

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

NETWORK-1 TECHNOLOGIES, INC.,
Patent Owner.

Case No. IPR2026-00115
U.S. Patent No. 11,606,204

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,606,204**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	1
III. FEE AUTHORIZATION	3
IV. GROUNDS FOR STANDING.....	3
V. PRECISE RELIEF REQUESTED	3
VI. THE CHALLENGED PATENT	4
VII. PROSECUTION HISTORY OF THE '204 PATENT.....	7
VIII. LEVEL OF ORDINARY SKILL IN THE ART.....	7
IX. PRIORITY DATE	7
X. CLAIM CONSTRUCTION	8
XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART	8
A. Semple (Ex-1005).....	8
B. Wang (Ex-1006).....	10
C. Bhuyan (Ex-1007).....	12
D. Pierce (Ex-1010).....	13
E. Jorgensen (Ex-1008).....	14
F. SEC1 (Ex-1012)	15
XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS.....	16
A. Ground 1: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang.....	16
1. A POSITA would have been motivated to combine Semple's teachings with Wang's teachings and would have had a reasonable expectation of success.	16
2. Independent Claim 1	18
a. Element 1[pre]: A mobile device comprising:	18
b. Element 1(a): at least one processor; and.....	19

TABLE OF CONTENTS
(continued)

	Page
c. Element 1(b): at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:	19
d. Element 1(b)(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;.....	21
e. Element 1(b)(2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;.....	28
f. Element 1(b)(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;.....	30
g. Element 1(b)(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;	32

TABLE OF CONTENTS

(continued)

	Page
h. Element 1(b)(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and	34
i. Element 1(b)(6) authenticating with the wireless network using a message digest with the pre-shared secret key.....	41
3. Dependent Claims 2-7, 11-12, 14-16, and 18-20.....	44
a. Claim 2: The mobile device of claim 1, wherein the message further comprises a module identity string, the module identity string comprising a temporary identification for the mobile device.	44
b. Claim 3: The mobile device of claim 1, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network.	45
c. Claim 4: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K.....	47
d. Claim 5: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.	47

TABLE OF CONTENTS

(continued)

Page

e.	Claim 6: The mobile device of claim 1, further comprising, in step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein, in step (2), the module public key and the module private key are derived using the standard curve.	48
f.	Claim 7: The mobile device of claim 6, wherein, in step (5), the message further comprises the parameters for the cryptographic algorithms, and wherein the server mutually derives the symmetric ciphering key using at least the module public key and the parameters for the cryptographic algorithms.	49
g.	Claim 9: The mobile device of claim 1, further comprising, in step (2), deriving (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number.	50
h.	Claim 11: The mobile device of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device.	51
i.	Claim 12: The mobile device of claim 1, wherein the server comprises a plurality of computers, wherein the plurality includes at least one sub-server and at least one database.	52
j.	Claim 14: The mobile device of claim 1, wherein the wireless network includes the server.	54
k.	Claim 15: The mobile device of claim 1, wherein, in step (1), the module identity is stored in a read-only nonvolatile memory address, wherein the mobile device designates the read-only nonvolatile memory address as read-only for a time interval.	55

TABLE OF CONTENTS

(continued)

	Page
l. Claim 16: The mobile device of claim 1, wherein the wireless network comprises at least one base station communicating with a 3GPP wireless technology.....	56
m. Claim 18: The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.	57
n. Claim 19: The mobile device of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.....	58
o. Claim 20: The mobile device of claim 1, wherein the mobile device comprises a smartphone.	59
B. Ground 2: Claims 5 and 8 are obvious over Semple in view of Wang and Bhuyan.	60
1. A POSITA would have been motivated to combine Semple-Wang's teachings with Bhuyan's teachings and would have had a reasonable expectation of success.	60
2. Dependent Claims 5 and 8.....	62
a. Claim 5: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.	62
b. Claim 8: The mobile device of claim 1, wherein the mobile device receives the pre-shared secret key via a wireless 802.11 connection to a web portal after a user for the mobile device submits a pre-shared secret key code for the mobile device to the web portal.	63
C. Ground 3: Claim 10 is obvious over Semple in view of Wang and Pierce.	65

TABLE OF CONTENTS

(continued)

	Page
a. Claim 10: The mobile device of claim 9, wherein the random number generator is configured to generate the random number from a seed value, and wherein the seed value comprises data from at least one of a sensor and a radio for the mobile device.....	65
D. Ground 4: Claims 13 and 17-18 are obvious over Semple in view of Wang and Jorgensen.	68
1. A POSITA would have been motivated to combine Semple-Wang’s teachings with Jorgensen’s teachings and would have had a reasonable expectation of success.	68
2. Dependent Claims 13 and 17-18.....	70
a. Claim 13: The mobile device of claim 1, wherein the server comprises at least one virtualized server operating on at least one computer.....	70
b. Claim 17: The mobile device of claim 1, wherein the message comprises a single user datagram protocol packet.....	71
c. Claim 18: The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.	72
E. Ground 5: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang and SEC1	72
1. Independent Claim 1	72
a. Element 1(b)(3).....	72
F. Grounds 6-8.....	73
XIII. CONCLUSION.....	73

LIST OF EXHIBITS¹

Ex. No.	Description
Ex-1001	U.S. Patent No. 11,606,204 (“the ’204 Patent”)
Ex-1002	Declaration of Dr. Christina Pöpper
Ex-1003	Curriculum Vitae of Dr. Christina Pöpper
Ex-1004	Prosecution History of U.S. Patent No. 11,606,204
Ex-1005	U.S. Patent Publication No. 2010/0174907 to Semple (“Semple”)
Ex-1006	PCT Patent Publication No. WO2008/005162 to Wang (“Wang”)
Ex-1007	U.S. Patent Publication No. 2010/0135491 to Bhuyan (“Bhuyan”)
Ex-1008	U.S. Patent Publication No. 2004/0221163 to Jorgensen (“Jorgensen”)
Ex-1009	INTENTIONALLY LEFT BLANK
Ex-1010	U.S. Patent Publication No. 2009/0323967 to Pierce (“Pierce”)
Ex-1011	INTENTIONALLY LEFT BLANK
Ex-1012	Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, v2 (May 21, 2009) (“SEC1”)
Ex-1013	INTENTIONALLY LEFT BLANK
Ex-1014	INTENTIONALLY LEFT BLANK
Ex-1015	INTENTIONALLY LEFT BLANK
Ex-1016	INTENTIONALLY LEFT BLANK

¹ Four-digit pin citations that begin with 0 are to the branded numbers added by Samsung in the bottom right corner of the exhibits. All other pin citations are to original page, column, paragraph, or line numbers.

Ex. No.	Description
Ex-1017	INTENTIONALLY LEFT BLANK
Ex-1018	INTENTIONALLY LEFT BLANK
Ex-1019	INTENTIONALLY LEFT BLANK
Ex-1020	Claim Mapping Table
Ex-1021	U.S. Patent Publication No. 2007/0083766 to Farnham (“Farnham”)
Ex-1022	U.S. Patent Publication No. 2012/0300934 to Ala-Laurila (“Ala-Laurila”)
Ex-1023	U.S. Patent Publication No. 2014/0219443 to Brainis (“Brainis”)
Ex-1024	U.S. Patent Publication No. 2014/0024343 to Bradley (“Bradley”)
Ex-1025	Prosecution History of U.S. Patent No. 12,166,869
Ex-1026	U.S. Patent Publication No. 2009/0068985 to Nguyen (“Nguyen”)
Ex-1027	U.S. Patent Publication No. 2012/0008775 to Natarajan (“Natarajan”)
Ex-1028	U.S. Patent No. 8,127,142 to Cuppett (“Cuppett”)
Ex-1029	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, Final Report (Sept. 25, 2012) (“CSMG”)
Ex-1030	U.S. Patent No. 9,210,138 to Nakhjiri (“Nakhjiri”)
Ex-1031	U.S. Patent Publication No. 2013/0012168 to Rajadurai (“Rajadurai”)
Ex-1032	U.S. Patent Publication No. 2013/0301828 to Gouget (“Gouget”)
Ex-1033	Boyd, C. and Mathuria, A., Protocols for Authentication and Key Establishment, Springer-Verlag (2003) (“Boyd-Mathuria”)

I. INTRODUCTION

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Petitioner”) request *inter partes* review (“IPR”) of Claims 1-20 of U.S. Patent No. 11,606,204 (“the ’204 Patent”) (Ex-1001), currently assigned to Network-1 Technologies, Inc. (“PO”).

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Parties-in-Interest: Petitioner identifies the following real parties-in-interest: Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

Related Matters: PO has asserted the ’204 Patent against Petitioner in *Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd. et al.*, No. 2:25-cv-00667 (E.D. Tex.) (“Samsung litigation”).

Lead and Backup Counsel:

- Lead Counsel:

William M. Fink (Reg. No. 72,332)
O’Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006
Telephone: (202) 383-5300
Fax: (202) 383-5414
Email: tfink@omm.com

- Backup Counsel:

Benjamin M. Haber (Reg. No. 67,129)
O’Melveny & Myers LLP
400 South Hope Street, 19th Floor
Los Angeles, CA 90071

Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: bhaber@omm.com

Marc J. Pensabene (Reg. No. 37,416)
O'Melveny & Myers LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: (212) 326-2000
Fax: (212) 326-2061
Email: mpensabene@omm.com

Brian Cook (Reg. No. 59,356)
O'Melveny & Myers LLP
400 South Hope Street, 19th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407
Email: bcook@omm.com

Caitlin P. Hogan (Reg. No. 61,515)
O'Melveny & Myers LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: (212) 326-2000
Fax: (212) 326-2061
Email: chogan@omm.com

Service Information: Petitioner consents to electronic service by email to the following addresses:

- tfink@omm.com
- bhaber@omm.com
- mpensabene@omm.com
- bcook@omm.com
- chogan@omm.com

III. FEE AUTHORIZATION

The PTO is authorized to charge any fees due during this proceeding to Deposit Account No. LA500639.

IV. GROUNDS FOR STANDING

Petitioner certifies that the '204 Patent is available for review, and Petitioner is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Petitioner requests review and cancellation of Claims 1-20 as unpatentable based on the following grounds, supported by a declaration from Dr. Christina Pöpper. Ex-1002 ¶¶1-40; Ex-1003. In the summary below, note that grounds 5-8 are identical to grounds 1-5 except that an additional reference, SEC1, has been added.

Ground	Summary
1	Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple (Ex-1005) and Wang (Ex-1006)
5	Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple, Wang, and SEC1 (Ex-1012)
2	Claims 5 and 8 are obvious over Semple, Wang, and Bhuyan (Ex-1007)
6	Claims 5 and 8 are obvious over Semple, Wang, SEC1, and Bhuyan
3	Claim 10 is obvious over Semple, Wang, and Pierce (Ex-1010)
7	Claim 10 is obvious over Semple, Wang, SEC1, and Pierce

Ground	Summary
4	Claims 13, 17, and 18 are obvious over Semple, Wang, and Jorgensen (Ex-1008)
8	Claims 13, 17, and 18 are obvious over Semple, Wang, SEC1, and Jorgensen

VI. THE CHALLENGED PATENT

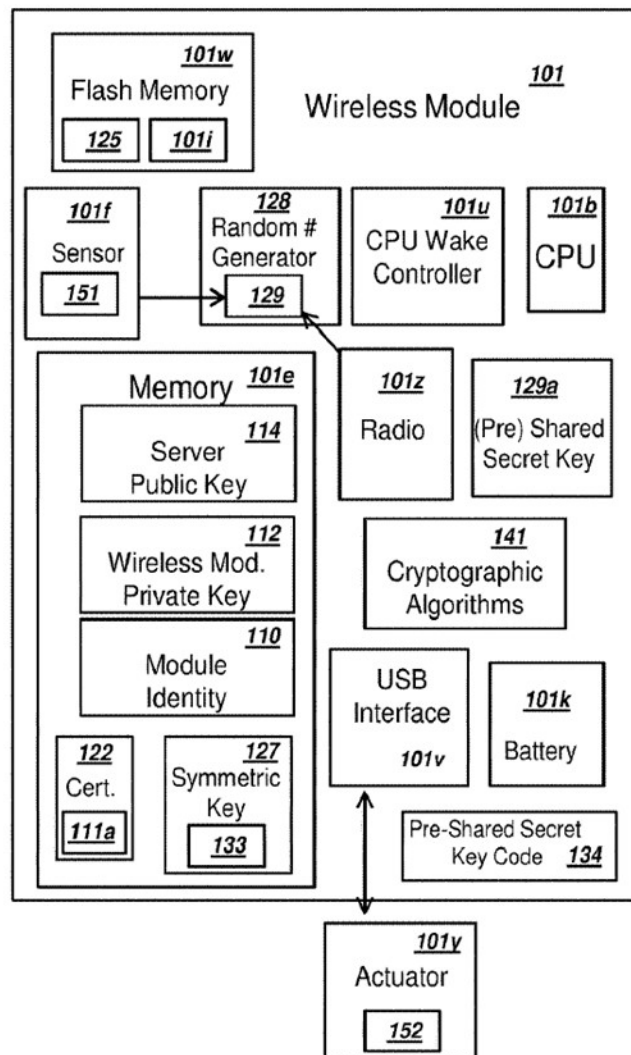
The '204 Patent teaches “efficient methods and systems for supporting secure, efficient, and flexible communications using Internet Protocol networks, where a server can communicate with both a ‘machine-to-machine’ modules and an application.” Ex-1001, 1:43-46; Ex-1002 ¶¶41-43.

As shown in Figure 1e below,² the '204 Patent teaches a wireless module 101, which may operate “as a smartphone or mobile phone.” Ex-1001, 14:65-67, Fig. 1e. Module 101 stores “module private key 112, server public key 114, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation.” Ex-1001, 27:23-26. Module identity 110 is “a unique identifier of module 101” such as “an international mobile subscriber identity number (IMSI).” Ex-1001, 28:44-47. Module 101 also stores cryptographic algorithms 141, which include a suite of algorithms that are used for “(i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using

² Throughout, emphasis and annotations are added unless otherwise specified.

private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys.” Ex-1001, 30:1-10. Moreover, module 101 stores “a pre-shared secret key 129a,” which is “shared between module 101 and server 105.” Ex-1001, 32:25-28.

Figure 1e



The '204 Patent teaches that module 101 derives “module private key 112 and a corresponding module public key 111 using (i) random number generator 128, (ii)

parameters 126, (iii) cryptographic algorithms 141, and/or (iv) a key pair generation algorithm 141e.” Ex-1001, 64:21-25. Derivation of these keys may use, for example, “values such as constants or variables in a parameters 126 to define an elliptic curve equation for use with an ECC algorithm 154,” which may “be input into a key pair generation algorithms 141e in the form of ECC parameters 137 or an ECC standard curve 138.” Ex-1001, 64:43-49. The ’204 Patent further teaches generating “module encrypted data ... ciphered with a symmetric key.” Ex-1001, 7:19-20. Symmetric key 127 is “a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms” 141 (Ex-1001, 27:53-55), which may be derived according to “the Elliptic Curve Integrated Encryption Scheme (ECIES) and/or ECDH ... using module public key 111, server public key 114, and a random number from random number generator 128.” Ex-1001, 28:1-6. Module 101 then sends the module encrypted data in a message to the server “using the derived keys” Ex-1001, 60:43-48. The server authenticates the message according to a “message digest, or using the shared secret key 510 as a symmetric key 127 within asymmetric ciphering algorithm 141b, where the successful encryption and decryption of data within” the message “using the shared secret key” on both ends is confirmation that the message is authenticated, “since both parties would only be able to mutually encrypt and decrypt by sharing the same shared secret key.” Ex-1001, 66:39-47.

VII. PROSECUTION HISTORY OF THE '204 PATENT

The '204 Patent was filed January 12, 2022, and claims priority through a chain of 5 continuation applications (now issued patents), the earliest of which was filed October 16, 2013. The Examiner did not issue any substantive prior art rejections during prosecution, only double patenting rejections based on related patent applications, which the Applicant overcame by filing terminal disclaimers. Ex-1002 ¶¶44.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art at the relevant time (“POSITA”) would have had at least a bachelor’s degree in electrical engineering, computer engineering, computer science, or a similar field, and 2–3 years of experience with cellular/WLAN security and mobile devices. Ex-1002 ¶¶17-19.

IX. PRIORITY DATE

For purposes of this proceeding only, Petitioner applies the earliest alleged priority date of the '204 Patent: October 16, 2013.³ Accordingly, AIA 35 U.S.C. §102 applies and the '204 Patent was never eligible for PGR.

³ Petitioner respectfully reserves the right to challenge the priority date in other proceedings.

X. CLAIM CONSTRUCTION

Petitioner interprets the claims according to *Phillips*. 37 C.F.R. §42.100(b). To resolve this Petition, Petitioner does not believe that any term requires express construction.⁴ CTPG, 44; Ex-1002 ¶45.

XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART

A. Semple (Ex-1005)

Semple (U.S. Patent Publication No. 2010/0174907) published on July 8, 2010 and is prior art to the '204 Patent under 35 U.S.C. §102(a)(1). Ex-1002 ¶¶46-49.

Semple teaches a “novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms.” Ex-1005 ¶3. As shown in Figure 6 below, Semple teaches a mobile terminal (MT) 606 including a SIM 608 that stores a module identity IMSI, a pre-shared secret integrity key Ki (which is also pre-stored in Home

⁴ The Samsung litigation is in its infancy. Petitioner respectfully reserves all rights to raise claim construction and other arguments in district court and will request leave to submit the district court’s claim construction as soon as it becomes available. Additionally, should PO raise express or implied claim construction arguments in its Preliminary Response, Petitioner will respectfully seek a Preliminary Reply to respond. Consolidated Trial Practice Guide (CTPG), 44-45.

Location Register (HLR) 602), and cryptographic algorithms including A3 and A8.

Ex-1005 ¶¶33, 47, Fig. 6.

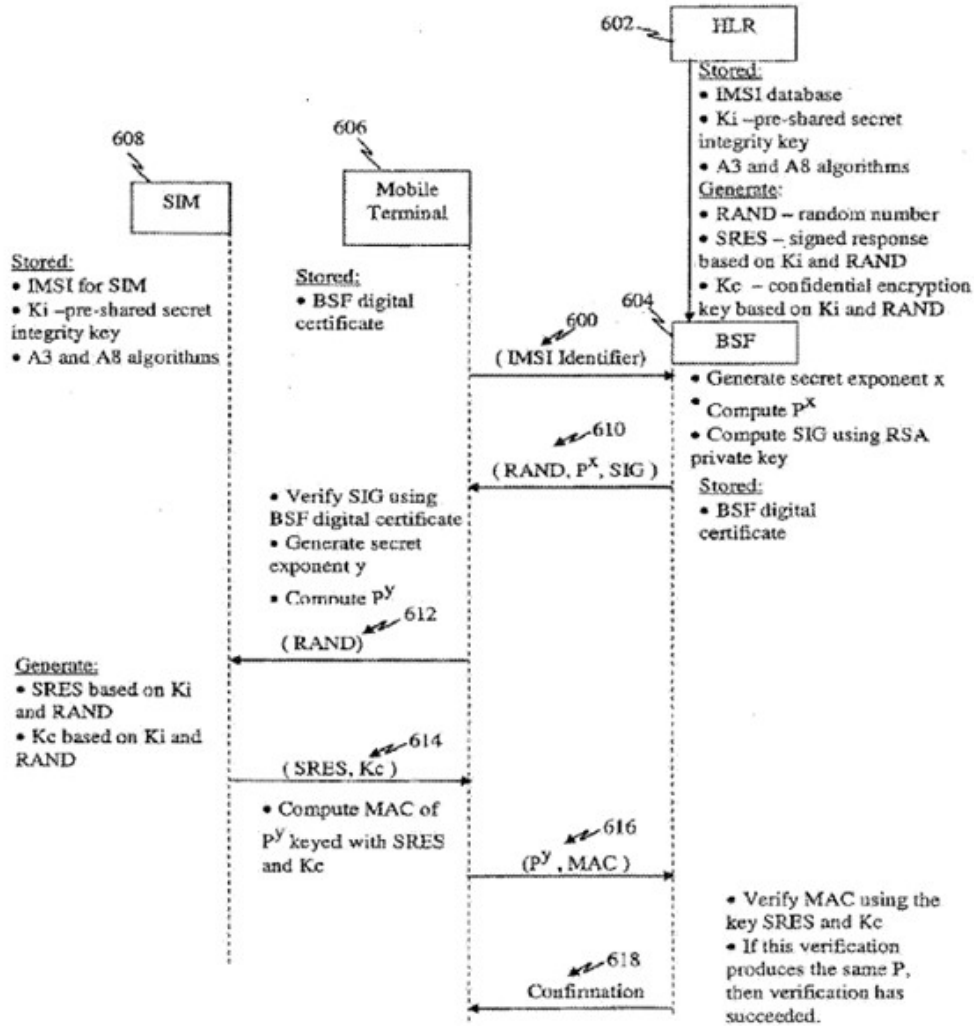


Figure 6

To support secure communications, Semple's bootstrapping server function (BSF) 604 and MT perform "a mutually authenticated Diffie-Hellman key exchange to agree on a key P^{xy} ." *Id.* ¶51. Specifically, "BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x , where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606." *Id.* ¶48.

As shown in Figure 6 at 610, the server public key P^x is sent to MT 606. Similarly, “MT 606 generates a random number y and computes P^y ,” which is sent to BSF 606 at step 616 of Figure 6. *Id.* ¶48. MT can then use its private key y and the server public key P^x to calculate P^{xy} , and BSF 604 similarly uses its private key x and MT public key P^y to calculate the same P^{xy} as a shared Diffie-Hellman secret. *See id.* ¶51. Semple discloses that a “key for further communications may then be computed, for instance, as a hash of P^{xy} , possibly including further information known to both the MT and BSF such as identity information, RAND, SRES, and K_c .” *Id.*

When the MT public key P^y is sent to the BSF, that message is authenticated using a message authentication code (MAC) computed from “ P^y keyed with SRES and K_c ,” which are, in turn, derived from the shared secret key K_i . *Id.*, Fig. 6 at 614, 616 (“Generate SRES based in K_i and RAND, K_c based on K_i and RAND,” “Compute MAC of P^y keyed with SRES and K_c ”).

B. Wang (Ex-1006)

Wang (PCT Patent Publication No. WO2008/005162) published on January 10, 2008 and is prior art to the '204 Patent under §102(a)(1). Ex-1002 ¶¶50-52.

Wang teaches “a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE).” Ex-1006 ¶3.

Wang teaches that “[t]he fact that the important [wireless transmit/receive unit] WTRU identity, (i.e., IMSI), is sent over the air unprotected provokes an ‘IMSI catching threat’” because “[t]he caught IMSI could be used by a malignant denial of service (DoS) attack or other possible attacks to the network and users.” Ex-1006 ¶12. Wang thus teaches the desirability “to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure.” Ex-1006 ¶13. In Wang’s method, “[a]n initial connection signaling message for network attachment, and a user ID, (e.g., an IMSI), are ciphered using the initial security parameters even before the WTRU is authenticated.” Ex-1006 ¶15. “The initial security parameters for ciphering include a CK.” *Id.* The ciphering key CK (and related integrity key IK) are conventionally symmetric session keys generated from a random value and the shared secret key K. *Id.* ¶8. However, Wang states in some embodiments, CK may be a public key “broadcast by or derived from network system information.” *Id.* ¶15. In either case, Wang states that the WTRU “performs ciphering on the attach message and the IMSI with the initial [ciphering key] CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer.” Ex-1006 ¶31. The “MAC-I” is a “hash computed ... on the message’s contents using the session key IK.” *Id.* ¶10.

Wang thus teaches that “[u]nlike the conventional attachment procedure, the attach message and the IMSI are protected with initial CK and IK.” Ex-1006 ¶31.

C. Bhuyan (Ex-1007)

Bhuyan (U.S. Patent Publication No. 2010/0135491) published on June 3, 2010 and is prior art to the ’204 Patent under §102(a)(1). Ex-1002 ¶¶53-54.

Bhuyan teaches “a method of authenticating a mobile device” in a telecommunications network “using a network provisioned security module and subsequent secure communications between the mobile device and the network.” Ex-1007 ¶1. Specifically, Bhuyan teaches that a SIM “is used to store a secret key that is been preloaded onto the card when the card is made” and the secret key is “shared a priori between the mobile phone and the network operator before any communication is initiated.” Ex-1007 ¶3. Moreover, as shown in Figure 3 below, Bhuyan teaches that “the user first connects to the provisioning server 204 using the computer ... over the internet.” Ex-1007 ¶57, Fig. 3. Bhuyan teaches that “[t]he user is then presented with a web page or similar where the user can input details of the mobile device where the security module is required” including “a password which is used ... for securing the security module components on the mobile device.” Ex-1007 ¶57. Bhuyan’s provisioning server then “makes a request to the authentication server 206 for security module parameters.” Ex-1007 ¶59. The authentication server “generates in response to the request a unique identifier for the mobile device”

referred to as the IMSI “as well as a secret key Ki.” Ex-1007 ¶59. The provisioning server then “encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device ... using the password provided by the user” along with “the software-based security module,” which “is an application that is run by the mobile device.” Ex-1007 ¶62. The user then “installs the security module on the mobile device 210 and also stores the security parameters IMSI and Ki.” Ex-1007 ¶65.

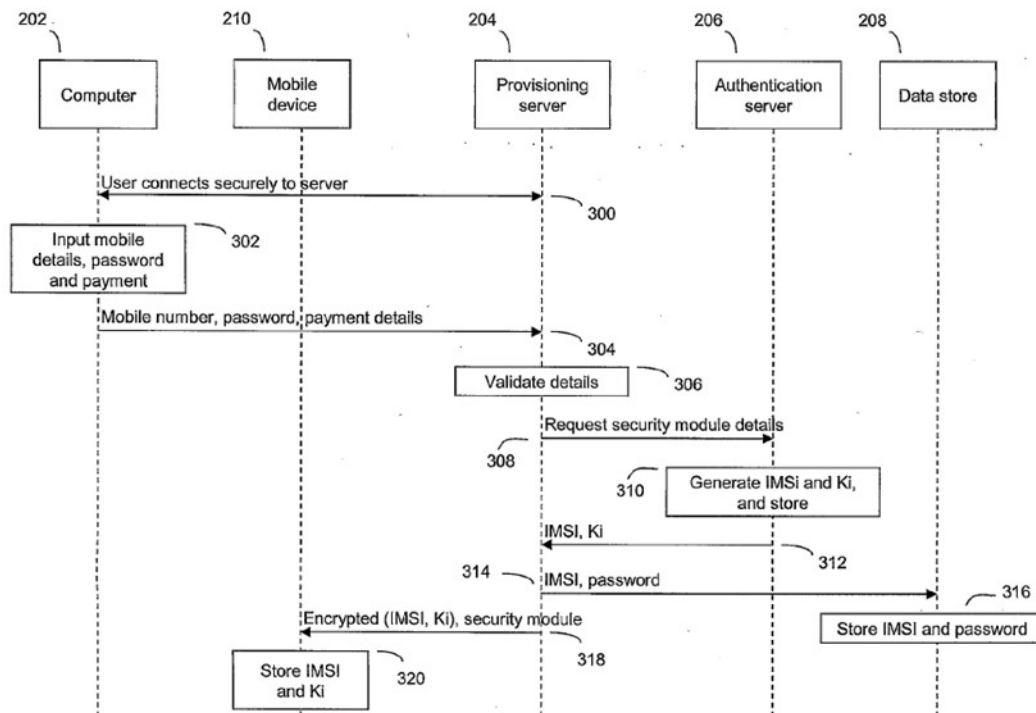


Figure 3

D. Pierce (Ex-1010)

Pierce (U.S. Patent Publication No. 2009/0323967) published on December 31, 2009 and is prior art to the '204 Patent under §102(a)(1). Ex-1002 ¶¶55-56.

Pierce teaches “techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.” Ex-1010 ¶1. Specifically, Pierce teaches a method for enabling “the automatic generation of strong cryptographic keys by an embedded processing device at the time of manufacturing, before the product is released for distribution to end users ... by supplying the embedded device with entropy data that it uses to seed a pseudo random number generator (PRNG) that is used to generate the keys.” Ex-1010 ¶19. Pierce further teaches that the “entropy data can be obtained by the embedded device from any of a number of sources, including those both internal and external to the manufactured product” (Ex-1010 ¶19) such as, for example, “a sensor,” “GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module,” or “an assigned mobile number for the telematics unit.” Ex-1010 ¶36.

E. Jorgensen (Ex-1008)

Jorgensen (U.S. Patent Publication No. 2004/0221163) published on November 4, 2004 and is prior art to the '204 Patent under §102(a)(1). Ex-1002 ¶¶57-58.

Jorgensen teaches methods and systems “for improving access control, administrative monitoring, reliability, as well as flexibility of data transmission and remote application sharing over a network.” Ex-1008, Abstract. Specifically,

Jorgensen teaches an “authentication and encryption scheme” that “uses Secure Key Exchange (SKE)” using “Elliptic Curve Cryptosystem (ECC) private keys.” Ex-1008 ¶34. Jorgensen teaches that “[t]he data transmission between the client and the server is effectuated by a dynamic datagram switch based on a datagram schema” such as a user datagram protocol (“UDP”). Ex-1008 ¶101. Jorgensen further teaches that “[r]andom number generators” are used to “generate pools of random numbers based on the supply of one or more seeds,” which are “generated by sampling and processing a source of entropy outside the computer systems or networks involved.” Ex-1008 ¶131. The true random values are used to generate “[m]ultiple and separate private keys.” Ex-1008 ¶134. Jorgensen also teaches an Encrypted Virtual File System (“EVFS”), which is a “server-based file system ... which allows the users of a network system to store files or data away from their local hosts or client carriers.” Ex-1008 ¶142. Jorgensen teaches that the use of an EVFS “[a]long with encryption, authentication, and other features ... enables secure delivery and stand-alone operation of applications through” the device. Ex-1008 ¶150.

F. SEC1 (Ex-1012)

SEC1 (Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography) published on May 21, 2009 and is prior art to the '204 Patent under §102(a)(1). Ex-1002 ¶¶59-60.

SEC1 teaches “public-key cryptographic schemes based on elliptic curve cryptography (ECC).” Ex-1012, 1. SEC1 teaches that “[t]he list of supported key derivation functions at this time is: ANSI-X9.63-KDF.” Ex-1012, 31-32. SEC1 further teaches that “[t]he key derivation function ANSI-X9.63-KDF is the simple hash function construct described in ANS X9.63 [X9.63].” Ex-1012, 32-33. Moreover, SEC1 teaches that “[e]ntities U and V should perform the following setup procedure to prepare to use the elliptic curve Diffie-Hellman scheme ... Let KDF denote the key derivation function chosen.” Ex-1012, 56-57.

XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

A. Ground 1: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang.

1. A POSITA would have been motivated to combine Semple’s teachings with Wang’s teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine the teachings of Semple and Wang and had a reasonable expectation of success in doing so because each relates to secure methods of authenticating a mobile device with a wireless network, and each focuses on well-known and complementary weaknesses in that process. Ex-1002 ¶61. As described above, Semple addresses the need to generate a set of session keys to secure communications between a mobile device and the network through a bootstrapping process using a Diffie-Hellman key agreement procedure

based on deriving private/public key pairs at the mobile device and authentication server. Ex-1005 ¶¶3, 40-44, Fig. 6. But Semple initiates its server attachment sequence by sending, to the network server, the mobile device's permanent subscriber identity, IMSI, in the clear, exposing it to potential IMSI capture attacks. *Id.* ¶41. Wang addresses this specific security problem and teaches the desirability “to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure.” Ex-1006 ¶13. In Wang's method, “[a]n initial connection signaling message for network attachment, and a user ID, (e.g., an IMSI), are ciphered using the initial security parameters even before the WTRU is authenticated.” Ex-1006 ¶15. Wang thus teaches that “[u]nlike the conventional attachment procedure, the attach message and the IMSI are protected with initial [keys] CK and IK.” Ex-1006 ¶31. However, a POSITA would have understood that Wang's method of securing the IMSI by ciphering it with the initial key CK from the USIM could be improved by instead ciphering it with the symmetric Diffie-Hellman key taught by Semple for securing messages between the mobile device and authentication server because such an approach would remove the dependency on long-term secrets that could potentially have been compromised. Ex-1002 ¶61 (explaining perfect forward secrecy). Thus, the combination of Semple and Wang results in a more secure authentication process that both protects the IMSI by

encrypting it instead of sending it in the clear, and performs that encryption using the secure key derivation process taught by Semple for protecting communications between the mobile device and authentication server.

A POSITA would have had a reasonable expectation of success in combining the teachings of Semple and Wang. Ex-1002 ¶62. Both describe methods for securing wireless communications using similar authentication and key agreement mechanisms and they address complementary security issues resulting in a more robust system for network authentication. Ex-1005 ¶3; Ex-1006, Abstract, ¶3. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶62.

2. Independent Claim 1

a. Element 1[pre]: A mobile device comprising:

Semple in view of Wang (“Semple-Wang”) teaches⁵ the preamble, to the extent it is limiting. Ex-1002 ¶¶63-64.

Semple teaches that mobile terminal “**MT 102** may be a legacy *wireless communication device* that registers or connects with a service provider using a

⁵ Petitioner uses the term “teaches” to include both express teachings and those fairly suggested to a person of ordinary skill in the art. *In re Baird*, 16 F.3d 380, 383 (Fed. Cir. 1994); *In re Keller*, 642 F.2d 413, 425 (CCPA, 1981) (“The test for obviousness is...what the combined teachings of the references would have suggested to those of ordinary skill in the art.” (citations omitted)).

predefined protocol (e.g., a pre-3G protocol) in order to communicate over the network 100.” Ex-1005 ¶27. Semple further teaches that “the terms ‘mobile terminal’, ‘user equipment’, ‘mobile device’, ‘wireless device’, and ‘wireless mobile device’ are interchangeably used to refer to *mobile phones* ... and/or other mobile communication/computing devices which communicate, at least partially, through a cellular network.” Ex-1005 ¶24.

b. Element 1(a): at least one processor; and

Semple-Wang teaches Element 1(a). Ex-1002 ¶¶65-66.

Semple teaches that “MT 200 includes *a processing circuit 202 (e.g., processor)* coupled to” a communication interface 206 “to communicate with a wireless network, and a Subscriber Identity Module (SIM) card 204.” Ex-1005 ¶33; *see also id.* ¶23 (“[a] processor may perform the necessary tasks”).

c. Element 1(b): at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:

Semple-Wang teaches Element 1(b). Ex-1002 ¶¶67-68.

Semple teaches that “[w]hen implemented in software, firmware, middleware or microcode, the *program code* or code segments to perform the necessary tasks may be *stored in a machine-readable medium* such as a storage medium or other storage(s).” Ex-1005 ¶23. Moreover, Semple teaches that its processing circuit

performs “part or all of the methods illustrated in FIGS. 4, 5, 6, and 7.” Ex-1005 ¶33. As shown below, Figure 4 teaches “*a method of performing a challenge-response mechanism that mutually authenticates a mobile terminal, having a legacy SIM, and a bootstrapping server function according to one implementation.*” Ex-1005 ¶35, Fig. 4. The BSF is “hosted in one or more network devices and/or servers that are part of the infrastructure of the network architecture.” Ex-1005 ¶26.

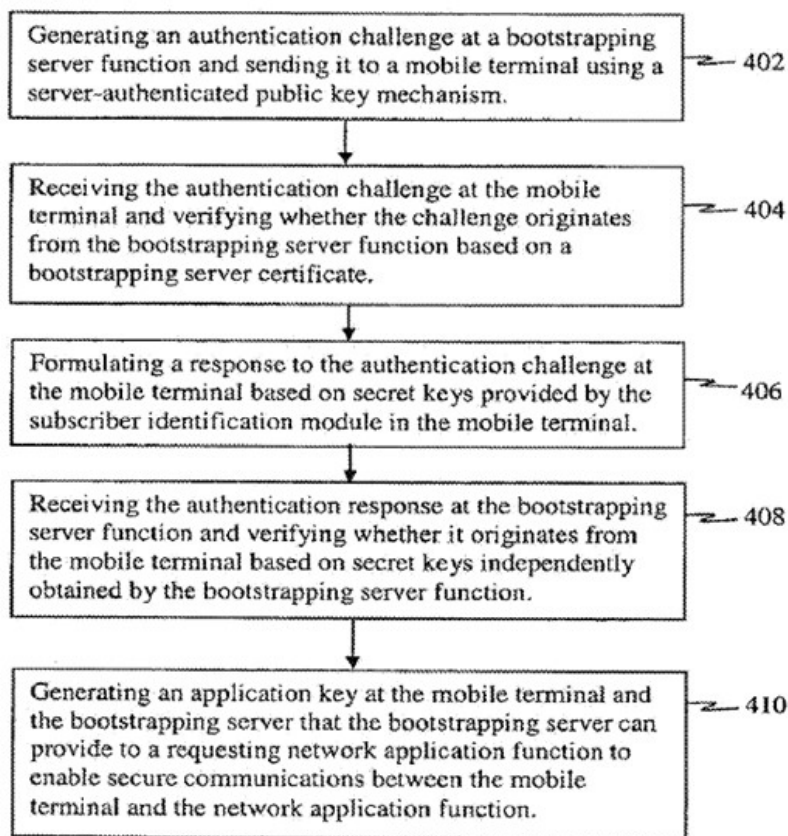


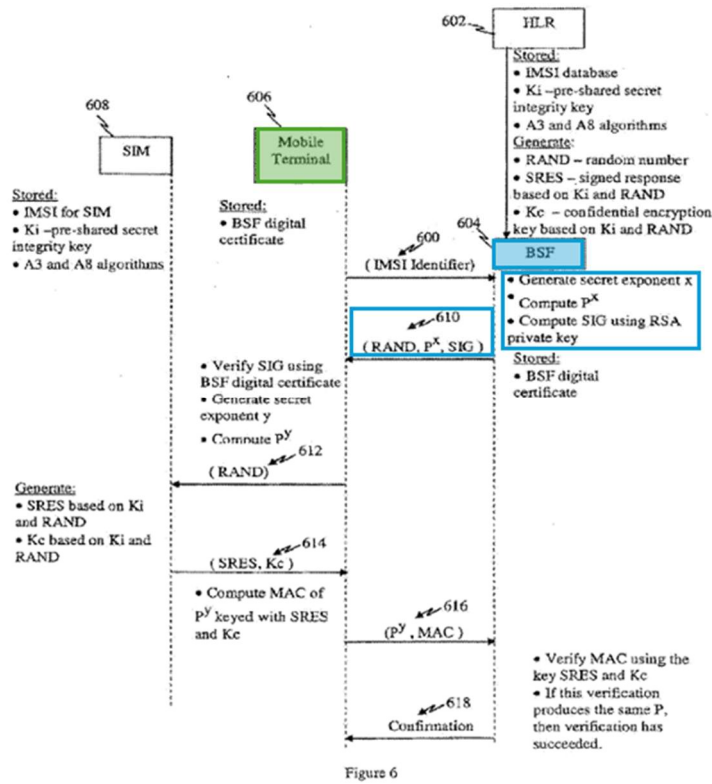
Figure 4

- d. **Element 1(b)(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;**

Semple-Wang teaches Element 1(b)(1). Ex-1002 ¶¶69-70.

(1) Storing a server public key

As shown in annotated Figure 6 below, Semple teaches that MT 606 (green) receives server public key P^x from BSF 604 (blue) and evidently stores it because MT later (in ¶51) uses it to compute P^{xy} . Ex-1005 ¶¶48 (“BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x ”), 49 (“MT 606 receives the triplet (RAND, P^x , SIG) 610”), 51 (“MT 606 and BSF 603 have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively.”).



Wang similarly discloses that the mobile device (WTRU) stores a server public key. Ex-1006 ¶42 (WTRU selects server public key k_a from a set of public keys broadcast by the LTE network). Ex-1002 ¶¶71-72.

Claim element	Sample	Wang
Server public key	P^x	k_a

(2) Storing a module identity comprising a permanent identifier for the mobile device

As shown in Figure 6 below, Semple teaches that the HLR 104 (yellow) “includes a database that contains mobile subscriber information for a wireless carrier, including an International Mobile Subscriber Identity (IMSI) for each MT 102 belonging to the subscriber” (red), which “is also stored in the Subscriber

Identity Module (SIM) [orange] of each MT 102.” Ex-1005 ¶47, Fig. 6; *see also id.*, Fig. 2. Semple further teaches that “[t]he IMSI is a unique number that is associated with an MT 102 in the network.” Ex-1005 ¶26. The IMSI corresponds to the recited “module identity.” Ex-1002 ¶73. An IMSI is well known to be a permanent identifier for the mobile device. Ex-1002 ¶¶73-74.

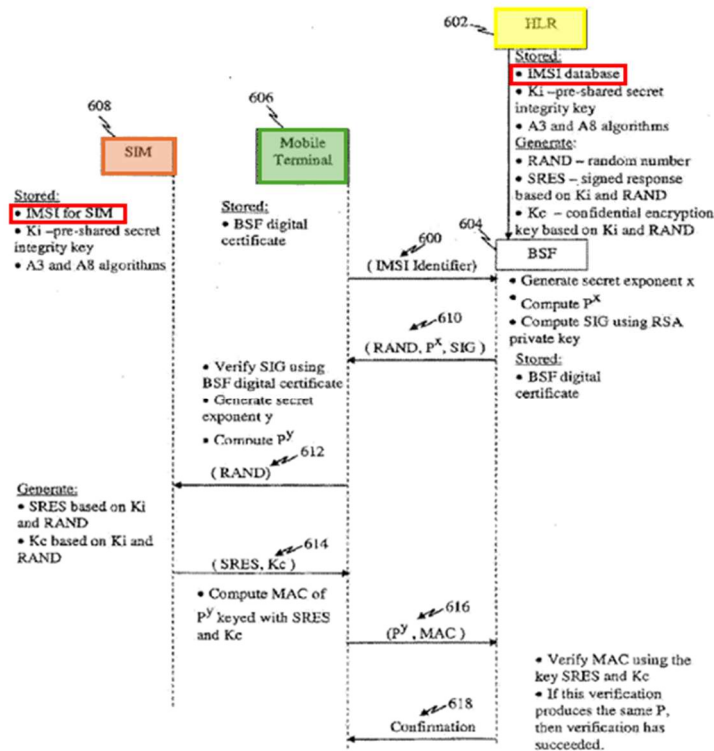


Figure 6

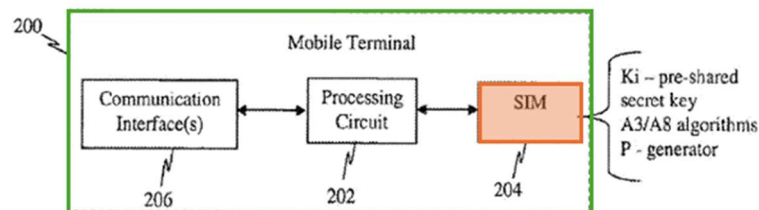


Figure 2

Wang similarly discloses that the mobile device (WTRU) stores a user ID in the form of an IMSI as part of the “initial security parameters.” Ex-1006 ¶15.

Claim element	Semple	Wang
Server public key	P ^x	k _a
Module identity	IMSI	

(3) Storing a pre-shared secret key

As shown in Figure 6 below, Semple teaches that the “process of registering with a service provider may involve authenticating MT 102 by using a pre-shared secret key (e.g., stored in a GSM SIM, CDMA Authentication Module, or other legacy module).” Ex-1005 ¶27. Semple also teaches that SIM 204 “may contain a secret key Ki” (red). Ex-1005 ¶33, Fig. 6 (“Ki=pre-shared secret integrity key”); *see also id.*, Fig. 2 (“Ki=pre-shared secret key”); Ex-1002 ¶75.

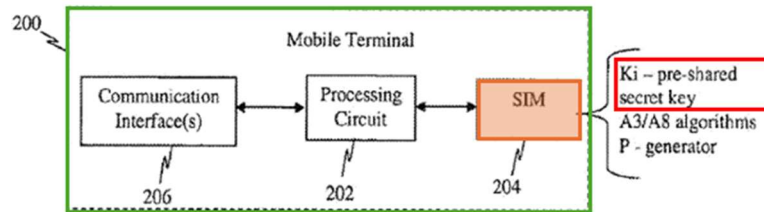
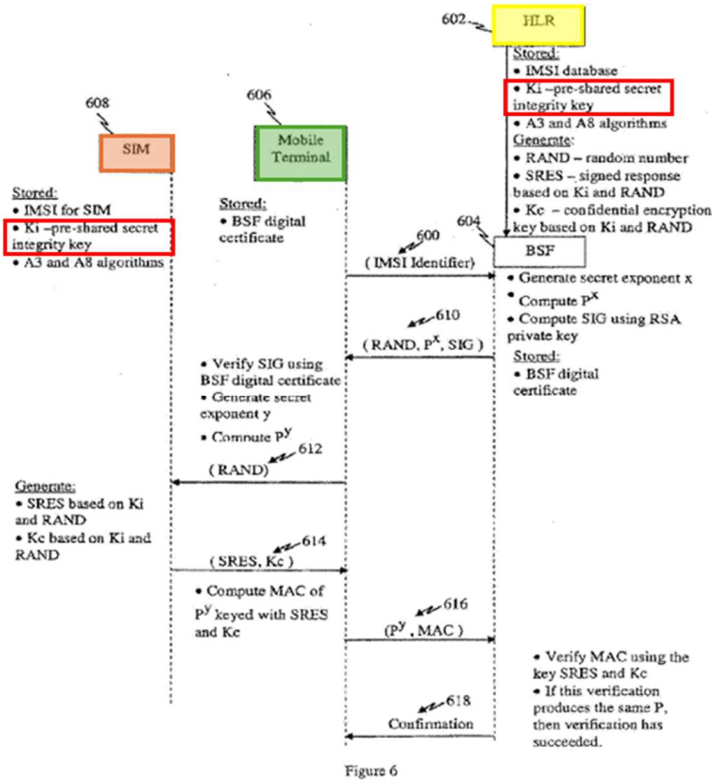


Figure 2

Claim element	Sample	Wang
Server public key	P^x	k_a
Module identity	IMSI	
Pre-shared secret key	Secret key Ki	

(4) Storing cryptographic algorithms including a symmetric ciphering algorithm

As shown in Figure 6 below, Semple teaches that “SIM 204 may contain a secret key K_i , an implementation of GSM authentication and key agreement algorithms (i.e., the GSM A3/A8 algorithms)” (red). Ex-1005 ¶33, Fig. 6; *see also id.*, Fig. 2. Semple further teaches that MT 102 and BSF 106 “may also share a predetermined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange,” (Ex-1005 ¶33), where P is “previously provisioned to both the BSF 604 and MT 606.” Ex-1005 ¶48. Semple stores the Elliptic Curve Diffie-Hellman algorithms (the symmetric ciphering algorithms) because Semple later uses them in claim step 1(b)(4) to encrypt module data using the symmetric ciphering key generated in the ECDH exchange, as described further below. Ex-1002 ¶76. Semple’s stored cryptographic algorithms thus include a symmetric ciphering algorithm, which is later used to apply the symmetric ECDH key. Ex-1002 ¶76.

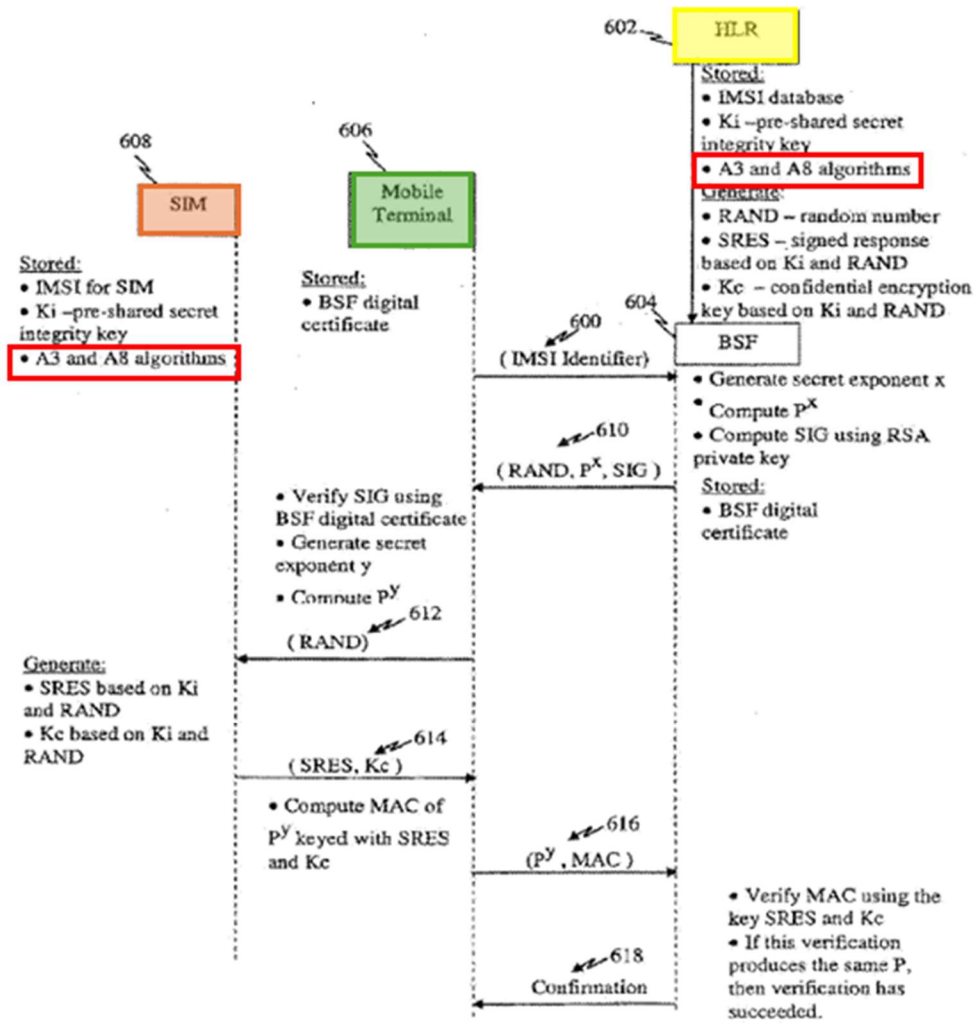


Figure 6

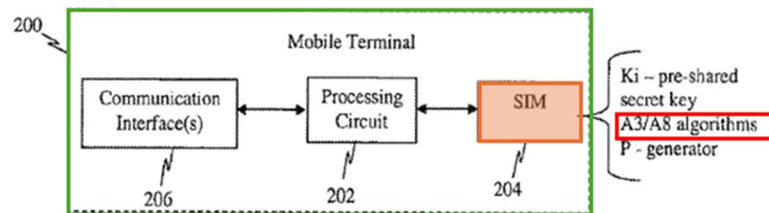


Figure 2

Claim element	Sample	Wang
Server public key	P ^x	k _a
Module identity	IMSI	
Pre-shared secret key	Secret key Ki	

Cryptographic algorithms	GSM A3/A8; generator P and ECDH symmetric algorithms	
---------------------------------	---	--

- e. **Element 1(b)(2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;**

Simple-Wang teaches Element 1(b)(2). Ex-1002 ¶77.

Simple teaches deriving a module private key and a corresponding module public key using the cryptographic algorithms. Simple teaches a Diffie-Hellman key derivation (ECDH) process based on a shared cryptographic parameter P, “where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of an elliptic curve.” Ex-1005 ¶48. As described above for Element 1(b)(1), “BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x ” which is sent to the MT. *Id.* ¶¶48-49. MT 606 performs the converse process and “generates a random number y and computes P^y ,” *id.* ¶49, where y is the module private key and P^y is the corresponding module public key. Ex-1002 ¶78. This private/public key pair is generated according to algorithms and parameters stored on the MT enabling a Diffie-Hellman key exchange. Ex-1005 ¶33 (“BSF 106 and MT 102 may also share a pre-determined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange.”). This process is shown in Figure 6, below (pink).

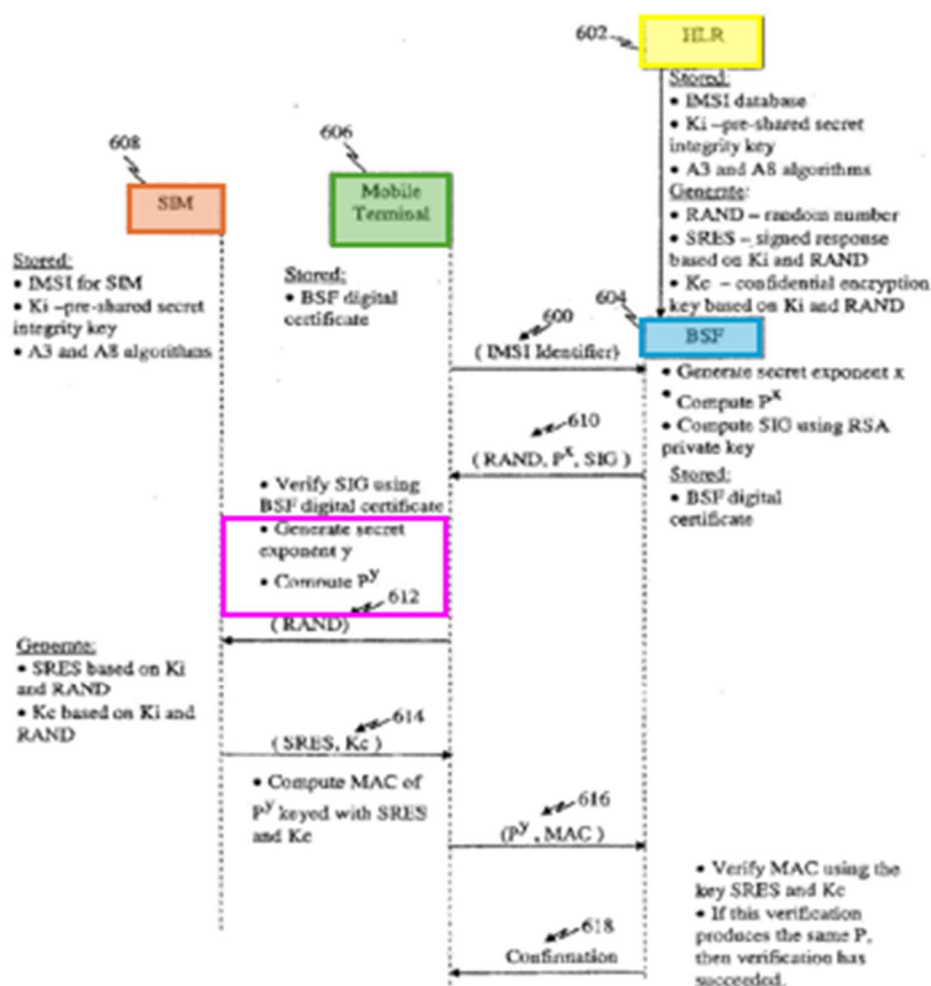


Figure 6

Claim element	Sample	Wang
Server public key	P^x	k_a
Module identity	IMSI	
Pre-shared secret key	Secret key Ki	
Cryptographic algorithms	GSM A3/A8; generator P and ECDH symmetric algorithms	
Module private key	Secret exponent y	
Module public key	P^y	

- f. **Element 1(b)(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;**

Semple-Wang teaches Element 1(b)(3). Ex-1002 ¶79.

- (1) **Deriving a symmetric ciphering key using an elliptic curve integrated encryption scheme with the server public key and the module private key**

Once Semple's MT has received the server public key P^x and has derived its own module private key y , it can calculate a Diffie-Hellman shared secret $(P^y)^x$, or P^{xy} ; the BSF similarly calculates $(P^y)^x$, or P^{xy} , using its own private key x and the module public key P^y , thus allowing them to mutually derive the same shared secret, P^{xy} . Ex-1005 ¶51 ("MT 606 and BSF 604 have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively."). Semple teaches using a Diffie-Hellman key exchange using a parameter P that is a generator of "a cyclic group, such as the multiplicative subgroup of a finite field or a *point in an elliptic curve*." *Id.* ¶¶33, 48. A POSITA would have understood Semple to disclose an elliptic curve integrated encryption scheme, as this is by definition an ECDH (elliptic curve Diffie-Hellman) key exchange. Ex-1002 ¶80. From the shared Diffie-Hellman secret P^{xy} , Semple discloses "[a] key for further communications may then be computed, for instance, as a hash of P^{xy} , possibly including further information known to both the MT and

BSF.” Ex-1005 ¶51. Such “key for further communications” is the recited “symmetric ciphering key.”

(2) And an ANSI standard X-9.63 key derivation function

While Semple refers generally to using a hash function to generate the “key for further communications,” it was commonly known to apply one of several specific hash-based key derivation functions (KDFs) to a Diffie-Hellman shared secret in order to generate a cryptographically sound symmetric key with desirable properties. Ex-1002 ¶81. It would have been an obvious design choice for Semple’s symmetric ciphering key to have been derived by applying the ANSI standard X-9.63 key derivation function to the Diffie-Hellman shared secret because this was a well-known concept by 2013, and X-9.63 was developed specifically for provisioning SIM environments such as those taught by Semple. *See* Ex-1001, 39:61-65 (identifying X-9.63 as an exemplary key derivation function); Ex-1002 ¶81. Specifically, a POSITA would have been motivated to apply SEC1’s well-known ECIES plus X9.63 key derivation function to process P^{xy} into a shared encryption key with good cryptographic properties according to a standardized algorithm.⁶ Ex-1002 ¶81 (citing Ex-1012, 31-33 (“The list of supported key

⁶ Ground 5, below, expressly combines Semple and Wang with SEC1 for this purpose.

derivation functions at this time is: ANSI-X9.63-KDF The key derivation function ANSI-X9.63-KDF is the simple hash function construct described in ANSI X9.63 [X9.63].”), 56-57 (“Entities U and V should perform the following setup procedure to prepare to use the elliptic curve Diffie-Hellman scheme ... Let KDF denote the key derivation function chosen.”)). Using Semple’s Diffie-Hellman scheme and applying ANSI X9.63 as the specific hash function would have involved applying a standardized reliable solution that would have been well known to a POSITA. Ex-1002 ¶81.

Claim element	Semple	Wang
Server public key	P^x	k_a
Module identity	IMSI	
Pre-shared secret key	Secret key K_i	
Cryptographic algorithms	GSM A3/A8; generator P and ECDH symmetric algorithms	
Module private key	Secret exponent y	
Module public key	P^y	
Symmetric ciphering key	Hash / KDF of P^{xy}	

- g. Element 1(b)(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;**

Semple-Wang teaches Element 1(b)(4). Ex-1002 ¶82. As discussed above, Wang discloses encrypting communications between the mobile device WTRU and the authentication server HLR/AuC. Specifically, Wang stresses the importance of

encrypting the *module identity IMSI* rather than sending it in the clear (as Semple does). Ex-1006 ¶28 (“The present invention provides methods for initial loading and generation of security parameters, encryption key arrangements between the WTRU 210 and a network, *IMSI encryption*, and WTRU signaling adjustment for the IMSI encryption for the initial NAS signaling messages, which will be explained in detail hereinafter.”). Specifically, Wang discloses “ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast)” and then sending the “connection request message including ciphered attach message and IMSI along with the MAC-I.” *Id.* ¶31. “Unlike the conventional attachment procedure, the attach message *and the IMSI* are protected with the initial CK and IK.” *Id.*

However, a POSITA would have been motivated to further improve this process by replacing the initial ciphering CK from the USIM with the *derived* “symmetric ciphering key” of Semple and using it to encrypt the module encrypted data instead of using CK because doing so would remove reliance on a long-term stored secret that could be compromised and replace it with a freshly generated Diffie-Hellman key to provide enhanced security. Ex-1002 ¶83.

Thus, in the Semple-Wang combination, the attach message from the mobile terminal to the authentication server that includes the IMSI identity would be encrypted with the symmetric encryption key derived from a Diffie-Hellman

exchange as described in Semple. As explained below for element 1(b)(5), a POSITA would have been motivated to send the IMSI in encrypted form with message 616 after deriving the symmetric key in order to protect it from being exposed when sent in the clear. Ex-1002 ¶84. The symmetric algorithms included with the stored cryptographic algorithms would govern how the ECDH symmetric key is applied to the message including the IMSI. Ex-1002 ¶84. A POSITA would have been motivated to combine Semple-Wang and had a reasonable expectation of success in doing so for the reasons described in Section XII.A.1. Ex-1002 ¶84.

- h. Element 1(b)(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and**

Semple-Wang teaches Element 1(b)(5). Ex-1002 ¶85.

- (1) Sending a message to a server for the wireless network comprising the module encrypted data and the module public key**

Wang teaches that it is desirable to protect “the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure” (Ex-1006 ¶13) and does so by ciphering it with “initial security parameters ... loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network.” *Id.* ¶15. As discussed above, the Semple-

Wang system instead encrypts the message with the symmetric key derived through Semple's Diffie-Hellman key exchange (at element 1(b)(3)), such that the message sent to the server includes the module-encrypted data (which includes the IMSI). The message also includes the module public key (P^y), as described further below.

As described above for element 1(b)(3), Semple's BSF 604 "generates a random secret exponent x and computes a Diffie-Hellman public key P^x , where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606," and then sends P^x to MT 606. Ex-1005 ¶48; Fig. 6, 610. MT 606 "generates a random number y ," "computes P^y ," and sends P^y to the BSF. Ex-1005 ¶49, Fig. 6, 616 (pink box). While Semple by itself describes the MT sending the IMSI before doing the Diffie-Hellman exchange, that is not necessary since computing x and P^x does not depend on IMSI or the pre-shared key associated with it. Thus, a POSITA would have understood that the MT could compute the ECDH symmetric key and encrypt IMSI, as taught by Wang, rather than sending it in the clear and that doing so would improve security and address the known problem of IMSI capture. Ex-1002 ¶¶86-87. Then, once the BSF receives P^y from the MT (along with the encrypted IMSI) and is able to decode the encrypted IMSI, (by independently deriving the ECDH key from P^y), it can then continue with the handshaking process of Figure 6. Ex-1002 ¶87.

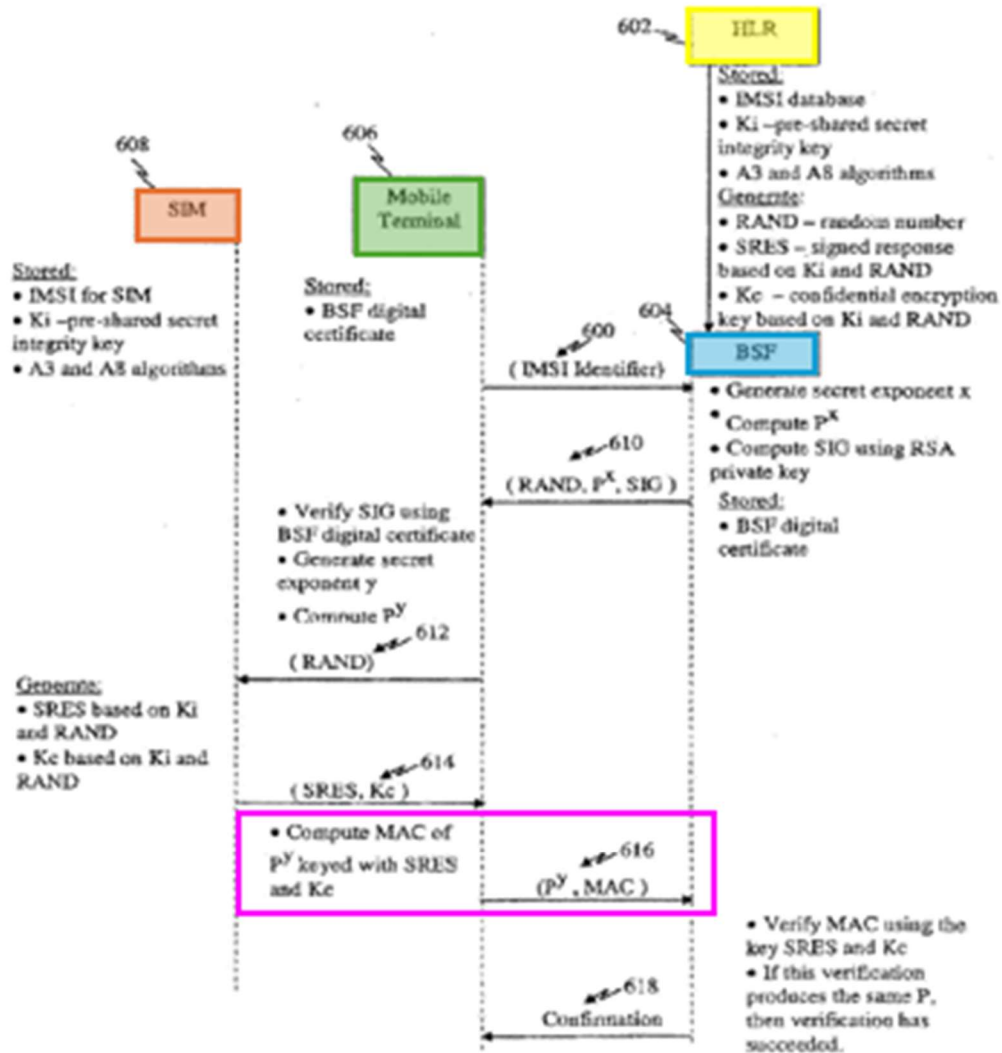
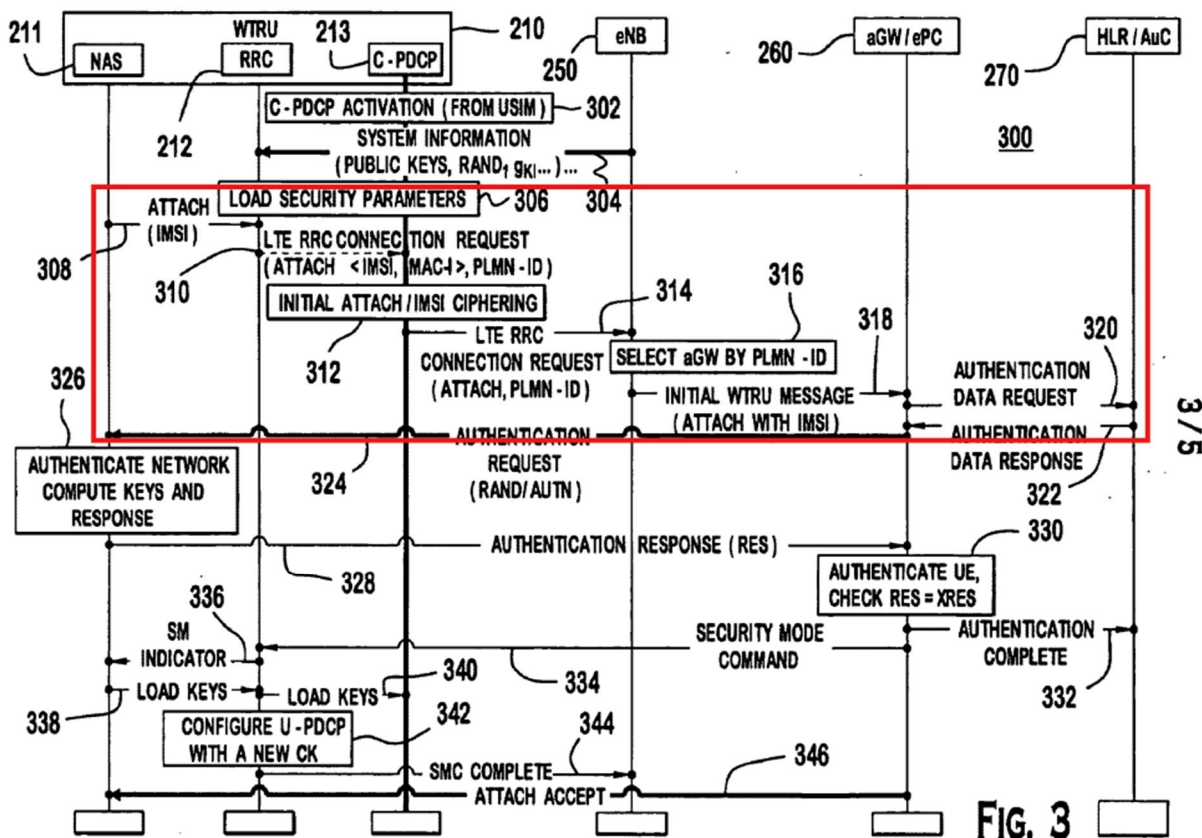


Figure 6

As explained above, Wang discloses preparing encrypted module data that includes the IMSI, and the encryption would be performed using the symmetric ciphering key in the combined Simple-Wang system. Wang discloses that the encrypted IMSI is sent from the WTRU to the network servers eNB, aGW/ePC, HLR/AuC, as shown in Figure 3, below. Ex-1006 ¶31 (“The C-PDCP layer 213

then performs ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer 213 (steps 312, 314)”, Fig. 3.



It would have been obvious to a POSITA to include Wang’s encrypted IMSI and MAC-I with Semple’s message 616 transferring P^y and a MAC as shown in Semple’s Figure 6, below, modified to include Wang’s message. Ex-1005, Fig. 6 (purple); Ex-1002 ¶88. In particular, by that time, Semple’s MT would already have received P^x and have calculated y and P^y , so it would already have been able to

calculate P^{xy} , apply the KDF function to derive the symmetric ciphering key and then would have used that symmetric ciphering key to encrypt IMSI according to the Semple-Wang combined system and then could have included the encrypted IMSI in message 616 to the BSF. Ex-1002 ¶88. Furthermore, because the MT already has the pre-shared key (K_i , pre-shared secret integrity key), it can use that key to prepare the MAC-I (to the extent necessary) before the authentication server and HLR have looked up the shared key corresponding to the decrypted IMSI value. Ex-1002 ¶88.

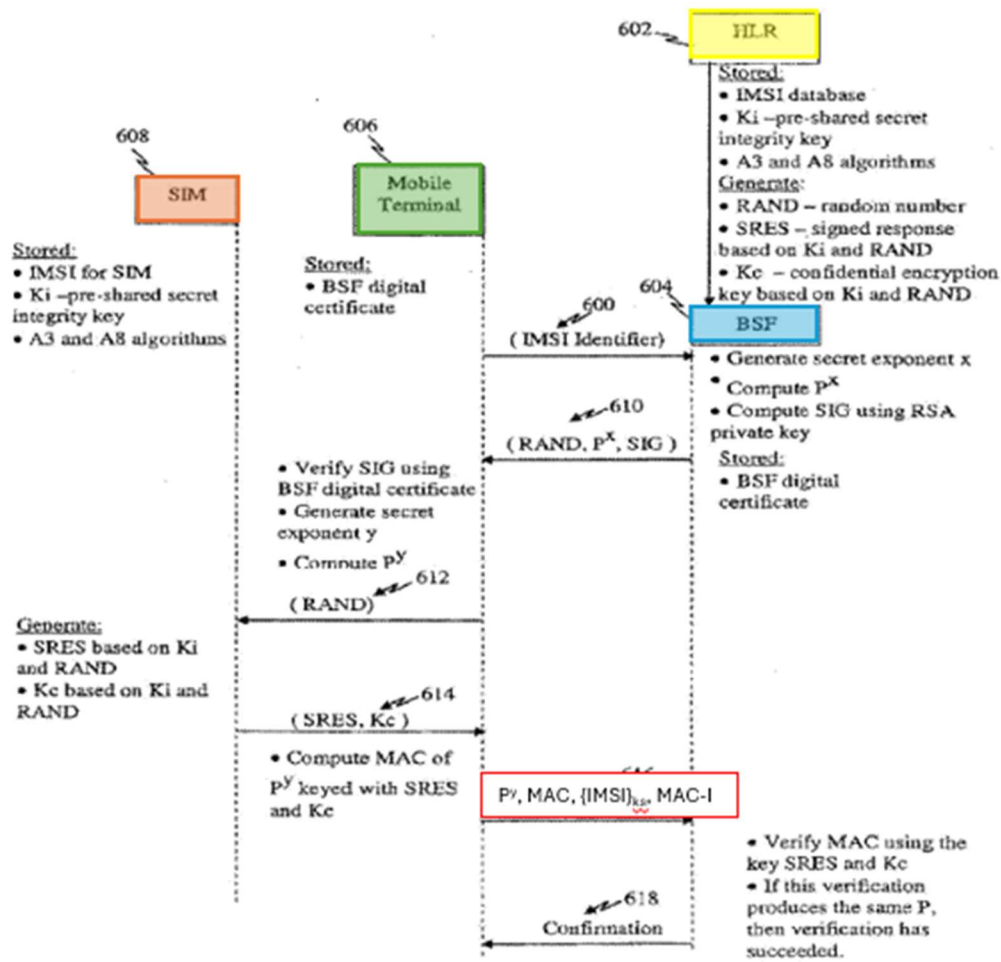


Figure 6

(2) Wherein the server mutually derives the symmetric ciphering key using at least the module public key and

As discussed above, Semple teaches that the BSF “receives P^y ,” which is the module public key. Ex-1005 ¶50, Fig. 6 (purple). Semple further teaches that the MT and BSF “have thus carried out a mutually authenticated Diffie-Hellman key exchange and agree on a key P^{xy} which they compute respectively.” Ex-1005 ¶51. Semple further teaches that the symmetric ciphering key (“a key for further communications”) is computed from P^{xy} using a hash function (i.e., the ANSI X9.63

KDF) and possibly “further information known to both the MT and BSF.” *Id.* In other words, the BSF server *derives the same symmetric ciphering key as the MT.* *Id.*; Ex-1002 ¶89.

(3) Wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity

Sample teaches that the BSF sends the IMSI to the HLR, which “may be operated by the service provider for the subscriber whose SIM is contained in MT,” so that the BSF “may verify whether the IMSI [] belongs to a MT that subscribes to the network.” Ex-1005 ¶48. As described above (element 1(b)(1)), Figure 6 also shows that the HLR includes an “IMSI database” and the “Ki=pre-shared secret integrity key.” *Id.*, Fig. 6. Moreover, Sample teaches that the HLR selects “a 128-bit random challenge RAND and together with *pre-shared secret key Ki*, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively,” and “then provides the triplets (RAND, SRES, Kc) to the BSF,” “*corresponding to the identity IMSI 600 of SIM 608.*” Ex-1005 ¶48. In other words, the network looks up the shared secret Ki based on the IMSI, as was the conventional procedure in 3G communication systems. Ex-1002 ¶90; *see also* Ex-1006 ¶47 (“Given the *secret key K* 604, which is shared between the WTRU 210 and the network 230 *via ISMI*, the

generated IK 502 bears affinity to the unique association between the WTRU 210 and the network 230”).

Claim element	Sample	Wang
Server public key	P^x	k_a
Module identity	IMSI	
Pre-shared secret key	Secret key K_i	
Cryptographic algorithms	GSM A3/A8; generator P and ECDH symmetric algorithms	
Module private key	Secret exponent y	
Module public key	P^y	
Symmetric ciphering key	Hash / KDF of P^{xy}	
Module encrypted data	Use KDF (P^{xy}) to create key for symmetric encryption	Encrypt IMSI
Send module public key and module encrypted data and	P^y and module encrypted data sent to server	Initial WTRU message with encrypted IMSI

i. Element 1(b)(6) authenticating with the wireless network using a message digest with the pre-shared secret key.

Sample-Wang teaches Element 1(b)(6). Ex-1002 ¶91.

As shown in Figure 6 below, Sample teaches that the BSF “verifies the MAC using the SRES and K_c which it received in the authentication triplet from the HLR” and “[i]f this MAC is correct, this verifies that the MT” possesses “the correct SIM 608, and a confirmation message 618 may be sent to the MT.” Ex-1005 ¶50, Fig. 6 (purple). Moreover, the SRES (signed challenge response) and K_c (ciphering key) are calculated from the pre-shared secret key K_i . *Id.* ¶36 (“[T]he pre-shared secret

key K_i and random number (e.g., RAND) may be used to generate secret keys (e.g., SRES and K_c) that are used to generate the authentication challenge parameters.”). A MAC is a message digest created using a secret symmetric key. Ex-1002 ¶92 (citing Ex-1033 (Boyd-Mathuria), 18). Moreover, a POSITA would have understood that the MAC is authenticated using the pre-shared secret key because “the SRES and K_c obtained from the HLR” in the triplet correspond “to random number RAND and pre-shared secret key K_i .” Ex-1005 ¶43; Ex-1002 ¶92.

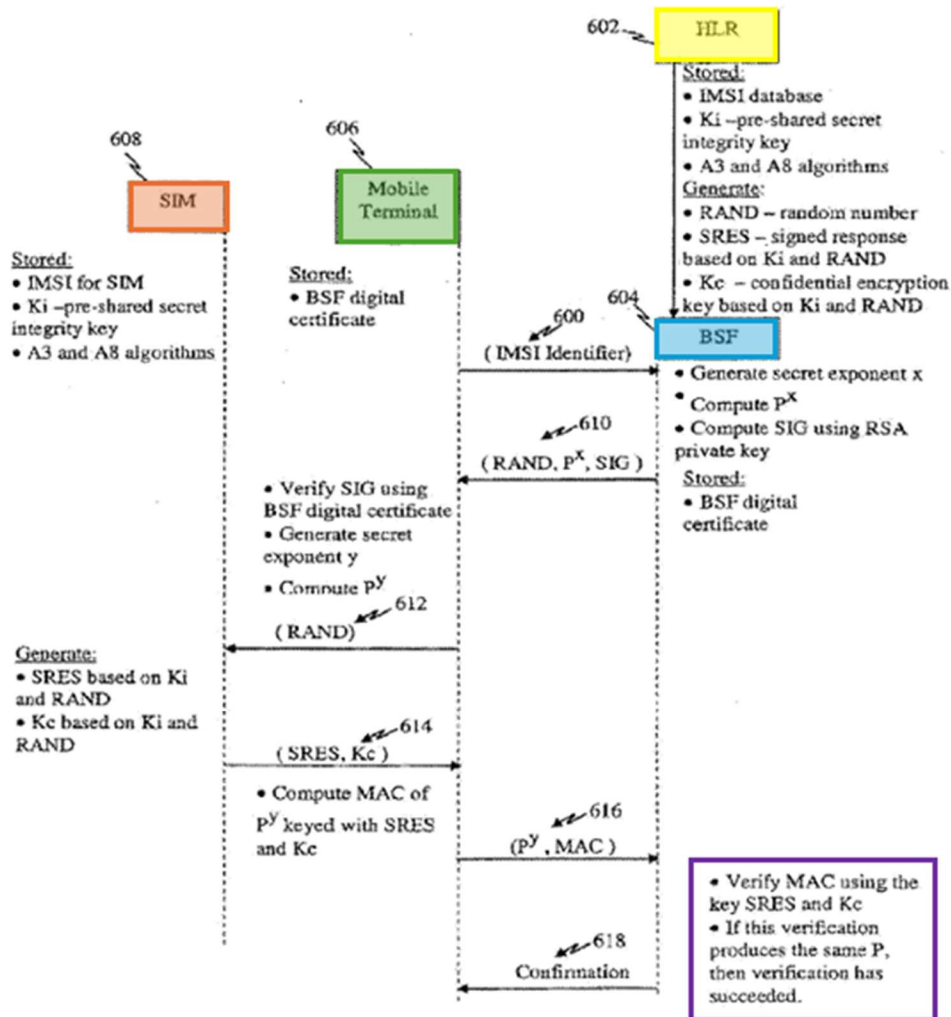
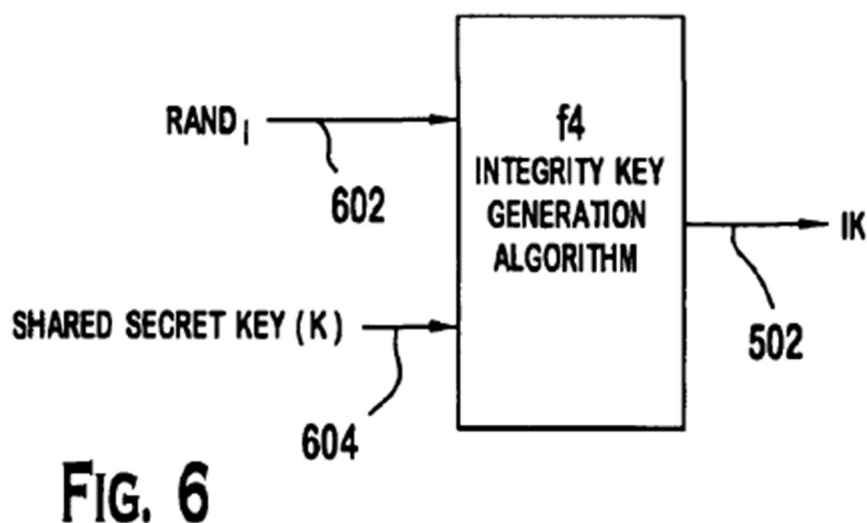


Figure 6

Wang similarly discloses that the encrypted identifier IMSI is sent with MAC-I (a MAC generated with the integrity key IK) for authentication: “The WTRU 210 uses the initial IK 502 to generate an MAC-I 512 for the first NAS/RRC message and sends the generated MAC-I 512 to the network 230 along with the NAS/RRC message. The LTE network 230 generates an expected MAC-I (XMAC-1) 514 with the same parameters 502-510 and compares the received MAC-I 512 and the XMAC-I 514 to verify the message integrity after it has decoded the IMSI for the WTRU 210.” Ex-1006 ¶¶10, 46. And the IK is generated from pre-shared key K and a random value. *Id.* ¶47, Fig. 6 (below). Thus, a message digest based on the pre-shared key is used for network authentication. Ex-1002 ¶¶93-94.



Claim element	Sample	Wang
Server public key	P ^x	k _a
Module identity	IMSI	
Pre-shared secret key	Secret key Ki	

Cryptographic algorithms	GSM A3/A8; generator P and ECDH symmetric algorithms	
Module private key	Secret exponent y	
Module public key	P^y	
Symmetric ciphering key	Hash / KDF of P^{xy}	
Module encrypted data	Use KDF (P^{xy}) to create key for symmetric encryption	Encrypt IMSI
Send module public key and module encrypted data and	P^y and module encrypted data sent to server	Initial WTRU message with encrypted IMSI
Message digest with pre-shared secret key	MAC	MAC-I

Thus, Semple-Wang renders obvious Claim 1.

3. Dependent Claims 2-7, 11-12, 14-16, and 18-20

- a. **Claim 2: The mobile device of claim 1, wherein the message further comprises a module identity string, the module identity string comprising a temporary identification for the mobile device.**

Semple-Wang teaches Claim 2. Ex-1002 ¶95.

As explained in Section XII.A.2.h, in the Semple-Wang combination, the message sent from the MT to the BSF includes (P^y , MAC), as taught by Semple, and the encrypted IMSI and MAC-I, as taught by Wang. A POSITA would have understood that “ P^y , MAC, IMSI (encrypted), MAC-I” is a module identity string comprising a temporary identification for the mobile device because, for example, the P^y parameter and encrypted IMSI (which is encrypted with a key based on P^{xy}) allow the BSF to determine a key that can be used to retrieve the permanent identity

of the mobile device. Ex-1002 ¶¶96. Specifically, given P^y , the BSF is able to calculate P^{xy} and derive the symmetric ciphering key that is used to decrypt IMSI. Ex-1005 ¶¶50-51; Ex-1002 ¶¶96. This is consistent with how the challenged patent describes what it means by a temporary identification. Ex-1001, 88:23-31 (“Message 208 could include module identity string 904, which *could represent a temporary or transient string or number used by module 101* and server 105 to *associate and identify message 208 with module identity 110*. Module identity string 904 could also comprise a module identity 110. Server 105 *can use module identity string 904 to select a symmetric key 127 in order to decrypt module encrypted data 403*, since module identity string 904 may preferably be not encrypted.”).

- b. Claim 3: The mobile device of claim 1, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network.**

Semple-Wang teaches Claim 3. Ex-1002 ¶¶97.

(1) Pre-shared secret key comprises a key K

Semple teaches “a pre-shared secret key (e.g., K_i) known to a network database and a subscriber identification module in the MT.” Ex-1005 ¶36. A POSITA would have understood that Semple’s pre-shared secret key “ K_i ” corresponds to the recited “key K.” Ex-1002 ¶98. Specifically, Semple’s pre-shared key K_i is used to calculate K_c and SRES, which are known in the ETSI and 3GPP

specifications to be calculated from the pre-shared subscriber key K. Ex-1002 ¶¶98.

To the extent PO argues that the key must be named “K,” this is obvious in view of Wang, which explicitly teaches a “shared secret key K.” Ex-1006 ¶¶8, 47.

(2) Mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K

Sample teaches that a “random number (e.g., RAND) received in the authentication challenge and the pre-shared secret key (e.g., Ki), stored in the subscriber identification module of the MT, may be used to generate keys (e.g., SRES and Kc) that are used to generate the authentication response parameters.” Ex-1005 ¶37. Sample also teaches that “[t]he BSF receives the authentication response and verifies whether it originates from the MT based on secret keys (e.g., SRES and Kc) independently obtained by the” BSF from the HLR’s “database based on the random number RAND and the pre-shared secret key (e.g., Ki).” Ex-1005 ¶38. Secret keys SRES and KC correspond to the recited mutually derived response. Ex-1002 ¶99.

(3) Mobile device receives the random value from the wireless network

Sample teaches that “the random number (e.g., RAND)” was “received in the authentication challenge” by MT. Ex-1005 ¶38; *see also id.* ¶41 (“the HLR/AuC selects a 128-bit random challenge RAND which is input, together with Ki, into two algorithms A3 and A8 to yield 32-bit output SRES and 64-bit output Kc,

respectively,” “[t]riplets (RAND, SRES, Kc), corresponding to the SIM of the requesting MT, are then provided to the BSF to authenticate the SIM inside the requesting MT,” and “[t]he BSF then challenges the MT with a random number RAND (generated by the HLR) and other parameters 506”), Fig. 6 (610); Ex-1002 ¶100.

- c. Claim 4: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K.**

Sample-Wang teaches Claim 4. Ex-1002 ¶¶101-102.

Sample teaches that “the pre-shared secret key (e.g., K_i)” is “stored in the subscriber identification module of the MT.” Ex-1005 ¶37; *see also* Ex-1006 ¶34 (Wang teaches “shared secret key K”).

- d. Claim 5: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.**

Sample-Wang teaches Claim 5. Ex-1002 ¶103.

Sample teaches that “MT 102 may be a legacy wireless communication device that registers or connects with a service provider using a predefined protocol (e.g., a pre-3G protocol) in order to communicate over the network 100.” Ex-1005 ¶27. Sample further teaches that “this process of registering with a service provider may involve authenticating MT 102 by using a pre-shared secret key (e.g., stored in a

GSM SIM, CDMA Authentication Module, or other legacy module).” Ex-1005 ¶27. Thus, a POSITA would have understood that the pre-shared secret key is stored in the SIM before the MT tries to authenticate with the wireless network. Ex-1002 ¶104. It was also well known that a SIM card comes with the secret key. Ex-1002 ¶104 (citing Ex-1022 (Ala-Laurila) ¶¶18 (“[t]he SIM is provided by the mobile network GSMNW operator” and “comprises a secret key K_i ”), 25 (“[t]he terminal MT is offered an identifier IMSI and a secret key K_i by the subscriber identity application SIM included therein”)).

- e. **Claim 6: The mobile device of claim 1, further comprising, in step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein, in step (2), the module public key and the module private key are derived using the standard curve.**

Semple-Wang teaches Claim 6. Ex-1002 ¶¶105-106.

- (1) **In step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography**

As explained in Section XII.A.2.d, Semple teaches that “SIM 204 may contain a secret key K_i , an implementation of GSM authentication and key agreement algorithms (i.e., the GSM A3/A8 algorithms).” Ex-1005 ¶33. Semple further teaches that the BSF and MT “may also share a pre-determined generator P of a cyclic group,

such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange.” Ex-1005 ¶33.

(2) In step (2), the module public key and the module private key are derived using the standard curve

As explained in Section XII.A.2.e, Semple teaches that the MT “generates a random number y and computes P^y .” Ex-1005 ¶49. The random secret exponent y generated by the MT corresponds to the recited “module private key” and the Diffie-Hellman public key P^y computed by the MT corresponds to the recited “module public key,” derived using the standard curve. Ex-1002 ¶107 (citing Ex-1033 (Boyd-Mathuria), 196).

f. Claim 7: The mobile device of claim 6, wherein, in step (5), the message further comprises the parameters for the cryptographic algorithms, and wherein the server mutually derives the symmetric ciphering key using at least the module public key and the parameters for the cryptographic algorithms.

Semple-Wang teaches Claim 7. Ex-1002 ¶108.

(1) Message further comprises the parameters for the cryptographic algorithms

Semple teaches that the BSF and MT “share a pre-determined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange.” Ex-1005 ¶33. Moreover, Semple teaches that the MT “computes a message authentication code MAC of P^y , keyed with SRES and K_c , and sends a response (P^y , MAC) 616 to

the BSF.” Ex-1005 ¶49. P^y is a parameter for the cryptographic algorithm because it is the Diffie-Hellman public key for the module. Ex-1002 ¶109.

(2) Server mutually derives the symmetric ciphering key using at least the module public key and the parameters for the cryptographic algorithms

As explained in Section XII.A.2.f, both Semple’s MT and BSF calculate a Diffie-Hellman shared secret P^{xy} , thus allowing them to mutually derive the same shared secret from the module public key P^y and server public key P^x . Ex-1005 ¶51. From the shared Diffie-Hellman secret P^{xy} , Semple discloses computing “[a] key for further communications ... as a hash of P^{xy} ,” i.e., the symmetric ciphering key, which possibly includes “further information known to both the MT and BSF.” Ex-1005 ¶51. The symmetric ciphering key is thus mutually derived using at least P^y and the parameters for the cryptographic algorithms. Ex-1002 ¶110.

g. Claim 9: The mobile device of claim 1, further comprising, in step (2), deriving (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number.

Semple-Wang teaches Claim 9. Ex-1002 ¶111.

As explained in Section XII.A.2.e, Semple’s random secret exponent y corresponds to the recited “module private key” and Semple’s Diffie-Hellman public key P^y corresponds to the recited “module public key.” Semple teaches that P^y is a computed Diffie-Hellman public key “where P is a generator of a cyclic group

previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve.” Ex-1005 ¶48. Diffie-Hellman is a key pair generation algorithm. Ex-1002 ¶112 (citing Ex-1033 (Boyd-Mathuria), 196). Semple further teaches that the MT “generates a random number y .” Ex-1005 ¶49. A POSITA would have understood that y would have been generated using a random number generator because it was well known that “[s]ecure random or pseudorandom number generation is required during key generation” in “the key deployment procedure of the elliptic curve Diffie-Hellman scheme.” Ex-1002 ¶112 (citing Ex-1012 (SEC1), 93-94, 77 (“The surest way to secretly generate a key is to generate it randomly.”)).

h. Claim 11: The mobile device of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device.

Semple-Wang teaches Claim 11. Ex-1002 ¶113.

Semple teaches that “a storage medium may represent one or more devices for storing data, including read-only memory (ROM)” and “flash memory devices,” which are nonvolatile memory. Ex-1005 ¶22. Semple further teaches that the “SIM 204 ... is inserted in a MT 102 containing a public key ... corresponding to a private key in BSF 106.” Ex-1005 ¶33. Thus, the server public key is stored in the MT, which includes nonvolatile memory. Ex-1002 ¶114. As also explained in Section XII.A.2.d, the MT receives the public key P^x from BSF 604 and evidently stores it

because MT later uses it to compute P^{xy} . Ex-1005 ¶48. A POSITA would have understood that P^x would be stored in nonvolatile memory so that it would not be lost if the mobile device were to be turned off. Ex-1002 ¶114. Further, Semple teaches “[t]he SIM is designed to be tamper-proof and contains secret data and algorithms that cannot be easily read out by a user.” Ex-1005 ¶40. And Semple notes that if the key P^{xy} is stored in the MT rather than in the SIM, it “should be deleted if the SIM 608 is removed from the MT,” *id.* ¶51, suggesting that these parameters used in the Diffie-Hellman exchange are otherwise permanently stored. *See also* Ex-1002 ¶114 (citing Ex-1021 (Farnham) ¶38 (“The non-volatile data memory 316 stores a public key, preferably within a digital certificate, the server storing a public key for one or more mobile users, the mobile device storing public keys for one or more server operators.”)).

- i. **Claim 12: The mobile device of claim 1, wherein the server comprises a plurality of computers, wherein the plurality includes at least one sub-server and at least one database.**

Semple-Wang teaches Claim 12. Ex-1002 ¶115.

As shown in Figure 1 below, Semple teaches network architecture 100, which includes “a home location register (HLR) 104, a bootstrapping server function (BSF) 106, and at least one network application function (NAF) 108.” Ex-1005 ¶26, Fig. 1. Semple further teaches that “HLR 104 and BSF 106 may be hosted in one or more

network devices and/or servers that are part of the infrastructure of the network architecture 100.” Ex-1005 ¶26. The HLR and BSF are thus sub-servers that are hosted in a network server in architecture 100. Ex-1002 ¶116. Moreover, Semple teaches that “HLR 104 includes a database that contains mobile subscriber information for a wireless carrier,” including an IMSI for each MT “belonging to the subscriber.” Ex-1005 ¶26. A POSITA would have understood that the sub-servers correspond to a plurality of computers. Ex-1002 ¶116 (citing Ex-1021 (Farnham) ¶¶20 (“[T]he invention provides computer program code to implement the method at the server-end of the link” and “the steps of the method as implemented ... need not be necessarily be performed within a single processing element but could be distributed amongst a plurality of such elements, for example on a network of processors.”), 32 (“mobile communications network 208 is in turn coupled to a computer network 210, such as the Internet, to which is attached a server 204”), 36 (“the computer system may comprise part of the server 204”)).

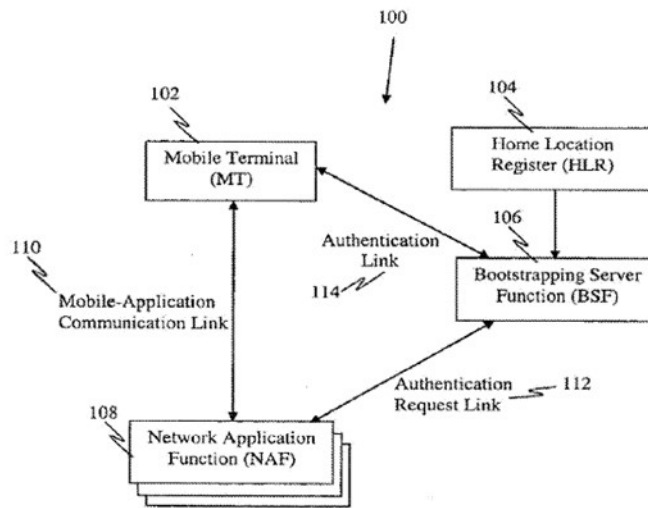


Figure 1

j. Claim 14: The mobile device of claim 1, wherein the wireless network includes the server.

Simple-Wang teaches Claim 14. Ex-1002 ¶¶117-118.

Simple teaches that the MT is coupled to a communication interface “to communicate with a wireless network.” Ex-1005 ¶33. As shown in Figure 1 below, Simple further teaches that network architecture 100 includes HLR 104 and BSF 106, which “may be hosted in one or more network devices and/or servers that are part of the infrastructure of the network architecture 100.” Ex-1005 ¶26.

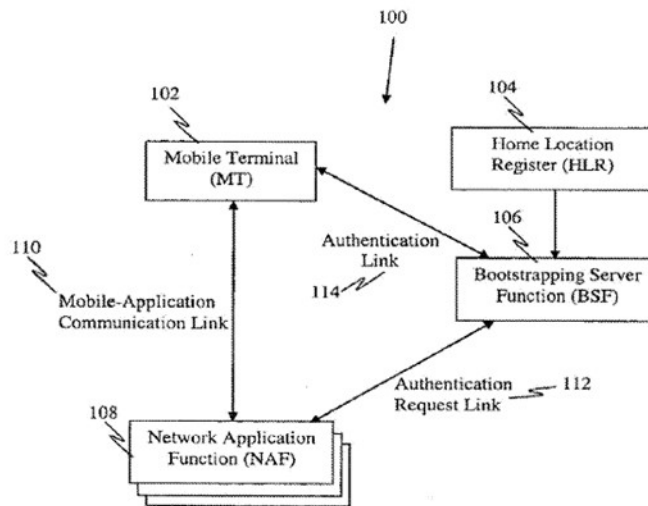


Figure 1

- k. **Claim 15:** The mobile device of claim 1, wherein, in step (1), the module identity is stored in a read-only nonvolatile memory address, wherein the mobile device designates the read-only nonvolatile memory address as read-only for a time interval.

Sample-Wang teaches Claim 15. Ex-1002 ¶119.

Sample teaches that “a storage medium may represent one or more devices for storing data, including read-only memory (ROM).” Ex-1005 ¶22. Sample further teaches that the module identity, i.e., “IMSI is also stored in the Subscriber Identity Module (SIM) of each MT.” Ex-1005 ¶26. Moreover, Sample teaches that the “SIM is designed to be tamper-proof and contains secret data and algorithms that cannot be easily read out by a user.” Ex-1005 ¶40. It would have been obvious that the IMSI is stored as read-only for a time interval because Sample teaches a method that is “not susceptible to replay attacks” (Ex-1005 ¶9) and that its authentication

challenges include a “timestamp” as a parameter. Ex-1005 ¶¶36-37. Wang also teaches that its authentication token includes a “key lifetime.” Ex-1006 ¶7. Using time stamps was a well-known method for hindering replay attacks and would have been an obvious component of Semple-Wang SIM card. Ex-1002 ¶120 (citing Ex-1021 (Farnham) ¶¶51 (“Utilizing a time stamp hinders replay attacks.”), 94 (“Timestamps may be used to provide freshness and (message) and can provide a time window for uniqueness guarantees, message reply. This helps provide security against known-key attacks is required, vulnerable to replay attacks of the unilateral key authentication protocols.”), Cl. 12 (“the secret number is valid for a time period and [] the message further comprises a time stamp ... checking the validity of said secret number using the time stamp”).

I. Claim 16: The mobile device of claim 1, wherein the wireless network comprises at least one base station communicating with a 3GPP wireless technology.

Semple-Wang teaches Claim 16. Ex-1002 ¶121.

Semple teaches that “3G standardization bodies are also developing a Generic Authentication Architecture (GAA), for example, in the third generation partnership project document 3GPP 33.220 Generic Authentication Architecture (GAA), for a generic bootstrapping architecture,” which “relies on the 3G AKA protocol to establish keys between a mobile subscriber’s User Equipment (UE) and a new server entity known as a Bootstrapping Server Function (BSF).” Ex-1005 ¶7. Semple does

not use the terminology “base station” but it would have been obvious that Semple’s wireless network would include at least one base station communicating with the 3GPP wireless technology. Ex-1002 ¶122 (citing Ex-1021 (Farnham) ¶¶2 (incorporating the 3GPP technical specifications by reference), 27 (“A mobile communications device 18 is shown in two-way communication with base station 14 across a radio or air interface 20.”)). This is also taught by Wang.

Wang teaches “a method and apparatus for security protection of an original user identity in an initial access signaling message in a wireless communication system including third generation (3G) LTE.” Ex-1006 ¶15. Wang further teaches that “the terminology ‘eNode-B’ includes but is not limited to a base station, a site controller, an access point (AP), or any other type of interfacing device capable of operating in a wireless environment.” Ex-1006 ¶25; Ex-1002 ¶123.

m. Claim 18: The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.

Semple-Wang teaches Claim 18. Ex-1002 ¶124.

As explained in Sections XII.A.2.f.-XII.A.2.g, it was commonly known to apply one of several specific hash-based KDFs to a Diffie-Hellman shared secret in order to generate a cryptographically sound symmetric key with desirable properties and it would have been an obvious design choice for Semple’s symmetric ciphering

key to have been derived by applying the X-9.63 KDF to the Diffie-Hellman shared secret. Ex-1002 ¶125. It was also well known by 2013 that the X-9.63 KDF process uses an AES algorithm with a length of 128 bits. *See, e.g.*, Ex-1002 ¶125 (citing Ex-1012, 35-36 (listing supported symmetric encryption schemes: “AES-128 in CBC mode” and “AES-128 in CTR mode”)); *see also* Ex-1002 ¶125 (citing Ex-1023 (Brainis) ¶35 (“The generated secret keys can be subsequently used for cryptographic purposes with, e.g., private-key ciphering algorithms such as AES or the information theoretically secure one-time-pad.”)). Using Semple’s Diffie-Hellman scheme and applying an AES-128 algorithm would have involved applying a standardized reliable solution that would have been well known to a POSITA. Ex-1002 ¶125.

n. Claim 19: The mobile device of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.

Semple-Wang teaches Claim 19. Ex-1002 ¶126.

Semple teaches that the module identity, i.e., “IMSI is a unique number that is associated with an MT 102 in the network” and “stored in the Subscriber Identity Module (SIM) of each MT 102.” Ex-1005 ¶26. A typical profile also includes a Mobile Station International ISDN Number (MSISDN), which is the phone number of the device associated with the IMSI. *See, e.g.*, Ex-1029 (CSMG), 16; Ex-1002 ¶127.

o. Claim 20: The mobile device of claim 1, wherein the mobile device comprises a smartphone.

Semple-Wang teaches Claim 20. Ex-1002 ¶128.

Semple teaches that the terms “mobile terminal,” “user equipment,” “mobile device,” “wireless device,” and “wireless mobile device” “are interchangeably used to refer to mobile phones ... and/or other mobile communication/computing devices which communicate, at least partially, through a cellular network.” Ex-1005 ¶24. Moreover, Semple teaches that the secret key K_i and authentication algorithms are stored in a SIM “smart card” in the MT. Ex-1005 ¶47. And Semple teaches that the mobile device may communicate with a network application function “that operates on a networked device, such as commercial transaction applications and/or location-based services.” Ex-1005 ¶28. Semple further teaches that GSM and GPRS protocols “are used for many types of wireless communications including voice, Internet browsing, e-mail, and multimedia data.” Ex-1005 ¶5. A POSITA would thus have understood that Semple’s mobile device is a smartphone because it includes advanced computing capabilities and allows users access to applications and services such as web browsing and email. Ex-1002 ¶129. A POSITA would also have been motivated to implement Semple’s mobile device as a smartphone because smartphones were well known since the 1990s and would have been the most obvious design choice. Ex-1002 ¶129 (citing Ex-1027 (Natarajan) ¶5).

B. Ground 2: Claims 5 and 8 are obvious over Semple in view of Wang and Bhuyan.

1. A POSITA would have been motivated to combine Semple-Wang's teachings with Bhuyan's teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine the teachings of Semple-Wang with Bhuyan and had a reasonable expectation of success in doing so because all three relate to methods for securing wireless communications using authentication and key agreement mechanisms. *See* Section XII.A.1; Ex-1007, Abstract; Ex-1002 ¶130.

Semple teaches that the “process of registering with a service provider may involve authenticating MT 102 by using a pre-shared secret key (e.g., stored in a GSM SIM, CDMA Authentication Module, or other legacy module).” Ex-1005 ¶37. A POSITA would have understood that the pre-shared secret key is stored in the SIM before the MT tries to authenticate with the wireless network because it was well known that a SIM card comes with the secret key. Ex-1002 ¶131 (citing Ex-1022 (Ala-Laurila) ¶¶18, 25).

Bhuyan teaches that a SIM “is used to store a secret key that is been preloaded onto the card when the card is made” and “shared a priori between the mobile phone and the network operator before any communication is initiated.” Ex-1007 ¶3. Moreover, Bhuyan teaches that the mobile device receives the pre-shared secret key after the user submits a password for the mobile device to the web portal.

Specifically, Bhuyan teaches that “the user first connects to the provisioning server 204 using the computer ... over the internet.” Ex-1007 ¶57. Bhuyan teaches that “[t]he user is then presented with a web page or similar where the user can input details of the mobile device where the security module is required” including “a password which is used ... for securing the security module components on the mobile device.” Ex-1007 ¶57. Bhuyan’s provisioning server then “makes a request to the authentication server 206 for security module parameters.” Ex-1007 ¶59. The authentication server “generates in response to the request” the IMSI and “a secret key Ki.” Ex-1007 ¶59. The provisioning server then “encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device ... using the password provided by the user” along with “the software-based security module,” which “is an application that is run by the mobile device.” Ex-1007 ¶62. The user then “installs the security module on the mobile device 210 and also stores the security parameters IMSI and Ki.” Ex-1007 ¶65; Ex-1002 ¶132.

A POSITA, seeking to improve identity protection in Semple’s protocol, would have been motivated to require that the user submits a pre-shared key code or password for the mobile device to the web portal in order to receive the pre-shared secret key, as taught by Bhuyan. Ex-1002 ¶133. This would improve the security of Semple’s method because, as Bhuyan teaches, “[e]ven if an attacker manages to steal a user’s encryption key (Ki), without knowledge of the user’s password, the attacker

will not be able to use those credentials to gain access to the network or decrypt the session traffic.” Ex-1007 ¶33. In the Semple-Wang-Bhuyan combination, Semple’s pre-shared key would be preloaded in the SIM and the user would submit a pre-shared key code for the mobile device to the web portal in order to receive the security module for the SIM, as taught by Bhuyan. Ex-1002 ¶133.

A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Bhuyan. Ex-1002 ¶134. All three describe methods for securing wireless communications using authentication and key agreement mechanisms. *See* Section XII.A.1; Ex-1007, Abstract. Moreover, Bhuyan teaches that “[p]rovisioning of the security module and associated security parameters can be done online with only an internet or other network connection” and “[n]o complex hardware provisioning is required.” Ex-1007 ¶32. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶134.

2. Dependent Claims 5 and 8

- a. Claim 5: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.**

Semple-Wang in view of Bhuyan (“Semple-Wang-Bhuyan”) teaches Claim 5. Ex-1002 ¶¶135-136.

Semple-Wang teaches Claim 5 for the reasons described in Section XII.A.3.d.

This claim is also taught by Bhuyan. Bhuyan teaches that “a SIM (subscriber identity module), is used to store a secret key that is been preloaded onto the card when the card is made.” Ex-1007 ¶3; *see also id.* ¶45 (“The subscriber is provided with a secret key, K_i , one copy of which is preloaded and stored securely in the SIM card when the card is manufactured, and the other copy stored securely at the AuC.”). Thus, the secret key is “shared a priori between the mobile phone and the network operator before any communication is initiated.” Ex-1007 ¶3.

b. Claim 8: The mobile device of claim 1, wherein the mobile device receives the pre-shared secret key via a wireless 802.11 connection to a web portal after a user for the mobile device submits a pre-shared secret key code for the mobile device to the web portal.

Semple-Wang-Bhuyan teaches Claim 8. Ex-1002 ¶137.

Bhuyan teaches that the mobile device receives the pre-shared secret key via a wireless 802.11 connection to a web portal after a user submits a pre-shared secret key code for the mobile device to the web portal. Specifically, Bhuyan teaches that “the user first connects to the provisioning server 204 using the computer 202 ... over the internet.” Ex-1007 ¶57. The internet connection may be “provided over WiFi” (Ex-1007 ¶53) such as for “a WiFi (IEEE 802.x) network.” Ex-1007 ¶54. Bhuyan teaches that “[t]he user is then presented with a web page or similar where the user can input details of the mobile device where the security module is

required,” including “the mobile phone number.” Ex-1007 ¶57. Bhuyan teaches that “[t]he user also provides a password which is used in the later authentication process and also for securing the security module components on the mobile device.” Ex-1007 ¶57. The user’s password corresponds to the recited “pre-shared secret key code.” Ex-1002 ¶138. Bhuyan’s provisioning server then “makes a request to the authentication server 206 for security module parameters.” Ex-1007 ¶59. The authentication server “generates in response to the request a unique identifier for the mobile device” referred to as the IMSI “as well as a secret key Ki.” Ex-1007 ¶59. Bhuyan further teaches that “[t]he identifier and Ki are both stored securely at the authentication server” and “copies of these parameters are sent to the provisioning server.” Ex-1007 ¶60. The provisioning server then “encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device ... using the password provided by the user” along with “the software-based security module,” which “is an application that is run by the mobile device” and “executes the various methods used for authentication and ciphering.” Ex-1007 ¶62. The user then “installs the security module on the mobile device 210 and also stores the security parameters IMSI and Ki.” Ex-1007 ¶65.

C. Ground 3: Claim 10 is obvious over Semple in view of Wang and Pierce.

- a. Claim 10: The mobile device of claim 9, wherein the random number generator is configured to generate the random number from a seed value, and wherein the seed value comprises data from at least one of a sensor and a radio for the mobile device.**

Semple-Wang in view of Pierce (“Semple-Wang-Pierce”) teaches Claim 10. Ex-1002 ¶139.

As explained in Section XII.A.3.g, a POSITA would have understood that Semple’s random secret exponent y would have been generated using a random number generator because it was well known that “[s]ecure random or pseudorandom number generation is required during key generation” in “the key deployment procedure of the elliptic curve Diffie-Hellman scheme.” Ex-1002 ¶140 (citing Ex-1012 (SEC1), 93-94, 21, 77). It would also have been obvious that Semple’s random number generator would generate the random number from a seed value comprising data from a sensor or radio of the mobile device. Ex-1002 ¶140. Specifically, it was known that when “generating a verifiably random elliptic curve or base point ... the user selects the seed and performs the selection routine” and when “verifying that an elliptic curve or a base point is verifiably random ... the user is given the seed from another user who generated the elliptic curve or base point.” Ex-1002 ¶140 (citing Ex-1012 (SEC1) at 21, 77 (“environmental data, user input, or specialized non-deterministic devices are necessary to use to generate random noise”

and “[h]ash functions may also be used as part of a deterministic random bit generators, also known as pseudorandom number generators, which take an initial seed value, such as one obtained from a truly random noise source (perhaps hashed to be appear uniformly random), and then produce a long stream of bits that appear to be distributed uniformly at random.”)). This is also taught by Pierce.

Pierce teaches generating “cryptographic keys using the [pseudo random number generator] PRNG within the embedded device.” Ex-1010 ¶38. Pierce also teaches that “PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number,” which “is then used to produce the cryptographic keys.” Ex-1010 ¶4. Specifically, Pierce teaches a method for enabling “the automatic generation of strong cryptographic keys by an embedded processing device at the time of manufacturing, before the product is released for distribution to end users ... by supplying the embedded device with entropy data that it uses to seed a pseudo random number generator (PRNG) that is used to generate the keys.” Ex-1010 ¶19; *see also id.* ¶38 (“The entropy data is used as a seed value for the PRNG, which will yield a nearly random number suitable for use in generating strong cryptographic keys ... including asymmetric public-private key pairs.”). Pierce further teaches that the “entropy data can be obtained by the embedded device from any of a number of sources, including those both internal and external to the manufactured product.” Ex-1010 ¶19. The entropy data can be

measured, for example, “from a sensor,” “GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module,” or “an assigned mobile number for the telematics unit.” Ex-1010 ¶36; Ex-1002 ¶141.

A POSITA would have been motivated to generate Semple’s random secret exponent y from a seed value comprising data from a sensor or radio of the mobile device because, as taught by Pierce, “[t]he generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered.” Ex-1010 ¶4. Moreover, as Pierce teaches, using entropy data such as sensor or mobile phone number data “protects against key compromise” (Ex-1010 ¶14) because the data is “transient and not later discernible” or “internal to the manufactured product and not readily discernible without possession and analysis of the product.” Ex-1010 ¶35. In the Semple-Wang-Pierce combination, Semple’s random secret exponent y would be generated by a random number generator using a seed value comprising data from a sensor or radio of the mobile device, as taught by Pierce. Ex-1002 ¶142.

A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Pierce. Ex-1002 ¶143. All three describe methods for securing wireless communications using authentication and key agreement mechanisms. *See* Section XII.A.1; Ex-1010, Abstract. A POSITA would thus have understood that these references disclose interrelated teachings based on

well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶143.

D. Ground 4: Claims 13 and 17-18 are obvious over Semple in view of Wang and Jorgensen.

1. A POSITA would have been motivated to combine Semple-Wang’s teachings with Jorgensen’s teachings and would have had a reasonable expectation of success.

A POSITA would have been motivated to combine the teachings of Semple-Wang with Jorgensen and had a reasonable expectation of success in doing so because all three relate to methods for securing wireless communications using authentication and key agreement mechanisms, including encryption schemes using ECC private keys. *See* Section XII.A.1; Ex-1008 ¶34, Abstract; Ex-1002 ¶¶144-145.

Jorgensen teaches an Encrypted Virtual File System (EVFS), which is a “server-based file system or file and data storage facility” that “allows the users of a network system to store files or data away from their local hosts or client carriers.” Ex-1008 ¶142. Jorgensen further teaches that the use of an EVFS “enhances the user-centric aspect of the secure network system” and “[a]long with encryption, authentication, and other features ... enables secure delivery and stand-alone operation of applications through” the device. Ex-1008 ¶150. Moreover, Jorgensen teaches that “[t]he data transmission between the client and the server is effectuated by a dynamic datagram switch based on a datagram schema” using network protocols such as user datagram protocol (“UDP”). Ex-1008 ¶101.

A POSITA, seeking to enhance the security of Semple's protocol, would have been motivated to include a virtualized server in the system, as taught by Jorgensen. Ex-1002 ¶146. Specifically, including a virtualized server such as the EVFS used in Jorgensen's secure network system in Semple's system would "provide[] enhanced protection to the data and applications belonging to each user" if, for example, the user's mobile device "is lost or stolen" because "the data stored in the EVFS" is "unreadable ... to anyone but the properly authenticated user, the owner of the file who has access to the private ECC encryption key that can unlock the files." Ex-1008 ¶149. Additionally, Semple is silent as to what type of datagram protocol packet it uses to send an authentication message. A POSITA would have been motivated to implement Semple's message to comprise a single user datagram protocol packet, as taught by Jorgensen, because UDP/IP was "the state of the art" for "packet switched network transmission" including in systems employing a key exchange algorithm based on the Diffie-Hellman scheme, such as Semple. Ex-1002 ¶146 (citing Ex-1026 (Nguyen) ¶59, Abstract). In the Semple-Wang-Jorgensen combination, Semple's system would include a virtualized server and its authentication message would comprise a single user datagram protocol packet, as taught by Jorgensen. Ex-1002 ¶146.

A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Jorgensen. Ex-1002 ¶147. All three describe

methods for securing wireless communications using authentication and key agreement mechanisms, including encryption schemes using ECC private keys. *See* Section XII.A.1; Ex-1008 ¶34, Abstract. A POSITA would thus have understood that these references disclose interrelated teachings based on well-understood technologies that would have been amenable to various well-understood and predictable combinations. Ex-1002 ¶147.

2. Dependent Claims 13 and 17-18

- a. Claim 13: The mobile device of claim 1, wherein the server comprises at least one virtualized server operating on at least one computer.**

Semple-Wang in view of Jorgensen (“Semple-Wang-Jorgensen”) teaches Claim 13. Ex-1002 ¶148.

Jorgensen teaches that “a Virtual Private Network (VPN) applies security procedures and tunneling to achieve privacy in network transactions while sharing public network infrastructure such as the Internet.” Ex-1008 ¶66. Jorgensen further teaches that “[t]he routing nodes in the public network are unaware that the transmission is part of a private network” and “[e]ncryption may be used in connection to and within the VPN.” Ex-1008 ¶66. A VPN is a virtualized server operating on a computer. Ex-1002 ¶149. Jorgensen further teaches an Encrypted Virtual File System (EVFS), which is a “server-based file system or file and data storage facility, which allows the users of a network system to store files or data

away from their local hosts or client carriers.” Ex-1008 ¶142; *see also id.* ¶148. Jorgensen also teaches that the EVFS used in its secure network system “provides enhanced protection to the data and applications belonging to each user” if, for example, the user’s mobile device “is lost or stolen” because “the data stored in the EVFS” is “unreadable ... to anyone but the properly authenticated user, the owner of the file who has access to the private ECC encryption key that can unlock the files.” Ex-1008 ¶149. Thus, Jorgensen teaches that the use of an EVFS “enhances the user-centric aspect of the secure network system” and “[a]long with encryption, authentication, and other features ... enables secure delivery and stand-alone operation of applications through” the device. Ex-1008 ¶150.

b. Claim 17: The mobile device of claim 1, wherein the message comprises a single user datagram protocol packet.

Semple-Wang-Jorgensen teaches Claim 17. Ex-1002 ¶¶150-151.

Jorgensen teaches that “[t]he data transmission between the client and the server is effectuated by a dynamic datagram switch based on a datagram schema” such that “[a]ll the data—whether the content data or transaction data—destined for transport through the server is formatted into a datagram.” Ex-1008 ¶101. Jorgensen further teaches that “network protocols such as [user datagram protocol] UDP, HTTP, and HTTPS may be used.” Ex-1008 ¶101.

- c. Claim 18: The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.**

Semple-Wang-Jorgensen teaches Claim 18. Ex-1002 ¶¶152-153.

Semple-Wang teaches Claim 18 for the reasons described in Section XII.A.3.m. Jorgensen also teaches using symmetric ciphering algorithms comprising and AES algorithm. Jorgensen teaches that its “authentication and encryption scheme comprises asymmetrical and symmetrical multi-cipher encryption” are based on “Advanced Encryption Standard (AES).” Ex-1008 ¶33; *see also id.* ¶120.

E. Ground 5: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang and SEC1

1. Independent Claim 1

a. Element 1(b)(3)

Semple-Wang in view of SEC1 (“Semple-Wang-SEC1”) teaches Element 1(b)(3). Ex-1002 ¶154.

To the extent PO argues that Element 1(b)(3)’s requirement to derive a symmetric ciphering key using an ANSI standard X-9.63 KDF is not obvious over Semple-Wang in view of a POSITA’s knowledge of the prior art, this is expressly taught by the Semple-Wang-SEC1 combination in Ground 5. *See* Section XII.A.2.f; Ex-1012, 31-33, 56-57. Semple teaches generating Diffie-Hellman public keys P^x and P^y based on ECC and SEC1 “specifies public-key cryptographic schemes based

on” ECC so a POSITA would have looked to SEC1 for additional implementation details for Semple’s method. Ex-1005 ¶¶33, 48; Ex-1012, 1; Ex-1002 ¶155. Specifically, a POSITA would have been motivated to apply SEC1’s well-known ECIES plus X9.63 KDF to process P^{xy} into a shared encryption key with good cryptographic properties according to a standardized algorithm. Ex-1002 ¶155. A POSITA would have been motivated to combine Semple-Wang with SEC1 and had a reasonable expectation of success in doing so because all three relate to methods for securing wireless communications using similar authentication and key agreement mechanisms. Ex-1002 ¶155.

F. Grounds 6-8

Claims 5, 8, 10, 13, and 17-18 are invalid for the same reasons set forth in Grounds 2-4, respectively, except that in Grounds 6-8 the Semple-Wang-SEC1 combination replaces the Semple-Wang combination of Grounds 2-5. Ex-1002 ¶¶156-158.

XIII. CONCLUSION

Petitioner requests institution of IPR for Claims 1-20 of the ’204 Patent based on each of the grounds in this Petition.

Respectfully Submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner certifies that this petition includes 13,343 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under §42.8, certificates of service, word count, and exhibits.

CERTIFICATE OF SERVICE (37 C.F.R. §42.6(e)(1))

The undersigned hereby certifies that the above document was served on November 7, 2025, by filing this document through the Patent Trial and Appeal Board P-TACTS System, as well as delivering a copy via express mail upon the following attorneys of record for the Patent Owner:

Amster, Rothstein, & Ebenstein LLP
405 Lexington Avenue
Floor 48
New York, NY 10174

A courtesy copy was sent to the below counsel via electronic mail:

Demetrios Anaipakos
Amir H. Alavi
Michael McBride
Steven Jugle
C. Ryan Pinckney
Connie Flores Jones
ALAVI & ANAIPAKOS PLLC
609 Main Street, Suite 3200
Houston, Texas 77002
Telephone: (713) 751-2362
Facsimile: (713) 751-2341
danaipakos@aatriallaw.com
aalavi@aatriallaw.com
mmcbride@aatriallaw.com
sjugle@aatriallaw.com
rpinckney@aatriallaw.com
cfloresjones@aatriallaw.com

Michael F. Heim
Eric J. Enger
R. Allan Bullwinkel
William B. Collier, Jr.
HEIM, PAYNE & CHORUSH, LLP
609 Main St. Suite 3200
Houston, Texas 77002
Telephone: (713) 221-2000
Facsimile: (713) 221-2021
mheim@hpcllp.com
eenger@hpcllp.com
abullwinkel@hpcllp.com
wcollier@hpcllp.com

Andrea L. Fair
Claire A. Henry
MILLER FAIR HENRY PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
(903) 757-6400 (telephone)
andrea@millerfairhenry.com
claire@millerfairhenry.com

Dated: November 7, 2025

Respectfully submitted,

/s/ William M. Fink

William M. Fink (Reg. No. 72,332)

O'Melveny & Myers LLP

1625 Eye Street, NW

Washington, DC 20006

Telephone: (202) 383-5300

Fax: (202) 383-5414

Email: tfink@omm.com

Attorney for Petitioner