



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.
12/152,354	05/14/2008	Kyung-Joo Suh	678-3502	4757

66547                      7590                      09/10/2012  
 THE FARRELL LAW FIRM, P.C.  
 290 Broadhollow Road  
 Suite 210E  
 Melville, NY 11747

EXAMINER

LEWIS, LISA C

ART UNIT	PAPER NUMBER
2495	

MAIL DATE	DELIVERY MODE
09/10/2012	PAPER

**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.



Art Unit: 2495

### **DETAILED ACTION**

Applicant's response with amendments filed 07/16/2012 has been received and entered.

Applicant has amended claim 4, cancelled claims 5-21, and added new claims 22-28.

#### ***Response to Arguments***

Applicant's arguments have been carefully considered but are deemed moot in view of the new grounds of rejection presented below.

#### ***Claim Rejections - 35 USC § 112***

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

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.

2. Claims 4 and 22-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 4 recites "the key for operating the Mobile IP, "the key for operating the CMIP", etc. It is unclear how a key can "operate" a protocol. It will be interpreted to mean "the key which is used in a Mobile IP protocol," etc.

#### ***Claim Rejections - 35 USC § 103***

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

A 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

Art Unit: 2495

ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 4, 22, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oba (US 2007/0250706) in view of Lee et al.(US 2007/0112967), and further in view of Feder (US 8,230,212).**

6. Regarding claims 4 and 25, Oba teaches a method and server for generating a security key in a mobile communication system including an AAA server, the method comprising:

a. Generating by the AAA server, a Master Session Key (MSK) and an Extended Master Session Key (EMSK) using a Long Term Credential Key (Long term credentials are used to generate both master session keys and enhanced master session keys at an AAA server) – see [0025] and [0032], for example.

b. Transmitting the MSK and the EMSK to each of a plurality of nodes included in the mobile communication system (The keys are exported – i.e., transmitted to nodes) – see [0025], for example.

7. Oba does not teach that one of the MSK and EMSK are used for generating keys for device and user authentication in a node.

8. Lee et al. teach that at an AAA, the user MSK is derived from the device MSK which are each used to authenticate the user and device, respectively - see [0041], for example.

9. Neither Oba nor Lee et al. teach that the EMSK is used for generating a key for operating a Mobile IP which is used for generating a CMIP and a PMIP.

10. Feder et al. teach a method wherein the EMSK is used to generate a Mobile IP key which is used to generate a CMIP and a PMIP key – see column 8 line 58 – column 9 line 21 and column 11 lines 29-53, for example.

11. It would have been obvious to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time of the claimed invention to modify

Art Unit: 2495

the teachings of Oba by using the MSK to authenticate the user and the device, for the purpose of providing mutual authentication to the system, based upon the beneficial teachings provided by Lee et al. It would have also been obvious to one of ordinary skill in the art at the time of the claimed invention to modify the teachings of Oba and Lee et al. by using the EMSK to generate the Mobile IP key which is used to generate the CMIP and PMIP keys, for the purpose of generating a secure key hierarchy without collisions (see column 2 line 64 – column 3 line 2, for example), based upon the beneficial teachings provided by Feder. These modifications would result in increased security, which is an obvious benefit to the skilled artisan. Further, the cited references are in the field of encryption, as is the instant application, and therefore, are in analogous arts.

12. Regarding claims 22 and 26, Lee et al. teach that the MSK-U is used to generate a new user master session key – see abstract, for example.

13. **Claims 23 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oba (US 2007/0250706) in view of Lee et al. and Feder, and further in view of Costa et al. (US 2009/0217033).**

14. **The teachings of Oba, Lee et al., and Feder are relied upon for the reasons set forth above.**

15. Regarding claims 23 and 27, Oba, Lee et al., and Feder do not teach that the session keys is used to generate a key used to encrypt data.

16. Costa et al. teach that an encryption key can be derived starting from a master session key 0 see [0008], for example.

17. It would have been obvious to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time of the claimed invention to modify the teachings of Oba, Lee et al., and Feder by using the session key to create an encryption key, for the purpose of providing secure encryption for a particular session, based upon the beneficial teachings

Art Unit: 2495

provided by Costa et al. These modifications would result in increased security, which is an obvious benefit to the skilled artisan. Further, the cited references are in the field of encryption, as is the instant application, and therefore, are in analogous arts.

**18. Claims 24 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oba (US 2007/0250706) in view of Lee et al. and Feder, and further in view of Koster et al. (US 2009/0132811).**

19. The teachings of Oba, Lee et al., and Feder are relied upon for the reasons set forth above.

20. Regarding claims 24 and 28, Oba, Lee et al., and Feder do not teach that long term credential is truncated to create the MSK and EMSK.

21. Koster et al. teach that when an authentication or encryption algorithm requires keys to be a specific length, one may truncate the output of the one way function to the required number of bits.

22. It would have been obvious to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time of the claimed invention to modify the teachings of Oba, Lee et al., and Feder by truncating the long term credential key to create the MSK and EMSK, for the purpose of adapting to the needs of a particular algorithm, based upon the beneficial teachings provided by Koster et al. These modifications would result in increased ease of use, which is an obvious benefit to the skilled artisan. Further, the cited references are in the field of encryption, as is the instant application, and therefore, are in analogous arts.

### *Conclusion*

A reference to specific paragraphs, columns, pages, or figures in a cited prior art reference is not limited to preferred embodiments or any specific examples. It is well settled that a prior art reference, in its entirety, must be considered for all that it expressly teaches and fairly suggests to one having ordinary

Art Unit: 2495

skill in the art. Stated differently, a prior art disclosure reading on a limitation of Applicant's claim cannot be ignored on the ground that other embodiments disclosed were instead cited. Therefore, the Examiner's citation to a specific portion of a single prior art reference is not intended to exclusively dictate, but rather, to demonstrate an exemplary disclosure commensurate with the specific limitations being addressed. *In re Heck*, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting *In re Lemelson*, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). *In re: Upsher-Smith Labs. v. PamLab, LLC*, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005); *In re Fritch*, 972 F.2d 1260, 1264, 23 USPQ2d 1780, 1782 (Fed. Cir. 1992); *Merck & Co. v. Biocraft Labs., Inc.*, 874 F.2d 804, 807, 10 USPQ2d 1843, 1846 (Fed. Cir. 1989); *In re Fracalossi*, 681 F.2d 792, 794 n.1, 215 USPQ 569, 570 n.1 (CCPA 1982); *In re Lamberti*, 545 F.2d 747, 750, 192 USPQ 278, 280 (CCPA 1976); *In re Bozek*, 416 F.2d 1385, 1390, 163 USPQ 545, 549 (CCPA 1969).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571) 270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

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.

Art Unit: 2495

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.

/L. L./  
Examiner, Art Unit 2495

/Farid Homayounmehr/  
Supervisory Patent Examiner, Art Unit 2495

<b>Notice of References Cited</b>	Application/Control No. 12/152,354	Applicant(s)/Patent Under Reexamination SUH ET AL.	
	Examiner Lisa Lewis	Art Unit 2495	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2007/0112967 A1	05-2007	Lee et al.	709/229
*	B <b>US-2007/0250706 A1</b>	<b>10-2007</b>	<b>Oba, Yoshihiro</b>	<b>713/159</b>
*	C US-2009/0132811 A1	05-2009	Koster et al.	713/156
*	D US-2009/0217033 A1	08-2009	Costa et al.	713/155
*	E US-8,230,212 B2	07-2012	Feder et al.	713/155
	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**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	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.