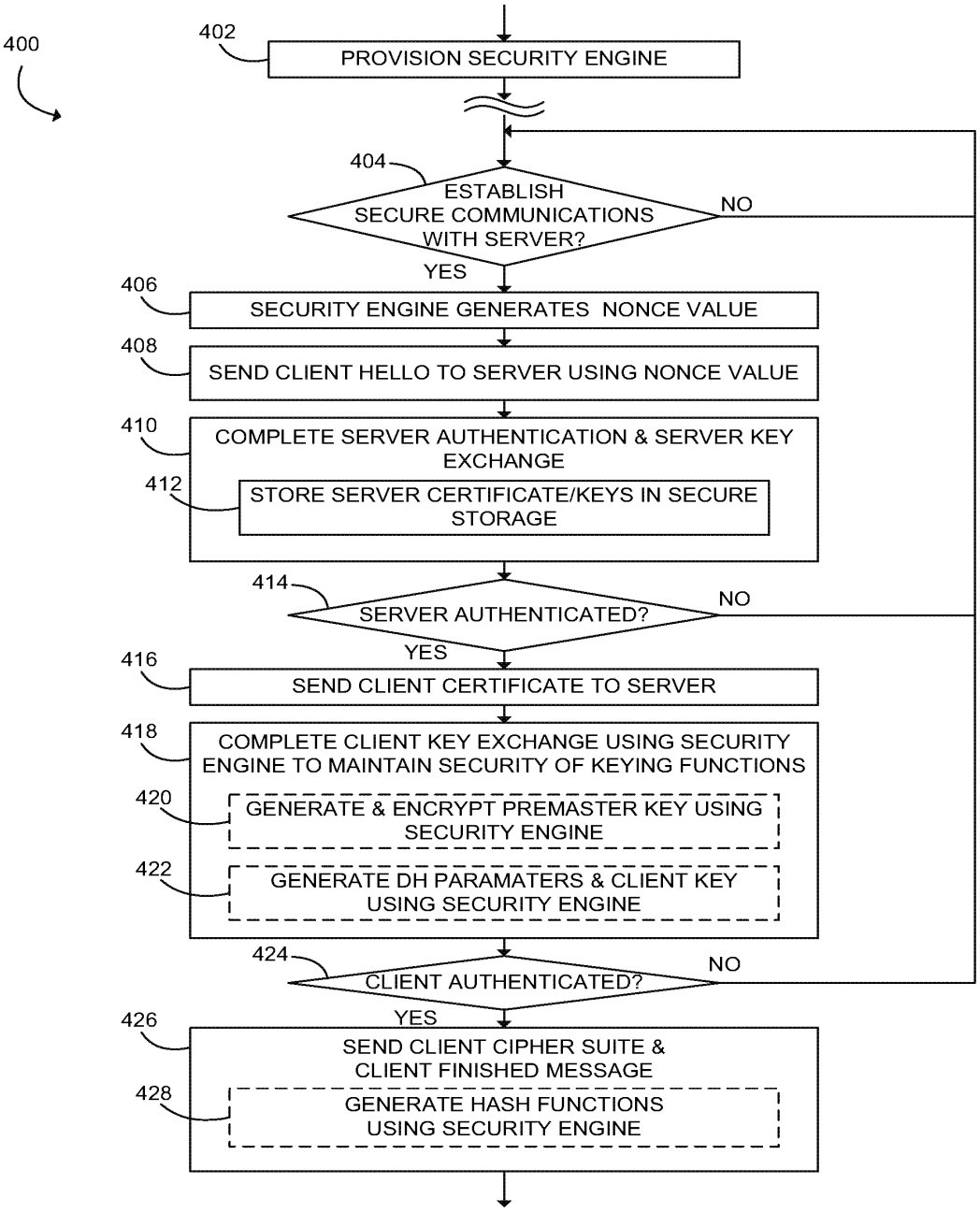

400
402
PROVISION SECURITY ENGINE
404
ESTABLISH SECURE COMMUNICATIONS WITH SERVER?
NO
YES
406
SECURITY ENGINE GENERATES NONCE VALUE
408
SEND CLIENT HELLO TO SERVER USING NONCE VALUE
410
COMPLETE SERVER AUTHENTICATION & SERVER KEY EXCHANGE
412
STORE SERVER CERTIFICATE/KEYS IN SECURE STORAGE
414
SERVER AUTHENTICATED?
NO
YES
416
SEND CLIENT CERTIFICATE TO SERVER
418
COMPLETE CLIENT KEY EXCHANGE USING SECURITY ENGINE TO MAINTAIN SECURITY OF KEYING FUNCTIONS
420
GENERATE & ENCRYPT PREMASTER KEY USING SECURITY ENGINE
422
GENERATE DH PARAMATERS & CLIENT KEY USING SECURITY ENGINE
424
CLIENT AUTHENTICATED?
NO
YES
426
SEND CLIENT CIPHER SUITE & CLIENT FINISHED MESSAGE
428
GENERATE HASH FUNCTIONS USING SECURITY ENGINE

FIG. 4

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O. BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)* 30 AUGUST 2012 (30.08.2012)	
Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No **PCT/US2011/065069**	International filing date *(day/month/year)* **15 DECEMBER 2011 (15.12.2011)**
Applicant **INTEL CORPORATION et al**	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 . 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer COMMISSIONER Telephone No. 82-42-481-8754

CPA GLOBAL SEP 11 2012

RECEIVED Coded Verified

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

http://www.kipo.go.kr/en/ => PCT Services => PCT Services

ID : PCT international application number
PW : **CZKLKWRL**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: http://www.ipkcenter.com
Email: ipkc@ipkcenter.com
Phone: +1 703 388 1066
Fax: +1 703 388 1084

Notes to Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
P41624PCT		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2011/065069	**15 DECEMBER 2011 (15.12.2011)**	

Applicant

INTEL CORPORATION et al

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of :
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065069

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01)i, H04L 9/32(2006.01)i

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)
H04L 9/14; H04L 9/08; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: secure communication, secure socket layer, SSL, transport layer security, IPSec, random nonce, handshake initiate, key exchange, session key, secure memory, hash code, handshake completion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0231923 A1 (ROLLAY SENN SAPIN et al.) 22 September 2011 See Claims 1,6; Paragraphs [27],[62],[70],[89]-[93],[95],[123]-[126]; Figures 2,5,8	1-32,35-36 33-34,37-47
Y	US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005 See Claims 1-4; Paragraphs [14],[15],[17],[20],[21],[26],[28],[33],[45],[49], [53],[54]; Figures 1,2,5	1-32,35-36 33-34,37-47
A	US 2010-0296525 A1 (SHAH PARAS et al.) 25 November 2010 See Claims 1,8; Paragraphs [47],[50],[54]-[56],[59],[60]; Figures 2,3	1-47
A	US 2008-0037793 A1 (BUER MARK) 14 February 2008 See Claims 11-17; Paragraphs [35],[39]-[43]; Figures 4,7-9	1-47

☐ Further documents are listed in the continuation of Box C. ☒ See patent family 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 application or patent 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 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
29 AUGUST 2012 (29.08.2012)	**30 AUGUST 2012 (30.08.2012)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea	Lee Hyoung Il
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-8199

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2011/065069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0231923 A1	22.09.2011	CN 102195878 A	21.09.2011
		US 2011-231649 A1	22.09.2011
		US 2011-231651 A1	22.09.2011
		US 2011-231652 A1	22.09.2011
		US 2011-231653 A1	22.09.2011
		US 2011-231655 A1	22.09.2011
		WO 2011-116342 A2	22.09.2011
		WO 2011-116342 A3	22.12.2011
US 2005-0213768 A1	29.09.2005	CN 1926837 A	07.03.2007
		CN 1926837 B	06.04.2011
		EP 1728376 A1	06.12.2006
		EP 1728376 B1	15.07.2009
		JP 04-579969 B2	03.09.2010
		JP 2007-525913 A	06.09.2007
		JP 4579969 B2	10.11.2010
		KR 10-0831437 B1	21.05.2008
		KR 10-2006-0127229 A	11.12.2006
		WO 2005-101794 A1	27.10.2005
US 2010-0299525 A1	25.11.2010	AU 2006-280301 A1	22.02.2007
		CN 101292233 A0	22.10.2008
		EP 1904931 A2	02.04.2008
		JP 2009-505493 A	05.02.2009
		US 2007-0038853 A1	15.02.2007
		US 2009-0119504 A1	07.05.2009
		WO 2007-021483 A2	22.02.2007
US 2008-0037793 A1	14.02.2008	EP 1484890 A2	08.12.2004
		EP 1484890 A3	11.07.2012
		EP 1484913 A2	08.12.2004
		EP 1484913 A3	15.04.2009
		US 2004-0247131 A1	09.12.2004
		US 2005-0041802 A1	24.02.2005
		US 2010-0296573 A1	25.11.2010
		US 6724335 B1	20.04.2004
		US 7289632 B2	30.10.2007
		US 7768434 B2	03.08.2010
		US 8111183 B2	07.02.2012

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O.
BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)* **30 AUGUST 2012 (30.08.2012)**

Applicant's or agent's file reference
P41624PCT

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2011/065069	**15 DECEMBER 2011 (15.12.2011)**	

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

H04L 9/14(2006.01)i, H04L 9/32(2006.01)i

Applicant

INTEL CORPORATION et al

1. This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [X] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	29 AUGUST 2012 (29.08.2012)	Lee Hyoung Il Telephone No.82-42-481-8199

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No
PCT/US2011/065069

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioant copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/065069

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-47	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	33-34,37-47	YES
	Claims	1-32,35-36	NO
Industrial applicability (IA)	Claims	1-47	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011
D2: US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005
D3: US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010
D4: US 2008-0037793 A1 (BUER MARK) 14 February 2008

1. Novelty and Inventive Step

1.1 Independent Claim 1

D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses an apparatus for a client to generate random number, send client hello message for SSL handshake initiation, perform a server key exchange and a client key exchange, generate a session key based on secret data, store the session in a data store, establish an encrypted session between the server and the client using the session key. Claim 1 differs from D1 in that the apparatus uses the secure memory. However, D2 discloses an apparatus storing the cryptographic key in a secure storage. Accordingly, claim 1 would have been obvious over D1 in view of D2. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.2 Dependent Claims 2-15

Claims 2-15, which are dependent on claim 1, lack an inventive step under PCT Article 33(3), because the additional features of claims 2-15 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.3 Independent Claim 16

Claim 16 relates to a method performing the functions of the apparatus according to claim 1. Claim 16 is considered to lack an inventive step under PCT Article 33(3), because the subject matter of claim 1 is considered to lack an inventive step under PCT Article 33(3).

[Continued on Supplemental Box]

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/065069

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 35-36 and 46-47 do not comply with PCT Rule 6.4(a) because the multiple dependent claims don't refer to other claims in the alternative way.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

[Box V]
[Box V]

1.4 Dependent Claims 17-32

Claims 17-32, which are dependent on claim 16, lack an inventive step under PCT Article 33(3), because the additional features of claims 17-32 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.5 Dependent Claims 33-34

The additional feature of claim 33 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 33 is novel and involves an inventive step under PCT Article 33(2) and (3).

The additional feature of claim 34 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 34 is novel and involves an inventive step under PCT Article 33(2) and (3).

1.6 Independent Claim 35

Claim 35 relates to a source device including a plurality of instructions performing the method of claims 16-32. Claim 35 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.7 Independent Claim 36

Claim 36 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 16-32. Claim 36 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.8 Claims 37-45

The subject matter of claim 37 differs from these prior art documents in generating a hash code as a function of the session key and sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 37 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 38-45 are dependent on claim 37 and therefore meet the requirements of PCT Article 33(2) and (3).

1.9 Claims 46-47

Claim 46 relates to a source device including a plurality of instructions performing the method of claims 37-45. Claim 46 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Claim 47 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 37-45. Claim 47 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

[Continued on Supplemental Box]

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of :

[Box V]

2. Industrial Applicability

Claims 1-47 are industrially applicable under PCT Article 33(4).

Box No. VIII (iv) DECLARATION: INVENTORSHIP (only for the purposes of the designation of the United States of America)
The declaration must conform to the following standardized wording provided for in Section 214; see Notes to Boxes Nos. VIII, VIII (i) to (v) (in general) and the specific Notes to Box No. VIII (iv). If this Box is not used, this sheet should not be included in the request.

Declaration of Inventorship (Rules 4.17(iv) and 51*bis*.1(a)(iv))
for the purposes of the designation of the United States of America:

I hereby declare that I believe I am the original, first and sole (if only one inventor is listed below) or joint (if more than one inventor is listed below) inventor of the subject matter which is claimed and for which a patent is sought.

This declaration is directed to the international application of which it forms a part (if filing declaration with application).

This declaration is directed to international application No. PCT/ PCT/US2011/065069 (if furnishing declaration pursuant to Rule 26*ter*).

I hereby declare that my residence, mailing address, and citizenship are as stated next to my name.

I hereby state that I have reviewed and understand the contents of the above-identified international application, including the claims of said application. I have identified in the request of said application, in compliance with PCT Rule 4.10, any claim to foreign priority, and I have identified below, under the heading "Prior Applications," by application number, country or Member of the World Trade Organization, day, month and year of filing, any application for a patent or inventor's certificate filed in a country other than the United States of America, including any PCT international application designating at least one country other than the United States of America, having a filing date before that of the application on which foreign priority is claimed.

Prior Applications:

I hereby acknowledge the duty to disclose information that is known by me to be material to patentability as defined by 37 C.F.R. § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the PCT international filing date of the continuation-in-part application.

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

Name: KHOSRAVI, Hormuzd, M.

Residence: Portland, OR
(city and either US state, if applicable, or country)

Mailing Address: ~~4016 NW 106th Ave~~ 4733 NW Rainier Ter Unit, Portland, OR, US 97229

Citizenship: India

Inventor's Signature: Unit Date: 2-22-2012
(The signature must be that of the inventor, not that of the agent)

Name: EPP, Edward, C.

Residence: Hillsboro, OR
(city and either US state, if applicable, or country)

Mailing Address: ~~2111 NE 25th Ave, Hillsboro, OR, US 97124~~ ECE
3035 NE 23rd Av., Portland, OR 97212

Citizenship: United States of America

Inventor's Signature: Edward C Epp Date: 2-22-2012
(The signature must be that of the inventor, not that of the agent)

☐ This declaration is continued on the following sheet, "Continuation of Box No. VIII (iv)".

PCT REQUEST

Original (for **SUBMISSION**)

0	**For receiving Office use only**	
0-1	International Application No.	PCT/US11/65069
0-2	International Filing Date	15 DEC 2011 (15.12.11)
0-3	Name of receiving Office and "PCT International Application"	PCT INTERNATIONAL APPLICATION RO/US

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT-SAFE [EASY/EFS-Web mode] Version 3.51.051.227 MT/FOP 20111001/0.20.5.19
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	United States Patent and Trademark Office (USPTO) (RO/US)
0-7	**Applicant's or agent's file reference**	P41624PCT
I	**Title of Invention**	METHOD AND DEVICE FOR SECURE COMMUNI-CATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States except US
II-4	Name	INTEL CORPORATION
II-5	Address	2200 Mission College Boulevard Santa Clara, California 95052 United States of America
II-6	State of nationality	US
II-7	State of residence	US
II-8	Telephone No.	317-236-1313
II-10	e-mail	docketing@cpaglobal.com
II-10(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	as advance copies followed by paper notifications

PCT REQUEST

Original (for **SUBMISSION**)

III-1	**Applicant and/or inventor**	
III-1-1	This person is	Applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	KHOSRAVI, Hormuzd M.
III-1-5	Address	4816 NW 166th Avenue Portland, Oregon 97229 United States of America
III-1-6	State of nationality	IN
III-1-7	State of residence	US
III-2	**Applicant and/or inventor**	
III-2-1	This person is	Applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	EPP, Edward C.
III-2-5	Address	2111 NE 25th Avenue Hillsboro, Oregon 97124 United States of America
III-2-6	State of nationality	US
III-2-7	State of residence	US
III-3	**Applicant and/or inventor**	
III-3-1	This person is	Applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	KABIR, Farhana
III-3-5	Address	20021 SE 3rd Circle Camas, Washington 98607 United States of America
III-3-6	State of nationality	US
III-3-7	State of residence	US

PCT REQUEST

Original (for **SUBMISSION**)

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent	
IV-1-1	Name (LAST, First)	KELLETT, Glen M.	
IV-1-2	Address	Barnes & Thornburg, LLP c/o CPA Global P.O. Box 52050 Minneapolis, Minnesota 55402 United States of America	
IV-1-3	Telephone No.	317-236-1313	
IV-1-5	e-mail	docketing@cpaglobal.com	
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	as advance copies followed by paper notifications	
IV-1-6	Agent's registration No.	60202	
V	**DESIGNATIONS**		
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**		
VI-1	**Priority Claim**	NONE	
VII-1	**International Searching Authority Chosen**	Korean Intellectual Property Office (ISA/KR)	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	–	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	–	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	–	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	–	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	–	

PCT REQUEST

Original (for **SUBMISSION**)

IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	15	–
IX-3	Claims	9	–
IX-4	Abstract	1	✓
IX-5	Drawings	4	–
IX-7	TOTAL	33	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	✓	–
IX-19	Other	PCT Transmittal	
IX-19	Other	PCT Transmittal	
IX-20	**Figure of the drawings which should accompany the abstract**	1	
IX-21	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	/Glen M. Kellet, Reg No. 60202/	
X-1-1	Name (LAST, First)	KELLETT, Glen M.	
X-1-2	Name of signatory		
X-1-3	Capacity (if such capacity is not obvious from reading the request)		

FOR RECEIVING OFFICE USE ONLY 15-12-2011

10-1	**Date of actual receipt of the purported international application**	15 DEC 2011 (15.12.11)
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/KR
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 June 2013 (20.06.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/089725 A1

(51) International Patent Classification:
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2011/065069

(22) International Filing Date:
15 December 2011 (15.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KHOSRAVI, Hormuzd M.** [IN/US]; 4816 NW 166th Avenue, Portland, Oregon 97229 (US). **EPP, Edward C.** [US/US]; 2111 NE 25th Avenue, Hillsboro, Oregon 97124 (US). **KABIR, Farhana** [US/US]; 20021 SE 3rd Circle, Camas, Washington 98607 (US).

(74) Agent: **KELLETT, Glen M.**; Barnes & Thornburg, LLP, c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

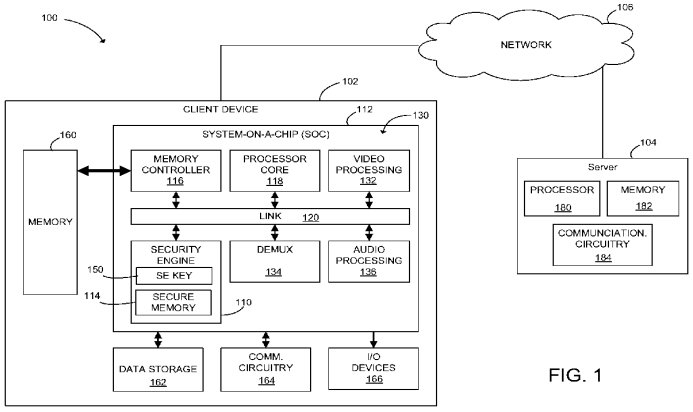


FIG. 1

(57) **Abstract**: A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SLL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

WO 2013/089725 A1

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

BACKGROUND

Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

MediaTek Exhibit 1012, Page 435 of 463

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to "one embodiment," "an embodiment," "an example embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

MediaTek Exhibit 1012, Page 436 of 463

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages. Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

MediaTek Exhibit 1012, Page 437 of 463

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

MediaTek Exhibit 1012, Page 438 of 463

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

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.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

MediaTek Exhibit 1012, Page 439 of 463

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11standard), and/or other communication protocols or standards.

MediaTek Exhibit 1012, Page 440 of 463

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104, and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

MediaTek Exhibit 1012, Page 441 of 463

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

MediaTek Exhibit 1012, Page 442 of 463

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization, which acts as a third-party verifier of the authentication of the server 104. The server certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a "ServerHelloDone" message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

MediaTek Exhibit 1012, Page 444 of 463

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the "master" key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

MediaTek Exhibit 1012, Page 445 of 463

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

MediaTek Exhibit 1012, Page 446 of 463

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

In block 410, the client device 102 completes the server authentication and server key exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

MediaTek Exhibit 1012, Page 447 of 463

However, if the server 104 is successfully authenticated, the method 400 advances to bock 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device key.

In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to bock 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

MediaTek Exhibit 1012, Page 448 of 463

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

MediaTek Exhibit 1012, Page 449 of 463

CLAIMS:

1. 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, 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;

perform a cryptographic key exchange with the 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;

store the session key in the secure memory,

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

2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip to establish a Secure Sockets Layer communication session with the server over the network using the session key.

3. The system-on-a-chip apparatus of claim 1, 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.

4 The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.

5 The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.

6. The system-on-a-chip apparatus of claim 5, 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.

MediaTek Exhibit 1012, Page 450 of 463

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.

8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.

11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.

12. The system-on-a-chip apparatus of claim 11, 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.

13. The system-on-a-chip apparatus of claim 12, wherein the security engine to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

14. The system-on-a-chip apparatus of claim 13, wherein the security engine to use the session key to encrypt a subsequent message sent from the client device to the server.

15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

MediaTek Exhibit 1012, Page 451 of 463

16. 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 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 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;

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

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

17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.

18. The method of claim 16, further comprising:

receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and

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

19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:

receiving a ServerHello message from the 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.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.

21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

23. The method of claim 22, 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 storage of the security engine of the system-on-a-chip.

24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

25. The method of claim 24, 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 server.

26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

receiving a public Rivest-Shamir-Adleman server key from the server; and

storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

MediaTek Exhibit 1012, Page 453 of 463

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the 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 a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key exchange with the server comprises:

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

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.

30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

MediaTek Exhibit 1012, Page 454 of 463

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, 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 server;

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.

MediaTek Exhibit 1012, Page 455 of 463

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key; and

sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device performing the method of claims 16-34.

37. 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 Sockets Layer communication session with a 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 server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer communication session;

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

generating, in the security engine, a hash code as a function of the session key; and

sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

MediaTek Exhibit 1012, Page 456 of 463

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;

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

sending the encrypted pre-master key to the server.

40. The method of claim 39, further comprising:

wrapping the pre-master key in the security engine using a server public key, and

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

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

42. The method of claim 41, 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 server.

43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the 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 a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

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

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.

46. A source device comprising:

a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

MediaTek Exhibit 1012, Page 458 of 463

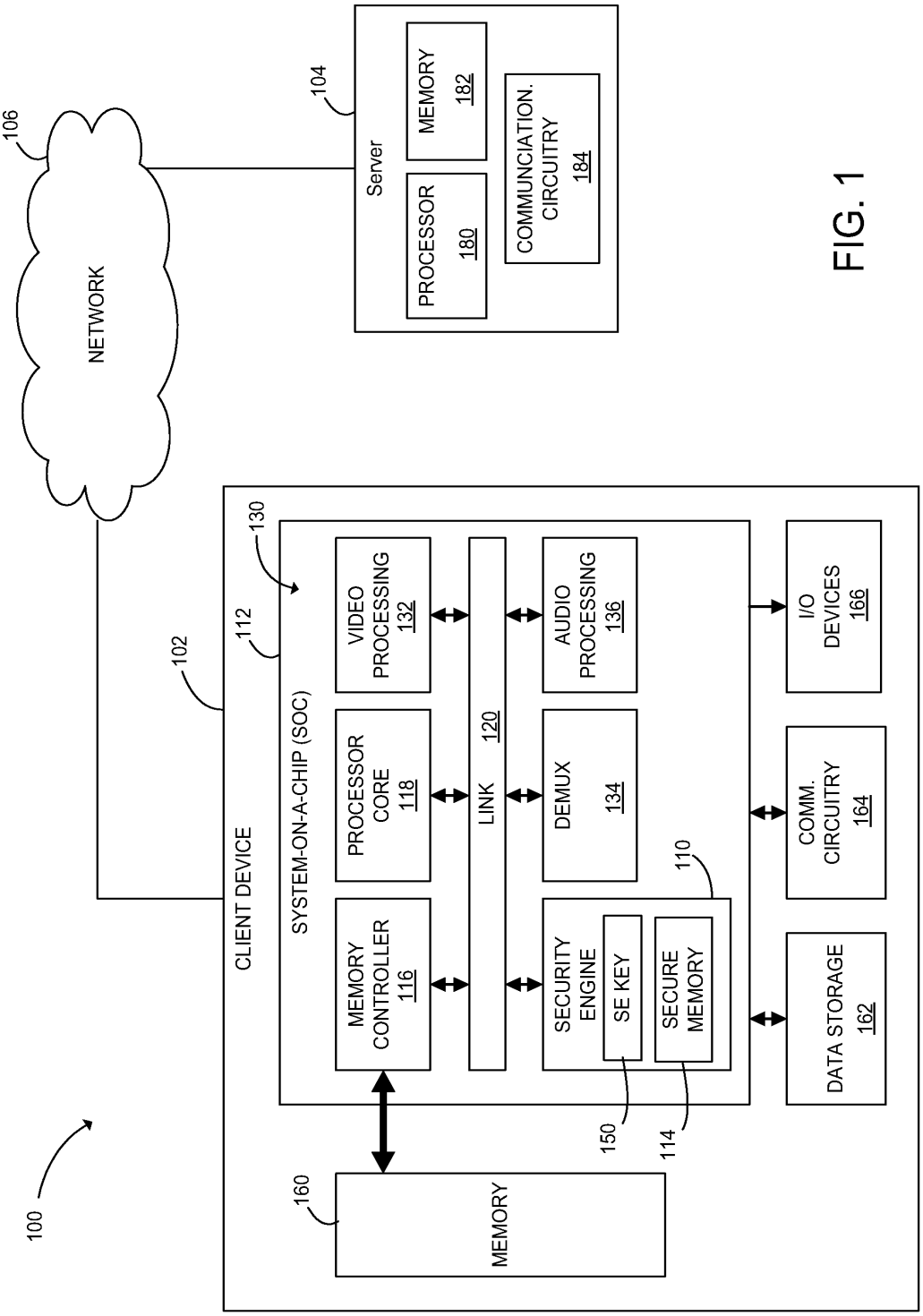

100
106
NETWORK
104
Server
MEMORY 182
PROCESSOR 180
COMMUNCIATION. CIRCUITRY 184
102
CLIENT DEVICE
112
SYSTEM-ON-A-CHIP (SOC)
130
VIDEO PROCESSING 132
AUDIO PROCESSING 136
I/O DEVICES 166
PROCESSOR CORE 118
LINK 120
DEMUX 134
COMM. CIRCUITRY 164
MEMORY CONTROLLER 116
SECURITY ENGINE
SE KEY
SECURE MEMORY
110
DATA STORAGE 162
150
114
160
MEMORY

FIG. 1

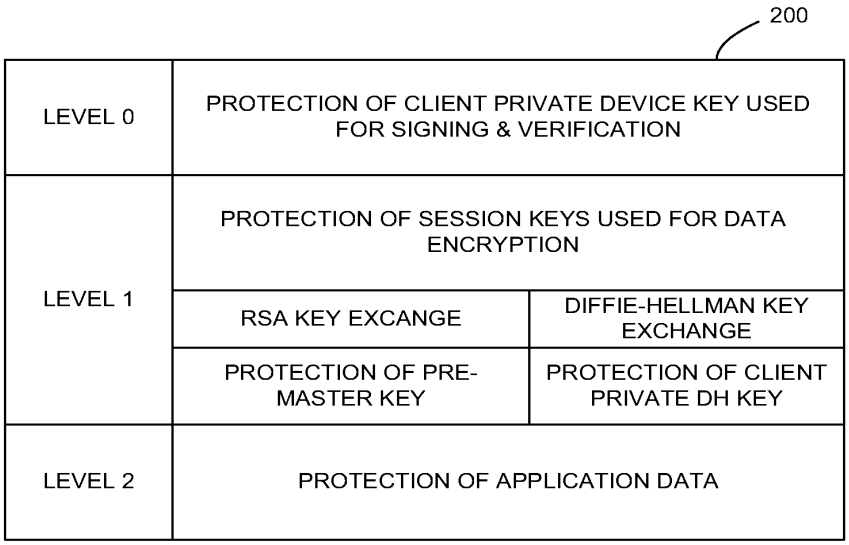

200
LEVEL 0
PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION
LEVEL 1
PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION
RSA KEY EXCANGE
DIFFIE-HELLMAN KEY EXCHANGE
PROTECTION OF PRE-MASTER KEY
PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2
PROTECTION OF APPLICATION DATA

FIG. 2

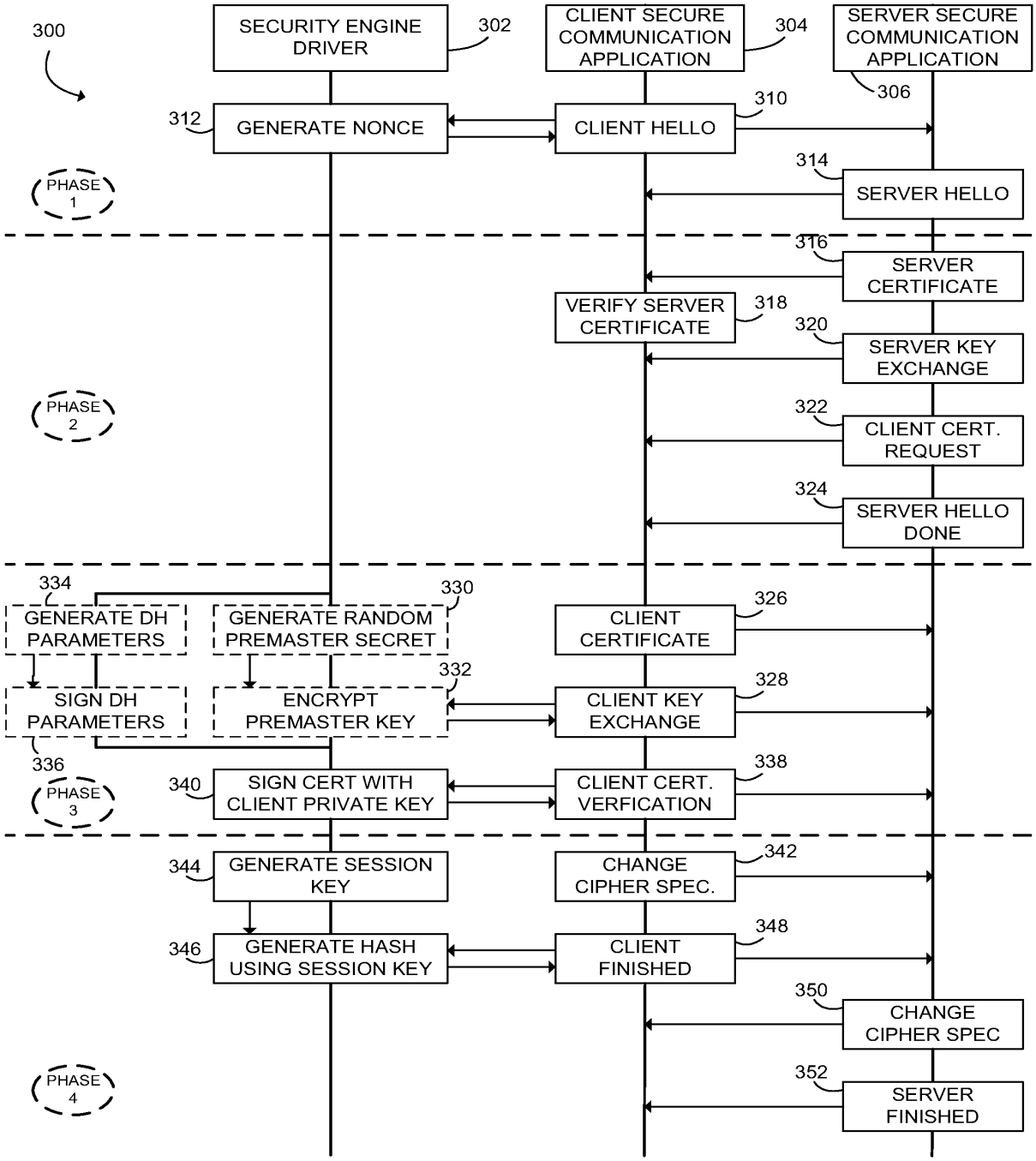

300
SECURITY ENGINE DRIVER
302
CLIENT SECURE COMMUNICATION APPLICATION
304
SERVER SECURE COMMUNICATION APPLICATION
306
312
GENERATE NONCE
CLIENT HELLO
310
314
SERVER HELLO
PHASE 1
316
SERVER CERTIFICATE
VERIFY SERVER CERTIFICATE
318
320
SERVER KEY EXCHANGE
PHASE 2
322
CLIENT CERT. REQUEST
324
SERVER HELLO DONE
334
330
GENERATE DH PARAMETERS
GENERATE RANDOM PREMASTER SECRET
CLIENT CERTIFICATE
326
332
328
SIGN DH PARAMETERS
ENCRYPT PREMASTER KEY
CLIENT KEY EXCHANGE
336
PHASE 3
340
SIGN CERT WITH CLIENT PRIVATE KEY
CLIENT CERT. VERFICATION
338
344
GENERATE SESSION KEY
CHANGE CIPHER SPEC.
342
346
GENERATE HASH USING SESSION KEY
CLIENT FINISHED
348
350
CHANGE CIPHER SPEC
PHASE 4
352
SERVER FINISHED

FIG. 3

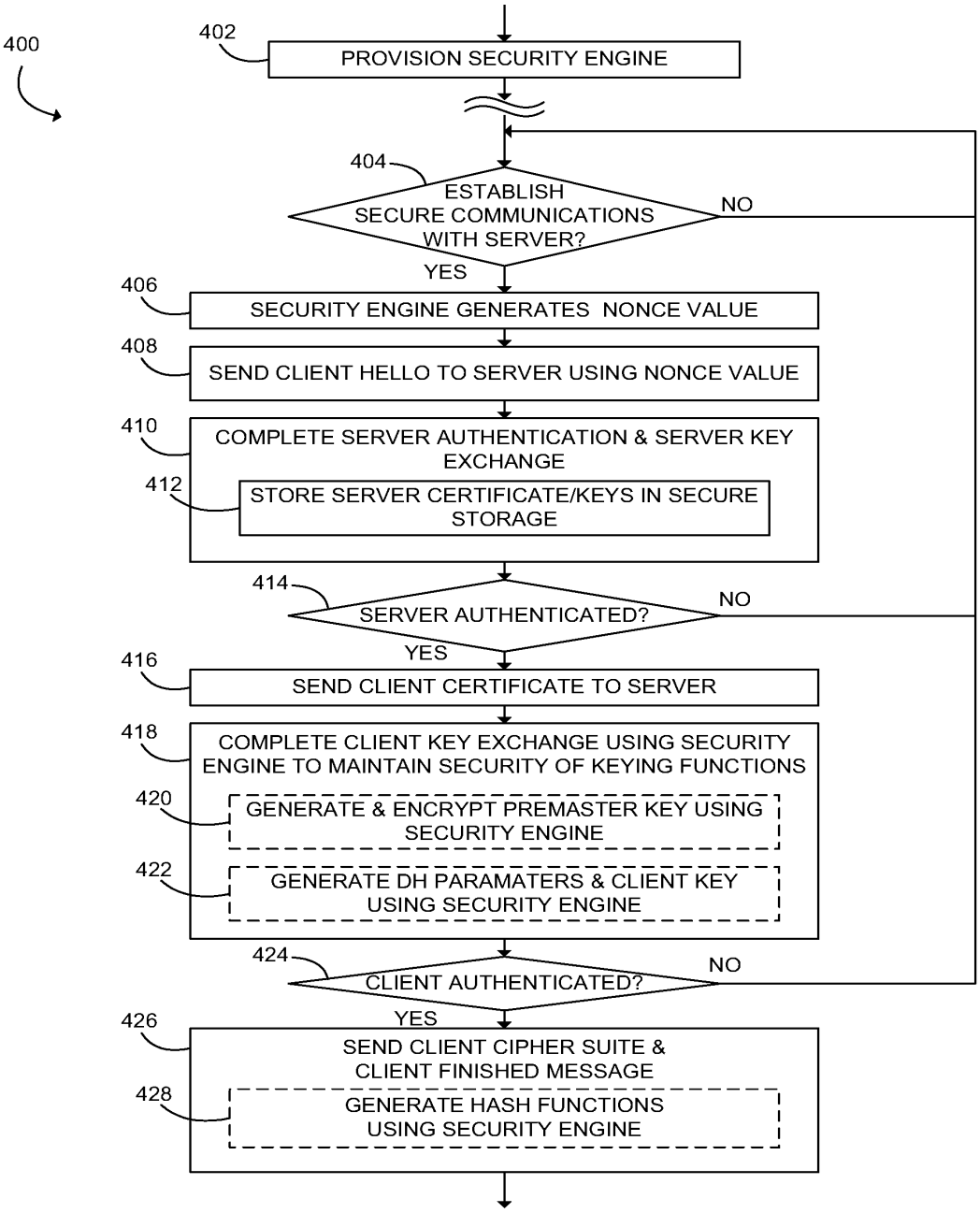

400
402
PROVISION SECURITY ENGINE
404
ESTABLISH SECURE COMMUNICATIONS WITH SERVER?
NO
YES
406
SECURITY ENGINE GENERATES NONCE VALUE
408
SEND CLIENT HELLO TO SERVER USING NONCE VALUE
410
COMPLETE SERVER AUTHENTICATION & SERVER KEY EXCHANGE
412
STORE SERVER CERTIFICATE/KEYS IN SECURE STORAGE
414
SERVER AUTHENTICATED?
NO
YES
416
SEND CLIENT CERTIFICATE TO SERVER
418
COMPLETE CLIENT KEY EXCHANGE USING SECURITY ENGINE TO MAINTAIN SECURITY OF KEYING FUNCTIONS
420
GENERATE & ENCRYPT PREMASTER KEY USING SECURITY ENGINE
422
GENERATE DH PARAMATERS & CLIENT KEY USING SECURITY ENGINE
424
CLIENT AUTHENTICATED?
NO
YES
426
SEND CLIENT CIPHER SUITE & CLIENT FINISHED MESSAGE
428
GENERATE HASH FUNCTIONS USING SECURITY ENGINE

FIG. 4

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 **06/24/2013**

	(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.

LDRC
/CHERRI FITZGERALD/

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.