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. IPR2026-00116
U.S. Patent No. 11,973,864

DECLARATION OF CHRISTINA PÖPPER IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,973,864

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND AND QUALIFICATIONS 1

III. INFORMATION CONSIDERED 2

IV. RELEVANT LEGAL STANDARDS 3

- A. Claim Interpretation 3
- B. Perspective of One of Ordinary Skill in the Art 3
- C. Obviousness 4

V. LEVEL OF ORDINARY SKILL IN THE ART 7

VI. SUMMARY OF MY OPINIONS 8

VII. TECHNOLOGICAL BACKGROUND 9

- A. A method of authentication with a wireless network 9
- B. Storing a server public key, module identity, cryptographic algorithms, and a pre-shared secret key 10
- C. Deriving a module private key and corresponding module public key associated with the mobile device using the cryptographic algorithms 14
- D. Deriving a symmetric ciphering key with the server public key and module private key 16
- E. Generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm 20
- F. Sending a message to a wireless network server comprising the module encrypted data and the corresponding module public key 22
- G. Authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key 25

VIII. THE '864 PATENT AND ITS FILE HISTORY 26

IX. CLAIM CONSTRUCTION 29

X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES 29

- A. Semple (Ex-1005) 29

TABLE OF CONTENTS
(continued)

Page

B. Wang (Ex-1006) 31

C. Bhuyan (Ex-1007) 33

D. Pierce (Ex-1010) 35

E. Jorgensen (Ex-1008) 35

F. SEC1 (Ex-1012) 37

XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS 37

A. Ground 1: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang. 37

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. 37

2. Independent Claim 1 40

a. Element 1[pre]: A method comprising: 40

b. Element 1(a)(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 a mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm; 42

c. Element 1(a)(2) deriving a module private key and a corresponding module public key associated with the mobile device using the cryptographic algorithms; 49

d. Element 1(a)(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; 51

Petitioner Samsung Ex-1002, 0003

TABLE OF CONTENTS
(continued)

Page

e. Element 1(a)(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; 53

f. Element 1(a)(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the corresponding 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 55

g. Element 1(a)(6) authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key. 61

3. Dependent Claims 2-7, 11-12, 14-16, and 18-20 65

a. Claim 2: The method of claim 1, wherein the message further comprises a module identity string, the module identity string comprising a temporary identification for the mobile device. 65

b. Claim 3: The method 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. 66

c. Claim 4: The method 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. 67

Petitioner Samsung Ex-1002, 0004

TABLE OF CONTENTS
(continued)

Page

d. Claim 5: The method of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network. 68

e. Claim 6: The method 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. 69

f. Claim 7: The method 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.....70

g. Claim 9: The method 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. 71

h. Claim 11: The method of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device. 72

i. Claim 12: The method 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. 73

j. Claim 14: The method of claim 1, wherein the wireless network includes the server. 74

Petitioner Samsung Ex-1002, 0005

TABLE OF CONTENTS
(continued)

Page

k. Claim 15: The method 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. 75

l. Claim 16: The method of claim 1, wherein the wireless network comprises at least one base station communicating with a 3GPP wireless technology.....76

m. Claim 18: The method of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits. 77

n. Claim 19: The method of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.....78

o. Claim 20: The method of claim 1, wherein the mobile device comprises a smartphone.....79

B. Ground 2: Claims 5 and 8 are obvious over Semple in view of Wang and Bhuyan. 80

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. 80

2. Dependent Claims 5 and 8 83

a. Claim 5: The method of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network. 83

Petitioner Samsung Ex-1002, 0006

TABLE OF CONTENTS
(continued)

Page

b. Claim 8: The method 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. 83

C. Ground 3: Claim 10 is obvious over Semple in view of Wang and Pierce. 85

a. Claim 10: The method 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. 85

D. Ground 4: Claims 13 and 17-18 are obvious over Semple in view of Wang and Jorgensen. 88

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. 88

2. Dependent Claims 13 and 17-18.....90

a. Claim 13: The method of claim 1, wherein the server comprises at least one virtualized server operating on at least one computer. 90

b. Claim 17: The method of claim 1, wherein the message comprises a single user datagram protocol packet. 91

c. Claim 18: The method of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits. 92

E. Ground 5: Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang and SEC1 92

1. Independent Claim 1 92

Petitioner Samsung Ex-1002, 0007

TABLE OF CONTENTS
(continued)

Page

a. Element 1(a)(3) 92
F. Grounds 6-8 93
XII. CONCLUSION 93

Petitioner Samsung Ex-1002, 0008

LIST OF EXHIBITS

Ex. No.	Description
Ex-1001	U.S. Patent No. 11,973,864 ("the '864 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. 11,973,864
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
Ex-1017	INTENTIONALLY LEFT BLANK
Ex-1018	INTENTIONALLY LEFT BLANK
Ex-1019	INTENTIONALLY LEFT BLANK

Ex. No.	Description
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")

Petitioner Samsung Ex-1002, 0010

I. INTRODUCTION

1. My name is Christina Pöpper. I am presently an Associate Professor at Computer Science at New York University Abu Dhabi.

2. I have been retained to provide this Declaration by Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Petitioner") as an independent expert consultant in this inter partes review ("IPR") proceeding before the United States Patent and Trademark Office ("PTO").

3. I have been asked by Petitioner Counsel ("Counsel") to consider whether certain references disclose, teach and/or suggest the features recited in Claims 1-20 of U.S. Patent No. 11,973,864 ("the '864 Patent") (Ex-1001), which I understand is currently assigned to currently assigned to Network-1 Technologies, Inc. ("PO"). My opinions and the bases for my opinions are set forth below.

4. I am being compensated at my ordinary and customary consulting rate for my work, which is $500 per hour. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other direct financial interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

5. I am a tenured faculty member of Computer Science at New York University Abu Dhabi (NYUAD). I am the Co-PI of Research at the Center for Cyber

Security (CCSAD) at NYUAD, and a Global Network Associate Professor of Computer Science at the Courant Institute of Mathematical Sciences at New York University. At NYUAD, I am heading the Cyber Security & Privacy (CSP-) Lab. I served as the Program Head of Computer Science at NYUAD from 2023-2025.

6. My research interest is cyber security and privacy and my focus areas are wireless and communication security, including cellular/mobile network security (5G, nextG), secure localization, and aerial cyber security, as well as privacy and anonymity in networks and systems. The research work of my group has been recognized by the Coordinated Vulnerability Disclosure program of GSMA, the GSM Association. I was co-chairing the TPCs of NDSS'25, NDSS'24, and ACNS'24. From 2021 to 2025, I was a member of the Executive Committee of ACM SIGSAC. I have been a member of the Steering Committee of NDSS (Network and Distributed System Security Symposium) since 2025 and of ACM WiSec (ACM Conference on Security and Privacy in Wireless and Mobile Networks) since 2018. I was also ACM WiSec TPC Co-Chair in 2018 and General Chair in 2021.

III. INFORMATION CONSIDERED

7. In preparation for my Declaration, I have considered the materials I discuss in my Declaration, including, for example, the '864 Patent, the references cited by the '864 Patent, the prosecution history of the '864 Patent (including the references cited therein), various background articles and materials referenced in my

Declaration, and the prior art references I identify in my Declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

IV. RELEVANT LEGAL STANDARDS

8. I am not an attorney and offer no legal opinions. For the purposes of my Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Claim Interpretation

9. I have been informed and understand that in an IPR proceeding, claims are to be interpreted according to the *Phillips* claim construction standard. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of a hypothetical "person of ordinary skill in the art" ("POSITA") at the time of the alleged invention. I have been informed and understand that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Patent Trial and Appeal Board ("PTAB").

10. I provide my opinions regarding terms that may require explicit construction to resolve the grounds I present in my Declaration in Section IX.

B. Perspective of One of Ordinary Skill in the Art

11. I have been informed and understand that a patent is to be understood from the perspective of a hypothetical POSITA. Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to

being a genius). I understand that in considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

C. Obviousness

12. I have been informed and understand that a patent claim is obvious under 35 U.S.C. §103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a POSITA as of the priority date of the patent based on one or more prior art references and/or the knowledge of a POSITA.

13. I understand that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long-felt but unmet need, failure of others, copying by others, and skepticism of experts).

14. I understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. §103. I understand that a reference may also be combined with the knowledge of a POSITA, and that this knowledge may be used to combine multiple references. I further understand that a POSITA is presumed to know the relevant prior art. I understand that the obviousness analysis may take into account the inferences and creative steps that a POSITA would employ.

15. In determining whether a prior art reference would have been combined with other prior art or other information known to a POSITA, I understand that the following principles may be considered:

a. whether the references to be combined involve non-analogous art;

b. whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;

c. whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;

d. whether the combination is of familiar elements according to known methods that yields predictable results;

e. whether a combination involves the substitution of one known element for another that yields predictable results;

f. whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;

g. whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;

h. whether the combination is "obvious to try";

i. whether the combination involves the known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces, where the variations are predictable to a POSITA;

j. whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;

k. whether the combination requires modifications that render the prior art unsatisfactory for its intended use;

l. whether the combination requires modifications that change the principle of operation of the reference;

m. whether the combination is reasonably expected to be a success; and whether the combination possesses the requisite degree of predictability at the time the invention was made.

16. I understand that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that a teaching, suggestion, or motivation to combine is not required.

V. LEVEL OF ORDINARY SKILL IN THE ART

17. I am familiar with the level of ordinary skill in the art with respect to the ’864 Patent around its filing date. Based on my experience working, teaching, and conducting research in the relevant field, and based on my review of the ’864 Patent specification, claims, file history, and prior art, I believe one of ordinary skill in the art around the time of the alleged invention of the ’864 Patent 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, with additional education substituting for experience and vice versa.

18. In determining the level of ordinary skill in the art, I considered, for example, the type of problems encountered in the art, prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field.

19. I met or exceeded the knowledge and experience that a POSITA would have had in 2011. I have extensive experience in conducting research in wireless and cellular network (4G/5G) security, as well as in teaching related concepts in lectures and in advising student projects and PhD theses.

VI. SUMMARY OF MY OPINIONS

20. As I explain below in detail in my Declaration, it is my opinion that Claims 1-20 of the '864 Patent would have been obvious under 35 U.S.C. §103 on the following grounds.

- **Ground 1:** Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple (Ex-1005) in view of Wang (Ex-1006).
- **Ground 2:** Claims 5 and 8 are obvious over Semple in view of Wang and Bhuyan (Ex-1007).
- **Ground 3:** Claim 10 is obvious over Semple in view of Wang and Pierce (Ex-1010).
- **Ground 4:** Claims 13, 17, and 18 are obvious over Semple in view of Wang and Jorgensen (Ex-1008).
- **Ground 5:** Claims 1-7, 9, 11-12, 14-16, and 18-20 are obvious over Semple in view of Wang and SEC1 (Ex-1012).
- **Ground 6:** Claims 5 and 8 are obvious over Semple in view of Wang, SEC1, and Bhuyan.
- **Ground 7:** Claim 10 is obvious over Semple in view of Wang, SEC1, and Pierce.
- **Ground 8:** Claims 13, 17, and 18 are obvious over Semple in view of Wang, SEC1, and Jorgensen.

VII. TECHNOLOGICAL BACKGROUND

A. A method of authentication with a wireless network

21. Methods for using a mobile device to perform an authentication method with a wireless device were well known by 2013. For example, Farnham teaches "[a] method of establishing a secure communications link between a terminal and a server." Ex-1021 (Farnham), Abstract. Farnham further teaches that "[w]ithin the context of a mobile phone network a user or the network operator can authenticate their identity by signing a message with their private key; likewise a public key can be used to verify their identity." Ex-1021 (Farnham) ¶7; *see also* Ex-1029 (CSMG), 5 (a mobile device's "SIM identifies the subscriber to the network and enables this identity to be securely authenticated"); Ex-1026 (Nguyen) ¶1 ("method and apparatus for end-to-end mobile user security in a network"); Ex-1030 (Nakhjiri), Abstract (teaching a method for providing "end-to-end security for transport of a profile to a target device (e.g., mobile computing device) over at least one communications network"); Ex-1027 (Natarajan) ¶2 ("system and method for secure transaction of data between at least one wireless communication device and a server by using … ECC (Elliptic Curve Cryptography) and SKE (Symmetric Key Encryption) mechanisms.").

B. Storing a server public key, module identity,[1] cryptographic algorithms, and a pre-shared secret key

22. Authentication methods involving storing a module identity, cryptographic algorithms, and a pre-shared secret key were well known by 2013. For example, CSMG teaches that "[t]he International Mobile Subscriber Identity (IMSI) is a unique identifier associated with each GSM and UMTS subscription," which "is stored as a 64-bit field in the SIM and is sent by the phone to the network when the device is asked to identify by the network." Ex-1029 (CSMG), 16. Moreover, CSMG teaches that "[i]n order to prove the identity of the device, a secret key, 'Ki' is also used" and "may be stored in a proprietary file specific to each SIM card vendor." Ex-1029 (CSMG), 16. CSMG further teaches that "MNO-specific authentication algorithms are also stored on the SIM and used to generate unique responses to network authentication challenges" to "ensure that each MNO retains unique ownership over the SIM card and its authentication abilities." Ex-1029 (CSMG), 16, 21 ("The authentication process for GSM uses MNO-specific encryption algorithms (A3, A8) to identify and authenticate a subscriber."); *see also* Ex-1022 (Ala-Laurila)

[1] The '864 Patent uses the term "module" interchangeably with a "machine-to-machine" device and a "wireless module." Ex-1001, 1:41-46, 2:3-19. The patent further teaches that "the terms 'mobile node', 'mobile station', 'mobile device', 'M2M module', 'M2M device', 'networked sensor', or 'industrial controller' can be used to refer to module 101." Ex-1001, 18:30-33. Thus, for purposes of my Declaration, I have applied the term "module" as used in the claims to refer to the mobile device. For example, the term "module identity" refers to the identity of the mobile device.

¶¶18 ("The SIM comprises an International Mobile Subscriber Identity IMSI which represents the subscriber in the network, thus operating as an identifier of the terminal MT. … The SIM also comprises a secret key Ki, an algorithm A8 for forming a ciphering key Kc and an algorithm A3 for forming an authentication response SRES (Signed Response)."), 25 ("MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein"); Ex-1024 (Bradley) ¶31 ("The secure vault … securely packages, encrypts and signs the entire personalisation script for the related embedded UICC … as well as the relevant subscription information such as the IMSI, K, Opc, IMPU and algorithm constants."); Ex-1021 (Farnham) ¶38 (non-volatile programme memory stores "symmetric and asymmetric cryptography code").

23. It was also known by 2013 that the module identity comprises a permanent identifier for the mobile device. For example, CSMG teaches that the IMSI "is a unique identifier associated with each GSM and UMTS subscription." Ex-1029 (CSMG), 16; *see also* Ex-1022 (Ala-Laurila) ¶18 ("The SIM comprises an International Mobile Subscriber Identity IMSI which represents the subscriber in the network, thus operating as an identifier of the terminal MT.").

24. Additionally, authentication methods involving storing a server public key were known by 2013. For example, Farnham teaches that non-volatile programme memory in the mobile device stores "public keys for one or more server

operators." Ex-1021 (Farnham) ¶38. Moreover, Farnham teaches that "[t]he mobile terminal B or client can obtain the server's public value $Y_A=g^a$ mod p where [a] is the private key of the server, for example from a server key exchange" or "[p]referably … the server's public value is stored in the SIM." Ex-1021 (Farnham) ¶68; *see also* Ex-1030 (Nakhjiri), 5:64-6:2 (UICC "creates the PEK to perform decryption" on an encrypted profile received from the MNO by using the ECC private key (MNO_ECC_PVKDEV) and the ***MNO ECC public key (MNO_ECC_PLKOP)*** to perform a local ECDH key agreement process"); Ex-1027 (Natarajan) ¶¶30 ("the server 110 generates a random number 'r' upon receiving client hello message," "computes a resultant masking process of random number … using the generated random number 'r', Mask, a transaction ID by matching hash function, wherein the Mask=156-bits," "encrypts a message with the resultant masking process of random number 's' thereby matching hash function, adding a nonce value for security with help of a public key 'PUB' of the wireless communication device 120 using an ECE Encryption algorithm and then the server 212 sends the encrypted message … to the wireless communication device"), 31 ("the wireless communication device 120 retrieves the random number 'r' and the Mask … thereby matching hash function with help of a private key 'k' of the wireless communication device 120 upon receiving the encrypted message thereby using an ECE Decryption algorithm and subsequently the wireless communication device

120 splits the random number 'r' and the Mask and then subsequently verifies the values of the random number with the Nonce value for security and the resultant masking process of random number 's' with hash function").

25. It was also known by 2013 that the cryptographic algorithms include a symmetric ciphering algorithm. For example, Farnham teaches employing "an anonymous Diffie-Hellman cryptographic technique." Ex-1021 (Farnham) ¶66. Specifically, Farnham teaches that "an appropriate prime p and generator g of Z_p * are selected and published, and, for example, stored on the terminal SIM," where "Z_p * is the multiplicative group 1, 2, 3 . . . p−1 and (2≦g≦p−2)." Ex-1021 (Farnham) ¶67; *see also* Ex-1026 (Nguyen) ¶19 ("The key exchange algorithm can be based on the Elliptic Curve Diffie-Hellman (ECDH) cryptosystem, which itself is a key exchange algorithm that is based on Elliptic Curve Cryptography (ECC) for public/private key generation."); Ex-1028 (Cuppett), 5:50-56 ("Examples of known asymmetric encryption systems that can be used include … Diffie-Hellman."); Ex-1030 (Nakhjiri), 5:27-32 ("One example of a key exchange algorithm that may be employed is an Elliptic Curve Diffie-Hellman exchange (ECDH) algorithm where both the UICC and the MNO end up with exactly the same Shared ECDH secret (using Elliptic Curve multiplication operation).").

C. Deriving a module private key and corresponding module public key associated with the mobile device using the cryptographic algorithms

26. Authentication methods involving deriving a module private key and a corresponding module public key using the cryptographic algorithms were well known by 2013. For example, Farnham teaches employing "an anonymous Diffie-Hellman cryptographic technique." Ex-1021 (Farnham) ¶66. Specifically, Farnham teaches that "[t]he terminal chooses a random value b, computes g^b mod p and sends M1 g^b mod p (encrypted) to the server." Ex-1021 (Farnham) ¶68; *see also* Ex-1026 (Nguyen) ¶36 ("MS_1 can use its own private key P_1 to compute its own public key Q_1 using a chosen base point B on a specific Elliptic Curve algorithm. The base point 'B' can be a random value selected from an elliptic curve algorithm."); Ex-1027 (Natarajan) ¶¶32 ("the wireless communication device 120 generates and adds the signature {signs} with message having a resultant value 'm', wherein the resultant value 'm' {m=r3 mod p=a 137-bit number} is obtained using permutation technique of the random number 'r', with respect to its private key 'k' thereby using an ECDSA-163 algorithm and subsequently the wireless communication device 120 sends the resultant message {sig_value} to the server"), 33 ("the server 110 verifies the signature {sig_value} of the received resultant message with help of the public key 'PUB' of the wireless communication device 120 using ECDSA-163 algorithm and subsequently the server 110 retrieves the resultant value 'm' {r3 mod p} by

using permutation technique of the random number 'r'"), 36 ("The wireless communication device 120 uses its private key 'k' of 163-bits for Elliptic Cryptography (EC) decryption and EC signature generation and uses its public key 'PUB' for Elliptic Cryptography (EC) decryption and EC signature verification and a known Pseudo Random Number Generator (PRNG) which accepts a seed for generating the random numbers.").

27. Moreover, Nakhjiri teaches that one "approach is to use public key algorithms that allow a private key to be generated as a random value" such as "Elliptic Curve Cryptography (ECC)." Ex-1030 (Nakhjiri), 4:28-31. "[O]nce the ECC_PVK and the ECC curve are known, the ECC public key (PLK) can be generated simply by having knowledge of the PVK and the ECC curve." Ex-1030 (Nakhjiri), 4:34-37. Specifically, "the UICC uses its private seed and the MNO identifier (MN_ID) to generate its own ECC private key (MNO_ECC_PVKDEV) using the pre-configured key generator function (KGF)" and "then creates the PEK to perform decryption … us[ing] the device ECC private key for this particular MNO (MNO_ECC_PVKDEV) and the MNO ECC public key (MNO_ECC_PLKOP) to perform a local ECDH key agreement process." Ex-1030 (Nakhjiri), 5:25-37; *see also id.*, 5:61-64 ("the UICC uses its private seed and the MNO identifier (MN_ID) to generate its own ECC private key (MNO_ECC_PVKDEV) using the pre-configured key generator function (KGF)"), 6:61-7:20 ("in one implementation an

alternative key agreement algorithm that may be employed is the Diffie-Hellman algorithm where the private key MNO_DH_PVKDEV may be derived from a random seed and the public key is generated … where g is called a generator and p is a large prime number … and where MNO_DH_PLKDEV is UICC's Diffie-Hellman public key, MNO_DH_PVK is the DH private key which belongs to the MNO and MNO_DH_PLK is the corresponding MNO public key").

D. Deriving a symmetric ciphering key with the server public key and module private key

28. Authentication methods involving deriving a symmetric ciphering key using an elliptic curve integrated encryption scheme with the server public and the module private key were well known by 2013. For example, Farnham teaches employing a Diffie-Hellman cryptographic technique, wherein "[t]he mobile terminal B can compute a key for a symmetric session $k=Y_A{}^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p$ and the server A can compute the same session key $k=(g^b \bmod p)^a \bmod p=g^{ba} \bmod p$" so that "[e]ncrypted data or software may then be sent to the terminal B by encrypting it with a session key or the session key may be used by both the terminal and server to generate another common key, for example by operating on data known to both with K." Ex-1021 (Farnham) ¶¶66, 68; <u>*see also id.* ¶¶12, 14, 57;</u> *see also, e.g.*, Ex-1027 (Natarajan) ¶¶14 ("In the ECC … [d]uring the communication, a permutation technique (cubing a random number w.r.to a prime p=2 mod 3)) is used between the wireless communication device and the server ends

in order to avoid reply attack."), 27-49 (examplary authentication process using ECC); Ex-1030 (Nakhjiri), 4:28-31 ("Another alternative approach is to use public key algorithms that allow a private key to be generated as a random value. An example of such a public key algorithm is Elliptic Curve Cryptography (ECC)."); Ex-1027 (Natarajan) ¶¶38-49 (describing an example "of the Secure Transaction of Data Using EAP Protocol Based on ECC").

29. Additionally, Gouget teaches generating "the common secret by the client (C) and by the server (S) … based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) of the client (C) … according to the Diffie-Hellman protocol." Ex-1032 (Gouget) ¶12. For example, Gouget teaches that "[i]n the Chip Authentication CA step: the client C is authenticated by the server S by verifying an authentication token computed from an exchanged Diffie-Hellman key" based on the client-side public key, which "is the long-term key pk_c certified during the passive authentication step PA" and the server-side public key, which "is the ephemeral key pk_s chosen by the server S during the terminal authentication step TA." Ex-1032 (Gouget) ¶39. Gouget further teaches that "[t]he Diffie-Hellman key shared between the client C and the server S is used to compute or verify the authentication token and also to establish the secure channel." Ex-1032 (Gouget) ¶39. "This Diffie-Hellman key is computed from pk_c and sk_s at the server side and from sk_c and pk_s at the client side." Ex-1032 (Gouget) ¶39; *see also id.*, ¶¶40-41.

Specifically, "[t]he client C calculates the common secret key as following: $K=KDF(sk_c,pk_s,sk_{cc},pk_s)$," the server "also calculates the common secret key as following: $K=KDF(sk_s,pk_c,sk_s,pk_{cc})$," "where KDF is a Key Derivation Function" and the protocol used "is the Diffie-Hellman protocol (DH or ECDH)." Ex-1032 (Gouget) ¶¶42-45.

30. It was also known by 2013 that the symmetric ciphering key could be derived using an American National Standards Institute standard X-9.63 key derivation function in addition to the elliptic curve integrated encryption scheme. For example, Farnham teaches that "[a]symmetric cryptography was first publicly disclosed by Diffie and Hellman in 1976" and "[o]ther more recent algorithms including elliptic curve crypto systems (*see, for example*, X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999))." Ex-1021 (Farnham) ¶9; *see also id.* ¶71 ("Under certain circumstances, the Diffie-Hellman and (DH) the related Elliptic Curve Diffie-Hellman (ECDH) key agreement schemes (X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)) are susceptible to a class of attacks known as 'small-subgroup' attacks. … This threat can be alleviated by using a predetermined group determined 'good' or 'strong' values of g and p and checking that received public keys do not lie in a small

subgroup of the group, or by not re-using ordinary DH key pairs. Background information on protection against these attack, can be found in the draft ANSI standards … X.9.63 (X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)).").

31. Moreover, Nakhjiri teaches that an "ECC private key (MNO_ECC_PVKDEV) can be calculated … using as input a key generation function (KGF) and an MNO identifier (MNO_ID)." Ex-1030 (Nakhjiri), 4:45-48. Specifically, "the UICC uses its private seed and the MNO identifier (MN_ID) to generate ***its own ECC private key*** (MNO_ECC_PVKDEV) ***using the pre-configured key generator function (KGF)***" and "then creates the PEK to perform decryption … us[ing] the device ECC private key for this particular MNO (MNO_ECC_PVKDEV) and the MNO ECC public key (MNO_ECC_PLKOP) ***to perform a local ECDH key agreement process***." Ex-1030 (Nakhjiri), 5:25-37. Nakhjiri further teaches that "[t]he KGF may be proprietary or a well-established function." Ex-1030 (Nakhjiri), 5:60. For instance "the KGF can be a standard MAC (Message Authentication Code) function such as HMAC-SHA1, HMAC-SHA256, AES-CMAC, and so on" and "should be chosen such that it generates a key of sufficient size which matches the Elliptic Curve parameters." Ex-1005 (Nakhjiri), 5:61-65.

E. Generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm

32. Authentication methods involving generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm were well known by 2013. For example, Farnham teaches that "the Diffie-Hellman value g^b mod p may be encrypted using the originator's (that is, in this example, B's) private key. More specifically it may be protected by sending the Diffie-Hellman value as a digital signature from which the signed message is recoverable. The recipient may then recover g^b mod p using the originator's public key, more specifically by extracting the message from the signature." Ex-1021 (Farnham) ¶70; *see also id.* ¶13 ("The identity of the sender or recipient may be included within the message with, optionally, a time stamp or random number or nonce (as described above with reference to other aspects of the invention)."). Moreover, Rajadurai teaches a method for "establishing a communication session with the operator network using the IMSI assigned to the user equipment." Ex-1031 (Rajadurai) ¶33, Fig. 4. Specifically, Rajadurai teaches that "the user equipment 102A sends a non-access stratum message including the assigned IMSI to the operator network 104." Ex-1031 (Rajadurai) ¶33.

33. Additionally, Gouget teaches that "a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key

sk_c has been revealed." Ex-1032 (Gouget) ¶22. Gouget further teaches that the client C "generates an ephemeral key pair (sk_{cc},pk_{cc}) during the chip Authentication step CA and sends the public key pk_{cc} of said ephemeral key pair (sk_{cc},pk_{cc}) to the server S." Ex-1032 (Gouget) ¶41. Specifically, "[t]he client C calculates the common secret key as following: K=KDF(sk_c,pk_s,sk_{cc},pk_s)," the server "also calculates the common secret key as following: K=KDF(sk_s,pk_c,sk_s,pk_{cc})," "where KDF is a Key Derivation Function" and the protocol used "is the Diffie-Hellman protocol (DH or ECDH)." Ex-1032 (Gouget) ¶¶42-45. Additionally, Gouget teaches that "[t]he secure channel can then be established with the common secret" and "[b]y doing so, the security impact is reduced significantly when the long-term secret of the client is compromised." Ex-1032 (Gouget) ¶¶47-48.

34. It was also known by 2013 that the module encrypted data includes the module identity. For example, Ala-Laurila teaches that the MT first "requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier." Ex-1022 (Ala-Laurila) ¶26. The MT then sends "the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI." Ex-1022 (Ala-Laurila) ¶26. Ala-Laurila teaches that "[t]he NAI ***comprises the IMSI*** identifier obtained from the identity module SIM." Ex-1022 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request "is ***preferably sent in ciphered form*** to the [Public Access Controller] PAC

using the Diffie-Hellman algorithm." Ex-1022 (Ala-Laurila) ¶26; *see also* Ex-1031 (Rajadurai) ¶33, Fig. 4.

35. As another example, Bradley teaches "a method for downloading a subscription in an UICC embedded in a" mobile terminal, which includes transferring an integrated circuit card identification number (ICCID) "to the terminal; sending the ICCID over an IP link to a secure vault; selecting in the secure vault a subscription corresponding to the ICCID; transmitting the subscription to the terminal over the IP link;" and "storing the subscription in the terminal." Ex-1024 (Bradley) ¶¶2, 17. Bradley further teaches that "[t]he secure vault verifies the ICCID/secret activation code pairing and if valid it securely packages, ***encrypts and signs the entire personalisation script for the related embedded UICC*** … as well as the relevant subscription information such as the ***IMSI***, K, Opc, IMPU and algorithm constants." Ex-1024 (Bradley) ¶31. The secure vault then transmits the "personalisation script to device X encrypted for Device X's embedded secure element … over the IP link" and "Device X (including its embedded secure element) decrypts and runs the personalisation script thus provisioning the subscription onto the embedded secure element." Ex-1024 (Bradley) ¶¶32-33.

F. Sending a message to a wireless network server comprising the module encrypted data and the corresponding module public key

36. Authentication methods involving sending a message to a server for the wireless network comprising the module encrypted data and the module public key

were well known by 2013. For example, Farnham teaches that "the Diffie-Hellman value g^b mod p may be encrypted using the originator's (that is, in this example, B's) private key. More specifically it may be protected by sending the Diffie-Hellman value as a digital signature from which the signed message is recoverable. The recipient may then recover g^b mod p using the originator's public key, more specifically by extracting the message from the signature." Ex-1021 (Farnham) ¶¶70, 79 ("The session key may be computed … using an appropriate publicly known non-reversible function *f* such as MD5 (Message Digest 5, as defined in RFC 1321) and SHA-1 (secure Hash Algorithm-1, see, for example, US National Bureau of Standards Federal Information Processing Standards (FIPS) Publication 180-1.")). Moreover, Ala-Laurila teaches that the MT sends "the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a" NAI. Ex-1022 (Ala-Laurila) ¶26. Ala-Laurila teaches that "[t]he NAI comprises the IMSI identifier obtained from the identity module SIM." Ex-1022 (Ala-Laurila) ¶26. Ala-Laurila also teaches that the request "is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm." Ex-1022 (Ala-Laurila) ¶26. Additionally, Rajadurai teaches that "the user equipment 102A sends a non-access stratum message including the assigned IMSI to the operator network 104" (Ex-1031 (Rajadurai) ¶33), which "includes an authentication and authorization server 108, and a home subscriber server 110." Ex-1031 (Rajadurai) ¶16.

37. Farnham also teaches that asymmetric cryptography can "be used to digitally sign messages by encrypting either the message or a message digest, using the private key." Ex-1021 (Farnham) ¶6 ("A message digest is derived from the original message and is generally shorter than the original message making it difficult to compute the original message from the digest; a so-called hash function may be used to generate a message digest."). Moreover, Gouget teaches that "a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key sk_c has been revealed." Ex-1032 (Gouget) ¶22. Gouget further teaches that the secure channel is "established with the common secret." Ex-1032 (Gouget) ¶47.

38. It was additionally known by 2013 that the server mutually derives the symmetric ciphering key using at least the module public key. For example, Farnham teaches that "[t]he mobile terminal B can compute a key for a symmetric session $k=Y_A{}^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p$ and the ***server A can compute the same session key*** $k=(g^b \bmod p)^a \bmod p=g^{ba} \bmod p$" so that "[e]ncrypted data or software may then be sent to the terminal B by encrypting it with a session key or the session key may be used by both the terminal and server to generate another common key, for example by operating on data known to both with K." Ex-1021 (Farnham) ¶68. Farnham also teaches that "[p]roviding the recipient has the original message they

can ***compute the same digest*** and thus authenticate the signature by decrypting the message digest." Ex-1021 (Farnham) ¶6; *see also* Ex-1026 (Nguyen) ¶38 ("Each MS can use the public key received from the other MS along with its own private key to generate a shared Diffie-Hellman authentication key.").

39. Moreover, it was known by 2013 that the wireless network selects the pre-shared secret key for the mobile device using the module identity. For example, CSMG teaches that "SM-DPs package the MNO SIM credentials (including the IMSI and Ki) for secure download." Ex-1029 (CSMG), 7, 16 (IMSI is stored "in the SIM and sent by the phone to the network when the device is asked to identify by the network" and "[i]n order to prove the identity of the device, a secret key, 'Ki' is also used," which "may be stored in a proprietary file specific to each SIM card vendor"), 21 ("SIM then attaches itself to the network by authenticating with the AuC … using the IMSI and Ki").

G. Authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key

40. Authentication methods involving authenticating with the wireless network using a message digest with the pre-shared secret key were well known by 2013. For example, Farnham teaches that "[a] Message Authentication Code (MAC) (for example a keyed hash function see, for example, Computer data authentication. National Bureau of Standards FIPS Publication 113, 1985) is used to protect the installation ticket. This MAC is computed using a secret key shared by the terminal

and the ticket server." Ex-1021 (Farnham) ¶¶40, 79 ("using an appropriate publicly known non-reversible function f such as MD5 (Message Digest 5, as defined in RFC 1321) and SHA-1 (secure Hash Algorithm-1"); *see also* Ex-1023 (Brainis) ¶37 ("both the authenticity and the data integrity" can be verified "with e.g. Message Authentication Code (MAC) or Hash-based Message Authentication Code (HMAC)").

VIII. THE '864 PATENT AND ITS FILE HISTORY

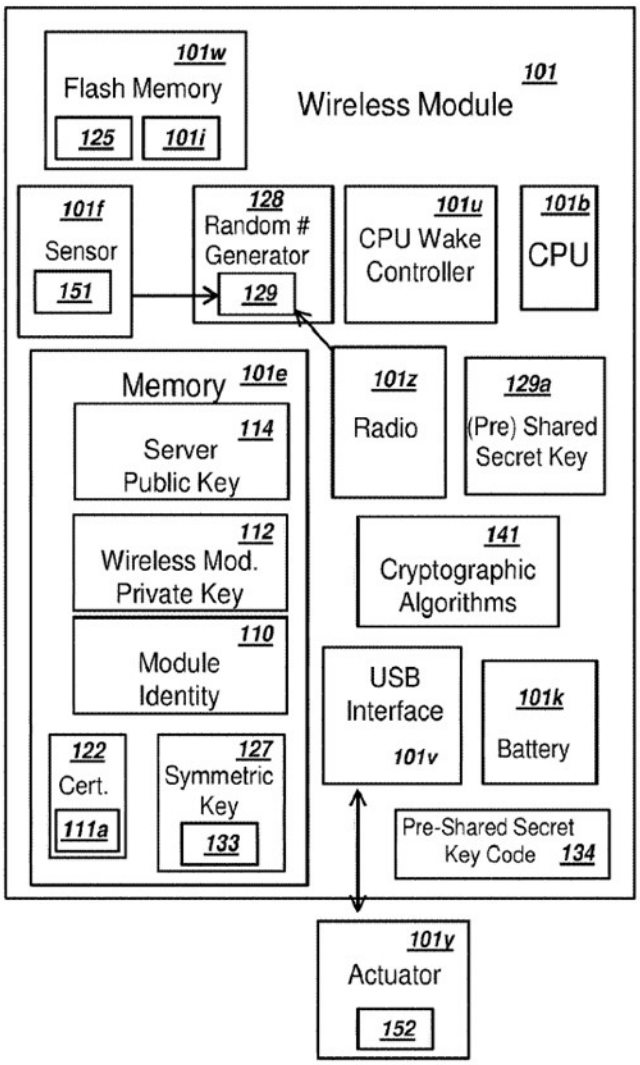
41. The '864 Patent teaches "efficient methods and systems for supporting secure, efficient, and flexible communications using Internet Protocol networks, where a server can communicate with both a 'machine-to-machine' modules and an application." Ex-1001, 1:44-48.

42. As shown in Figure 1e below,[2] the '864 Patent teaches a wireless module 101, which may operate "as a smartphone or mobile phone." Ex-1001, 15:67, 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, 27:27-30. Module identity 110 is "a unique identifier of module 101" such as "an international mobile subscriber identity number (IMSI)." Ex-1001, 28:48-51. Module 101 also stores cryptographic algorithms 141, which include a suite of algorithms that are used for "(i) deriving a pair of keys comprising

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

a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys." Ex-1001, 30:5-12. Moreover, module 101 stores "a pre-shared secret key 129a," which is "shared between module 101 and server 105." Ex-1001, 32:29-32.

Figure 1e



43. The ’864 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, 64:25-29. 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, 64:47-53. The ’864 Patent further teaches generating “module encrypted data … ciphered with a symmetric key.” Ex-1001, 7:23-24. Symmetric key 127 is “a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms” 141 (Ex-1001, 27:57-59), 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, 28:5-10. Module 101 then sends the module encrypted data in a message to the server “using the derived keys” Ex-1001, 60:46-51. 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, 66:44-52.

44. The '864 Patent was filed February 20, 2023, and claims priority through a chain of 6 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.

IX. CLAIM CONSTRUCTION

45. For the purposes of my Declaration, I do not believe that any term requires explicit construction to resolve the issues I present in my Declaration because the prior art discloses or renders obvious the claim limitations under any potential construction of the claims.

X. OVERVIEW OF THE APPLIED PRIOR ART REFERENCES

A. Semple (Ex-1005)

46. Semple (U.S. Patent Publication No. 2006/0205388) published on September 14, 2006, and I understand it qualifies as prior art to the '864 Patent.

47. 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

Location Register (HLR) 602), and cryptographic algorithms including A3 and A8. Ex-1005 ¶¶33, 47, Fig. 6.

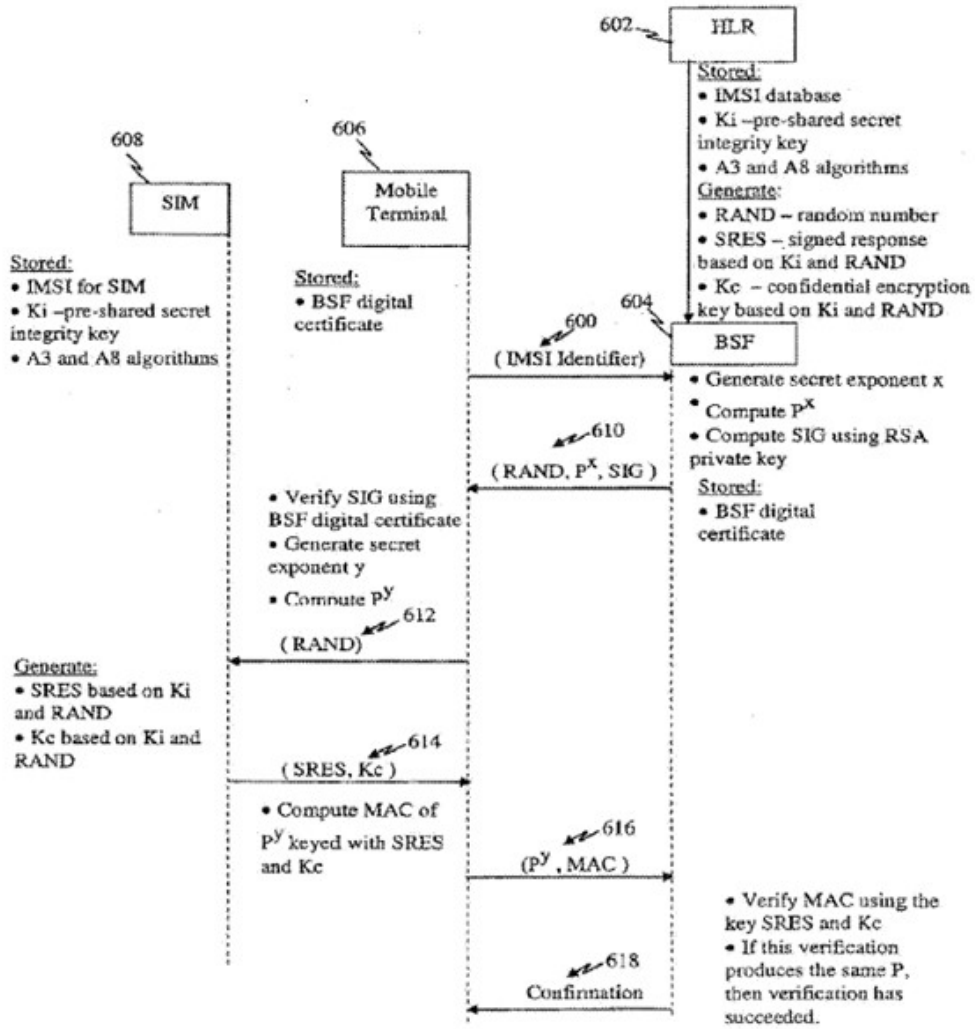


Figure 6

48. 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 Kc." *Id.*

49. 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 Kc", which are, in turn, derived from the shared secret key Ki. *Id.*, Fig. 6 at 614, 616 ("Generate SRES based in Ki and RAND, Kc based on Ki and RAND," "Compute MAC of P^y keyed with SRES and Kc").

B. Wang (Ex-1006)

50. Wang (PCT Patent Publication No. WO2008/005162) published on January 10, 2008, and I understand it qualifies as prior art to the '864 Patent.

51. 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.

52. 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)

53. Bhuyan (U.S. Patent Publication No. 2010/0135491) published on June 3, 2010, and I understand it qualifies as prior art to the '864 Patent.

54. Bhuyan teaches "a method of authenticating a mobile device" in a telecommunications network "using a network provisioned security module[3] 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

[3] SIM card "provisioning" refers to the process of preparing a SIM card to function properly within a mobile device, which involves a series of steps to ensure that the SIM is able to connect to the appropriate mobile network and access the necessary services. It includes loading the IMSI and MSISDN (mobile phone number), authentication keys, network settings, etc. on the SIM card.

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.

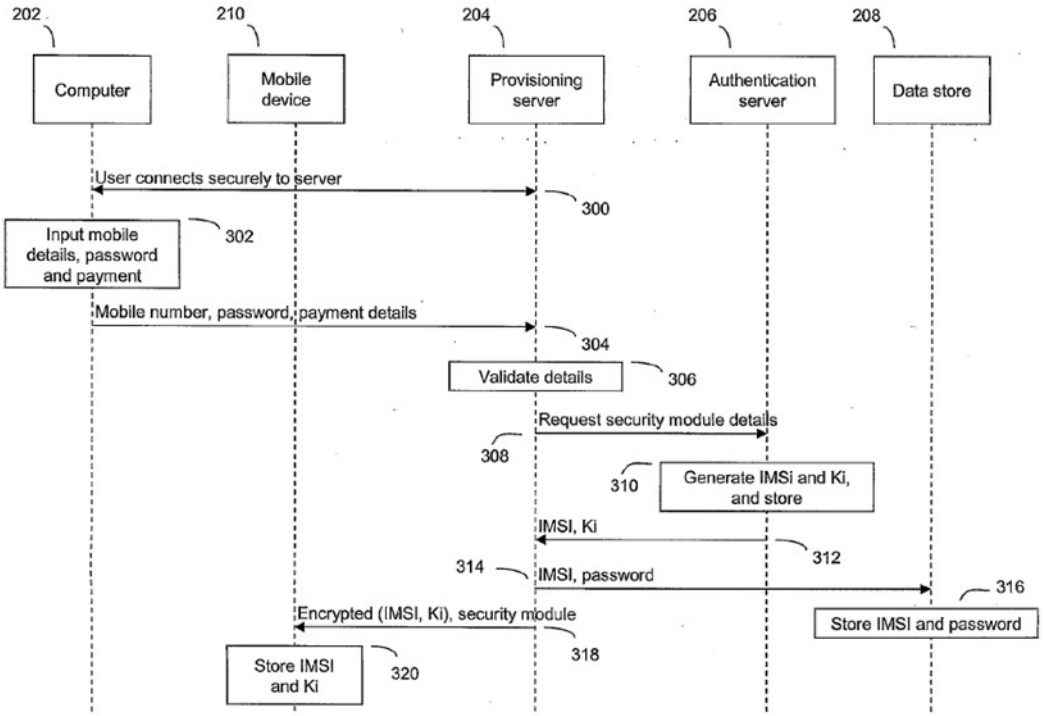


Figure 3

D. Pierce (Ex-1010)

55. Pierce (U.S. Patent Publication No. 2009/0323967) published on December 31, 2009, and I understand it qualifies as prior art to the '864 Patent.

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)

57. Jorgensen (U.S. Patent Publication No. 2004/0221163) published on November 4, 2004, and I understand it qualifies as prior art to the '864 Patent.

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)

59. SEC1 (Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography) published on May 21, 2009, and I understand it qualifies as prior art to the '864 Patent. SEC1 describes the well-known X9.63 key derivation function (KDF) standard using Elliptic Curve Cryptography, which is acknowledged by the '864 Patent at Ex-1001, 39:64-67 and by many prior art references. *See, e.g.,* Ex-1021 (Farnham), ¶71; Ex-1033 (Boyd), 292.

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.

XI. 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.

61. In addition to the reasons set forth below, 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. 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. This is known as perfect forward secrecy; because keys are created dynamically, they are valid for only a particular communication session. Thus, the compromise of those keys would reveal only the current communications and would not allow a malicious user to decrypt earlier messages that may have been intercepted. 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.

62. A POSITA would have had a reasonable expectation of success in combining the teachings of Semple and Wang. 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 method 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.

2. Independent Claim 1

a. Element 1[pre]: A method comprising:

63. In my opinion, Semple in view of Wang ("Semple-Wang") teaches the preamble, to the extent it is limiting.

64. 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.

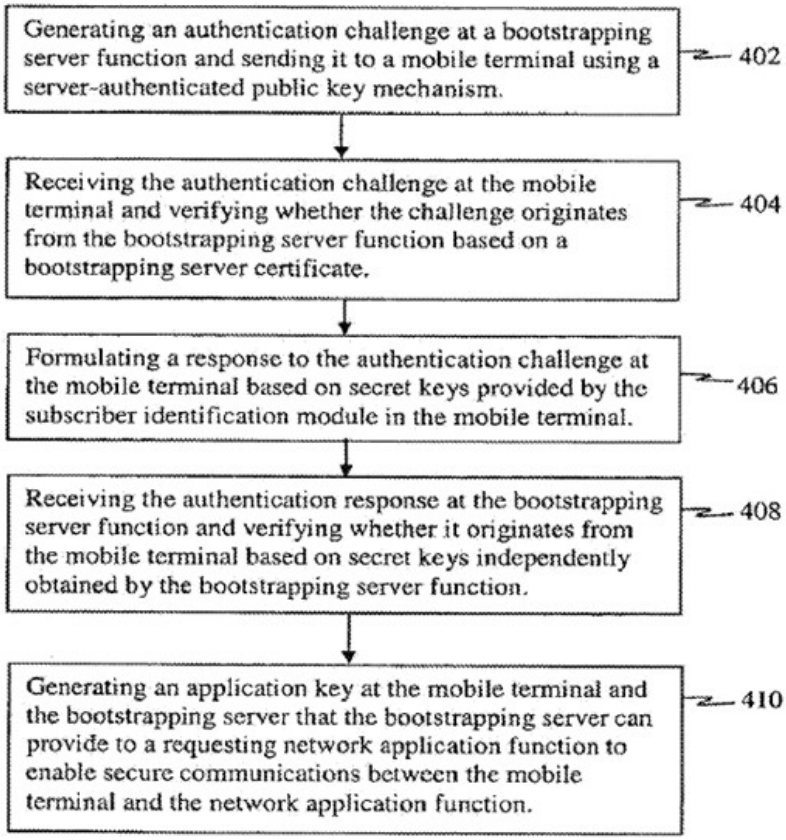


Figure 4

65. Semple teaches that mobile terminal "***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. 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)(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 a mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;

66. In my opinion, Semple-Wang teaches Element 1(a)(1).

(1) Storing a server public key

67. 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 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.").

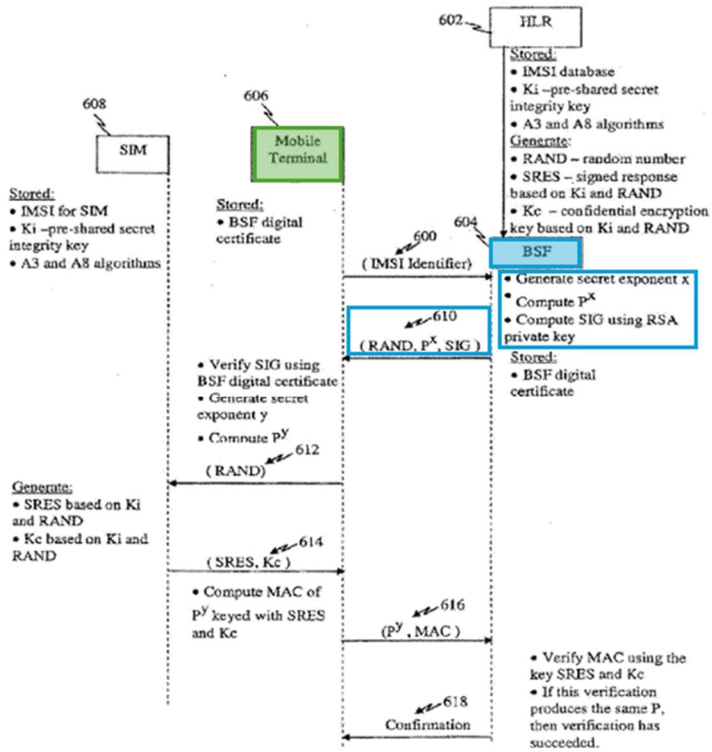


Figure 6

68. 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).

69. In the table below, I summarize how the prior art maps to key elements of the asserted patent claim. Here, I illustrate that the claimed "server public key" is met by Semple's disclosure of public key P^x. It is also met by Wang's disclosure of public key k_a.

Claim element	**Semple**	**Wang**
Server public key	**P^x**	**k_a**

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

70. 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." An IMSI is well known to be a permanent identifier for the mobile device.

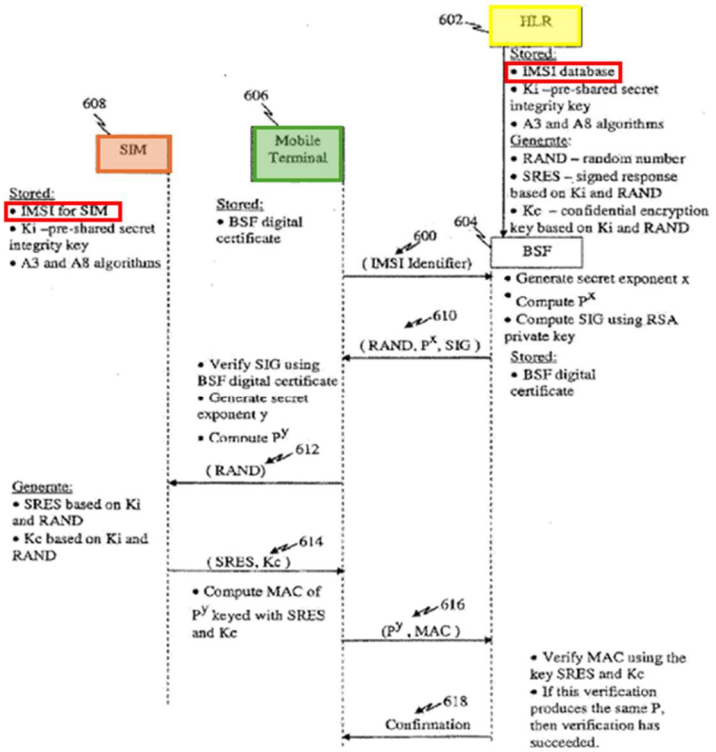


Figure 6

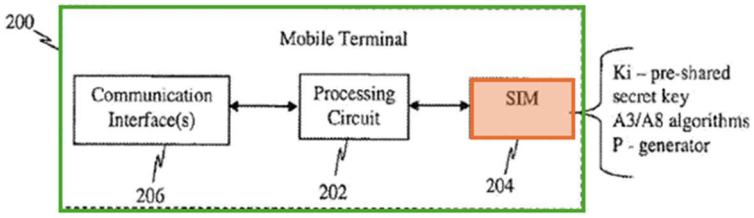


Figure 2

71. 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

72. 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").

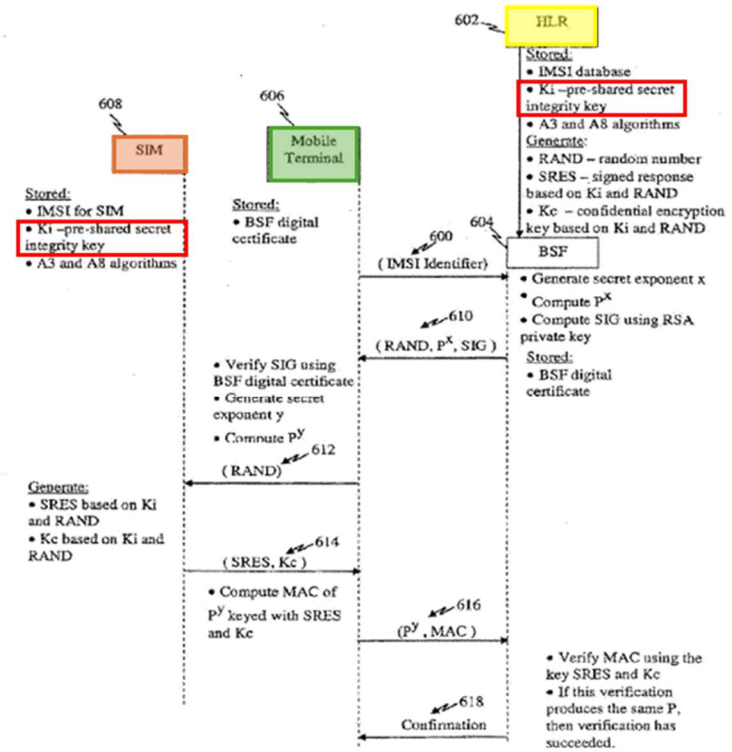


Figure 6

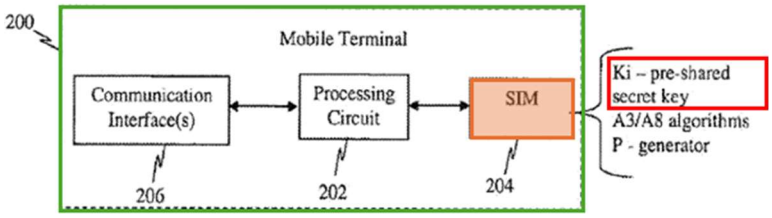


Figure 2

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

Petitioner Samsung Ex-1002, 0056

(4) Storing cryptographic algorithms including a symmetric ciphering algorithm

73. As shown in Figure 6 below, Semple teaches that "SIM 204 may contain a secret key Ki, 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 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. Semple notes that P is "previously provisioned to both the BSF 604 and MT 606." Ex-1005 ¶48. It is clear that Semple stores the symmetric Elliptic Curve Diffie-Hellman algorithms that allow it to use the derived symmetric key because Semple later uses the symmetric algorithms in claim step 1(a)(4) to encrypt module data using the symmetric ciphering key generated in the ECDH exchange, which I describe more fully with respect to that claim element. Thus, Semple's stored cryptographic algorithms include a symmetric ciphering algorithm, which is later used to apply the symmetric ECDH key.

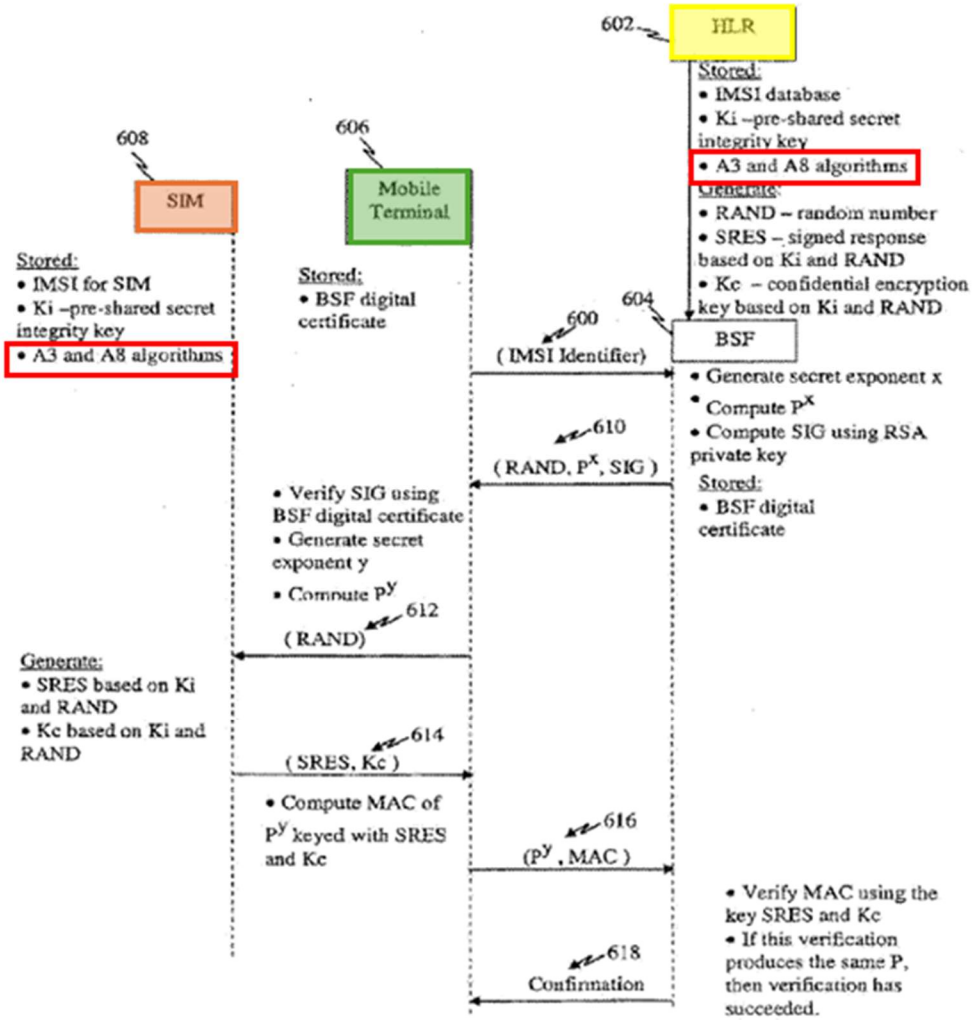


Figure 6

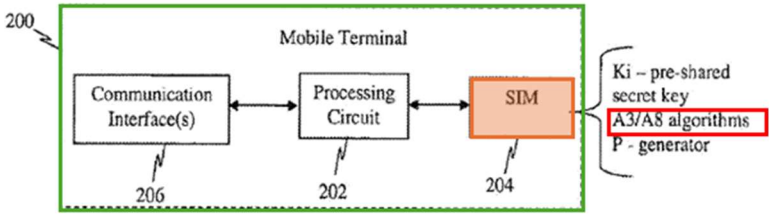


Figure 2

Claim element	Semple	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**	

c. Element 1(a)(2) deriving a module private key and a corresponding module public key associated with the mobile device using the cryptographic algorithms;

74. In my opinion, Semple-Wang teaches Element 1(a)(2).

75. Semple teaches deriving a module private key and a corresponding module public key associated with the mobile device using the cryptographic algorithms. Semple 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(a)(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. 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).

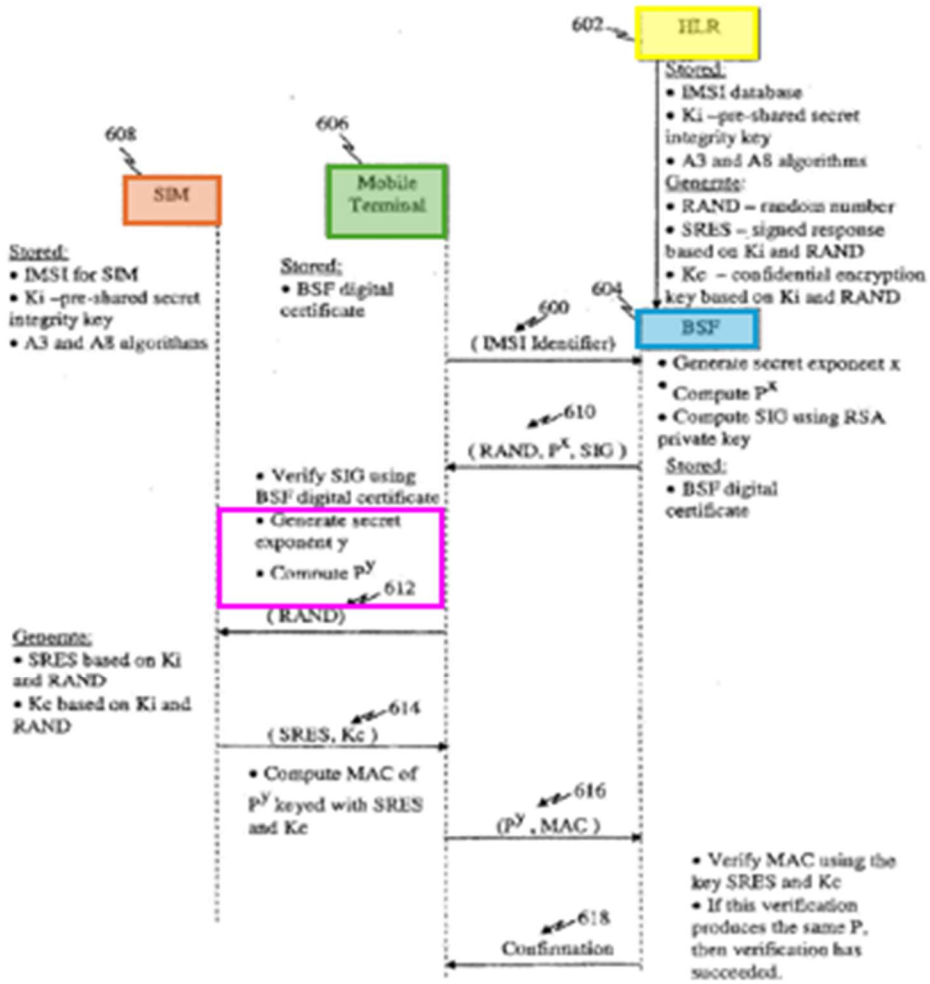


Figure 6

Claim element	Semple	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**	

Petitioner Samsung Ex-1002, 0060

d. Element 1(a)(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;

76. In my opinion, Semple-Wang teaches Element 1(a)(3).

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

77. 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. 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

78. 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. 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. For example, a version of SEC1's X-9.63 specification was published in 2011 and was widely known in the cryptographic community. Ex-1012. Indeed, the challenged patent identifies X-9.63 as an exemplary and well-known key derivation function. Ex-1001, 39:671-65. Thus, 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. Ex-1012, 31-33 ("The list of supported key 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 ANS 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.

Claim element	Semple	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}**	

e. Element 1(a)(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;

79. In my opinion, Semple-Wang teaches Element 1(a)(4). 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.*

80. A POSITA would have been motivated to further improve this process by replacing the initial ciphering CK from the USIM with the "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. It is well known that using freshly generated session keys can improve both forward security (i.e., protecting material that was not compromised before the long-term key was lost) and also can prevent key compromise impersonation, in which attacks are mounted before "compromise of the long-term key becomes known." E.g., Ex-1033 (Boyd-Mathuria) at 50-52 (discussing forward security and key compromise impersonation).

81. 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. The cryptographic algorithms governing how to create the key would also be used to govern how it is applied to the message. 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 XI.A.1.

f. Element 1(a)(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the corresponding 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

82. In my opinion, Semple-Wang teaches Element 1(a)(5).

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

83. 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 method instead encrypts the message with the symmetric key derived through

Semple's Diffie-Hellman key exchange, 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.

84. To start the ECDH process, Semple teaches that 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 it not necessary since computing x and Px does not depend on IMSI or the pre-shared key associated with it. Once the BSF receives P^y from the MT (along with the encrypted IMSI) and is able to decode the encrypted IMSI, it can then continue with the handshaking process of Figure 6.

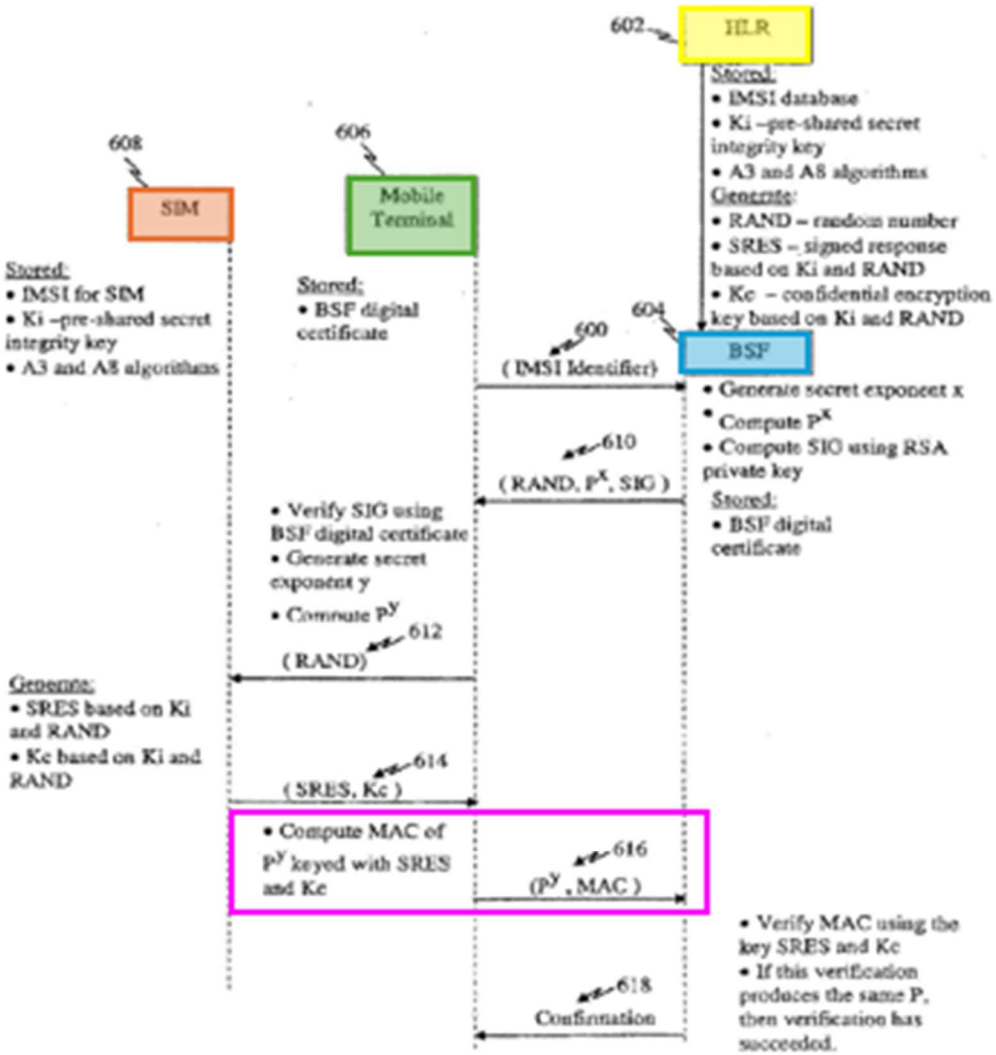


Figure 6

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 Semple-Wang method. 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.

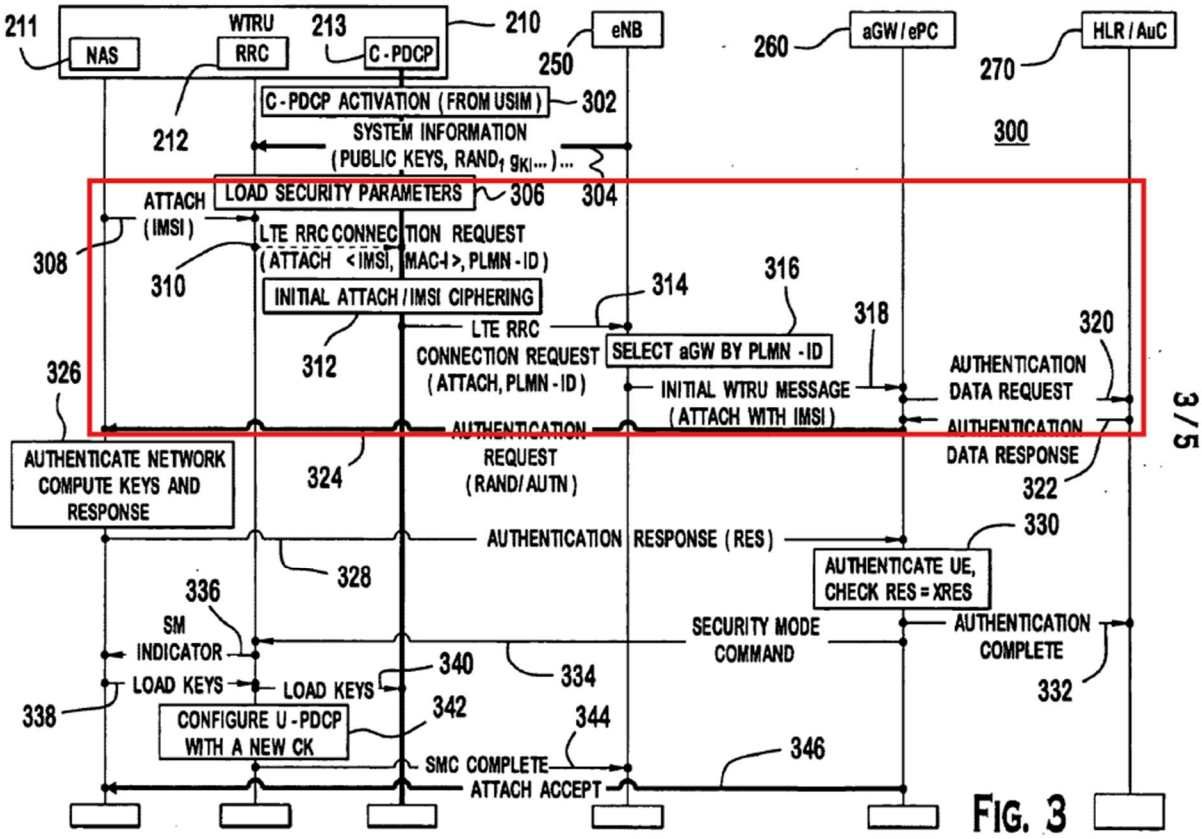


FIG. 3

85. 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). 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 method and then could have included the encrypted IMSI in message 616 to the BSF. Furthermore, because the MT already has the pre-shared key, it can use it to prepare the MAC-I (to the extent necessary) before the authentication server and HLR have looked up the shared key using the decrypted IMSI value.

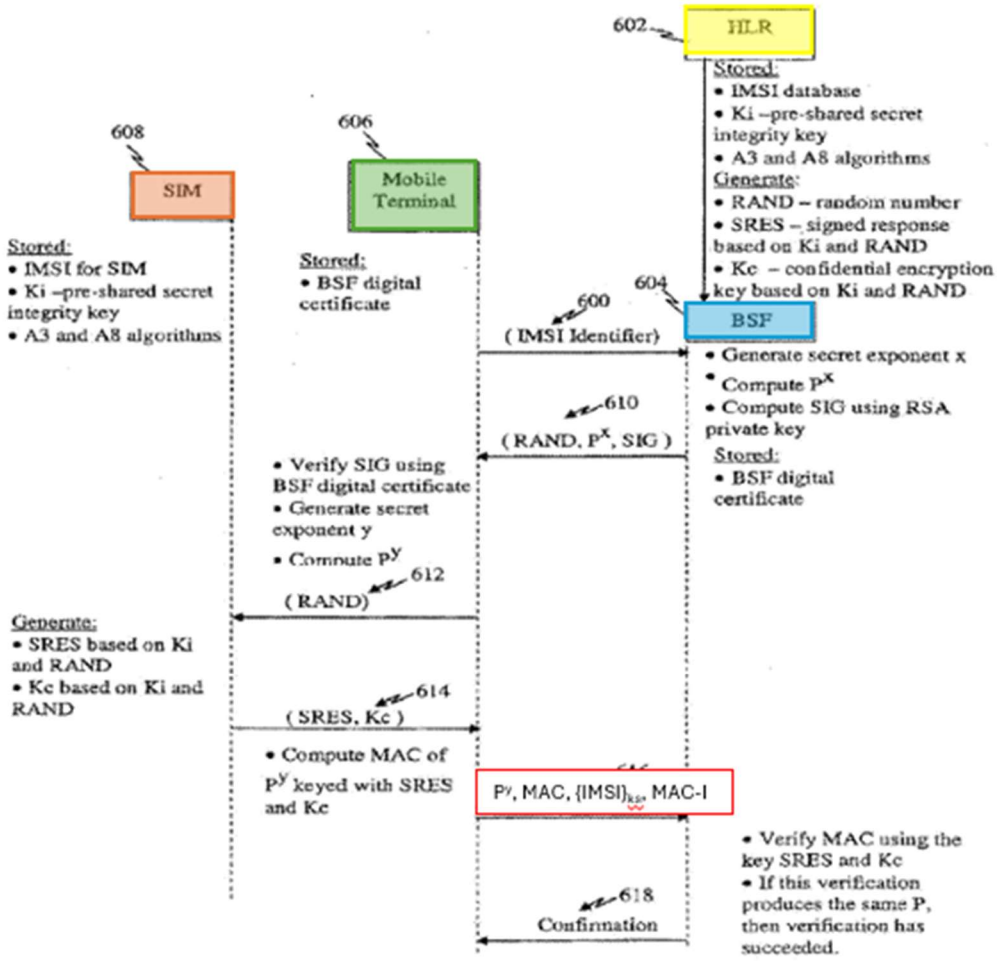


Figure 6

Petitioner Samsung Ex-1002, 0069

(2) Server mutually derives the symmetric ciphering key using at least the module public key

86. 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*.

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

87. Semple 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. Figure 6 also shows that the HLR includes an "IMSI database" and the "Ki=pre-shared secret integrity key." *Id.*, Fig. 6. Moreover, Semple 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-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	**Semple**	**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**

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

88. In my opinion, Semple-Wang teaches Element 1(a)(6).

89. As shown in Figure 6 below, Semple teaches that the BSF "verifies the MAC using the SRES and Kc 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 and Kc are calculated from the pre-shared secret key Ki. *Id.* ¶36 ("[T]he pre-shared secret key Ki and random number (e.g., RAND) may be used to generate secret keys (e.g., SRES and Kc) that are used to generate the authentication challenge parameters."). A MAC is a message digest created using a secret symmetric key. For example, Boyd-Mathuria defines a MAC as "a family of functions parametrised by a key K such that $MAC_K(m)$ takes a message m of arbitrary length and outputs a fixed length value," and further where it is computationally easy to calculate $MAC_K(m)$ but computationally difficult to find another message m that would give the same MAC. Ex-1033, 18.Moreover, a POSITA would have understood that the MAC is verified using the pre-shared secret key because "the SRES and Kc obtained from the HLR" in the triplet correspond "to random number RAND and pre-shared secret key Ki." Ex-1005 ¶53.

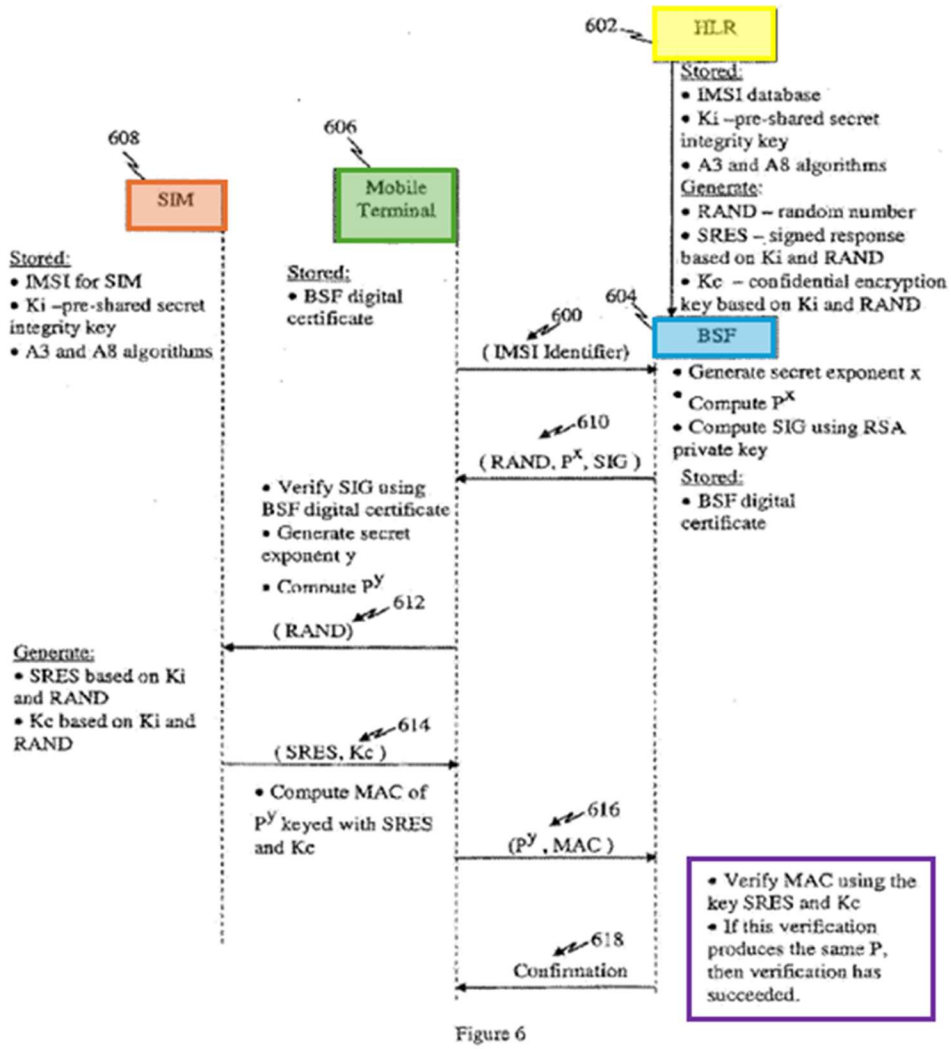


Figure 6

90. 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.

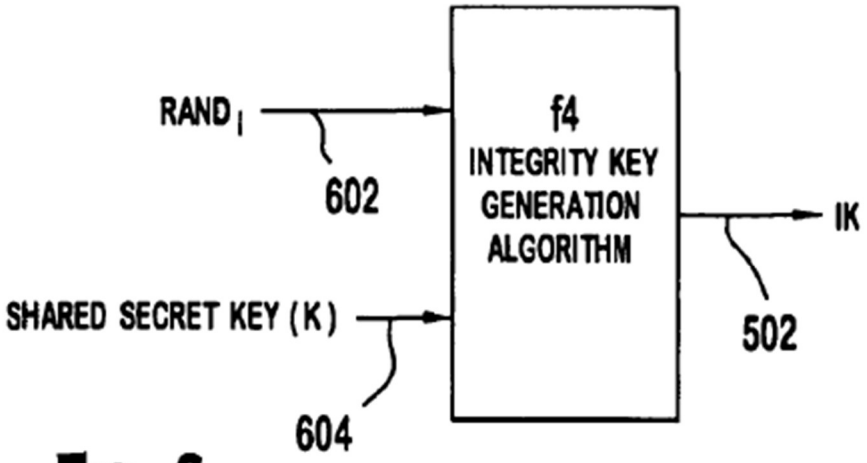


FIG. 6

Claim element	Semple	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**

91. Thus, Semple-Wang renders obvious Claim 1.

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

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

92. In my opinion, Semple-Wang teaches Claim 2.

93. As explained in the Section discussing claim limitation 1(a)(5), 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. 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. This is consistent with how the challenged patent describes what it means by a temporary identification. Ex-1001, 88:29-37 ("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 method 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.

94. In my opinion, Semple-Wang teaches Claim 3.

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

95. Semple teaches “a pre-shared secret key (e.g., Ki) 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 “Ki” corresponds to the recited “key K” (see row of table in discussion of claim 1, above). Specifically, Semple’s pre-shared key Ki is used to calculate Kc and SRES, which are known in the ETSI and 3GPP specifications to be calculated from the pre-shared subscriber key K. *See, e.g.,* 3GPP TS 33.102 (3G Security; Security Architecture). 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

96. Semple 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. Semple 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.

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

97. Semple 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"). *See also id.* Fig. 6 (610).

c. Claim 4: The method 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.

98. In my opinion, Semple-Wang teaches Claim 4.

99. Semple teaches that "the pre-shared secret key (e.g., Ki)" 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 method of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.

100. In my opinion, Semple-Wang teaches Claim 5.

101. Semple 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. Semple 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. It was also well known that a SIM card comes with the secret key. Ex-1022 (Ala-Laurila) ¶¶18 ("[t]he SIM is provided by the mobile network GSMNW operator" and "comprises a secret key Ki"), 25 ("[t]he terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein").

e. Claim 6: The method 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.

102. In my opinion, Semple-Wang teaches Claim 6.

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

103. As explained with reference to claim element 1(a)(1) above, Semple teaches that "SIM 204 may contain a secret key Ki, 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

104. As explained with reference to claim element 1(a)(2) above, 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.

Computing a public key from a private key in an elliptic curve group was a well known method of performing Diffie-Hellman key agreement. *E.g.,* Ex-1033 (Boyd-Mathuria), 196.

f. Claim 7: The method 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.

105. In my opinion, Semple-Wang teaches Claim 7.

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

106. 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 Kc, 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.

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

107. As explained with reference to claim element 1(a)(3), 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.

g. Claim 9: The method 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.

108. In my opinion, Semple-Wang teaches Claim 9.

109. As explained with reference to claim element 1(a)(2) above, 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-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-1012 (SEC1), 93-94, 77 ("The surest way to secretly generate a key is to generate it randomly.").

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

110. In my opinion, Semple-Wang teaches Claim 11.

111. 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. As also explained with respect to claim element 1(a)(1) above, 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. 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-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 method 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.

112. In my opinion, Semple-Wang teaches Claim 12.

113. 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. 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-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").

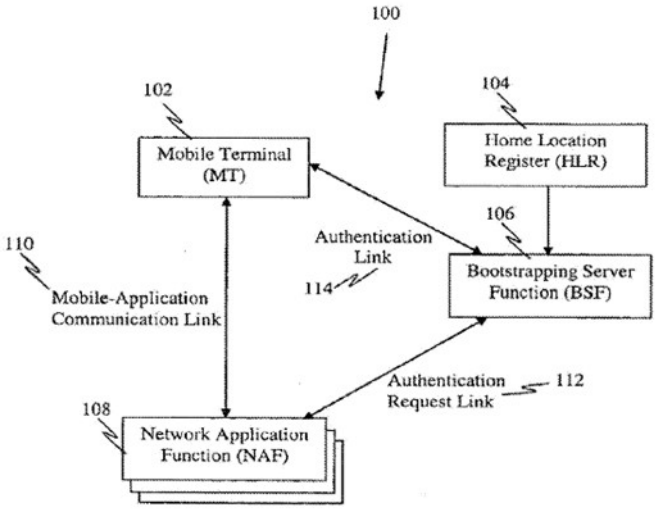


Figure 1

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

114. In my opinion, Semple-Wang teaches Claim 14.

115. Semple teaches that the MT is coupled to a communication interface "to communicate with a wireless network." Ex-1005 ¶23. As shown in Figure 1 below, Semple 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.

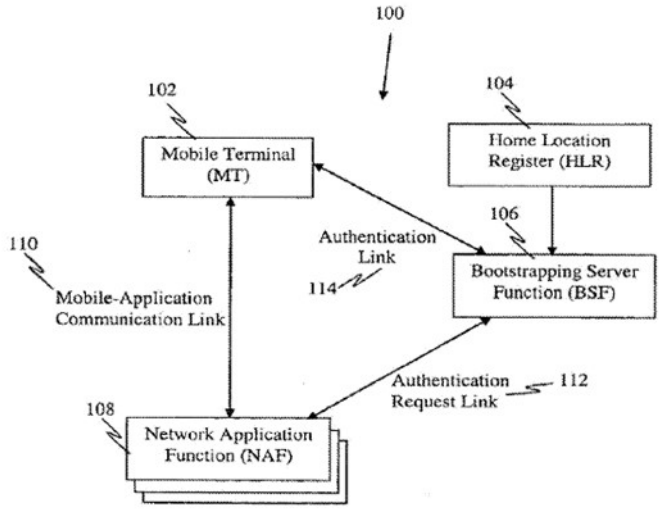


Figure 1

k. Claim 15: The method 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.

116. In my opinion, Semple-Wang teaches Claim 15.

117. Semple teaches that "a storage medium may represent one or more devices for storing data, including read-only memory (ROM)." Ex-1005 ¶22. Semple 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, Semple 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 Semple 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-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").

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

118. In my opinion, Semple-Wang teaches Claim 16.

119. 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-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.

120. 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.

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

121. In my opinion, Semple-Wang teaches Claim 18.

122. As explained with reference to claim limitations1(a)(3)-(1)(a)(4) above, 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. E.g., Ex-1033 (Boyd-Mathuria), 138 (describing KDF functions), 292 (discussing X9.63). 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-1012, 35-36 (listing supported symmetric encryption schemes: "AES-128 in CBC mode" and "AES-128 in CTR mode"); 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.

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

123. In my opinion, Semple-Wang teaches Claim 19.

124. 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. Ex-1029 (CSMG, Reprogrammable SIMs), 16.

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

125. In my opinion, Semple-Wang teaches Claim 20.

126. 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 Ki 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. 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. E.g., Ex-1027 (Natarajan) ¶5 ("mobile and wireless devices, like smart phones, PDAs, cellular phones and Remote control systems, play an increasingly important role in the digital environment.").

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.

127. In addition to the reasons set forth below, 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 XI.A.1; Ex-1007, Abstract.

128. 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-1022 (Ala-Laurila) ¶¶18, 25.

129. 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.

130. 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. 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.

131. A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Bhuyan. All three describe methods for securing wireless communications using authentication and key agreement mechanisms. *See* Section XI.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.

2. Dependent Claims 5 and 8

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

132. In my opinion, Semple-Wang in view of Bhuyan ("Semple-Wang-Bhuyan") teaches Claim 5.

133. Semple-Wang teaches Claim 5 for the reasons described in Section XI.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 [has] 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, Ki, 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 method 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.

134. In my opinion, Semple-Wang-Bhuyan teaches Claim 8.

135. 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." 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 method 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.

136. In my opinion, Semple-Wang in view of Pierce ("Semple-Wang-Pierce") teaches Claim 10.

137. As explained in Section XI.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-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. 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-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.

138. 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.

139. 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.

140. A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Pierce. All three describe methods for securing wireless communications using authentication and key agreement

mechanisms. *See* Section XI.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.

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.

141. In addition to the reasons set forth below, 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 XI.A.1; Ex-1008 ¶34, Abstract.

142. 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.

143. A POSITA, seeking to enhance the security of Semple's protocol, would have been motivated to include a virtualized server in the method, as taught by Jorgensen. Specifically, including a virtualized server such as the EVFS used in Jorgensen's secure network system in Semple's method 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-1026 (Nguyen) ¶59, Abstract. In the Semple-Wang-Jorgensen combination, Semple's method would include a virtualized server and its authentication message would comprise a single user datagram protocol packet, as taught by Jorgensen.

144. A POSITA would have had a reasonable expectation of success in combining the teachings of Semple-Wang with Jorgensen. All three describe methods for securing wireless communications using authentication and key agreement mechanisms, including encryption schemes using ECC private keys. *See* Section XI.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.

2. Dependent Claims 13 and 17-18

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

145. In my opinion, Semple-Wang in view of Jorgensen ("Semple-Wang-Jorgensen") teaches Claim 13.

146. 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. 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 method of claim 1, wherein the message comprises a single user datagram protocol packet.

147. In my opinion, Semple-Wang-Jorgensen teaches Claim 17.

148. 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 method of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.

149. In my opinion, Semple-Wang-Jorgensen teaches Claim 18.

150. Semple-Wang teaches Claim 18 for the reasons described in Section XI.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(a)(3)

151. In my opinion, Semple-Wang in view of SEC1 ("Semple-Wang-SEC1") teaches Element 1(a)(3).

152. To the extent PO argues that Element 1(a)(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 XI.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. 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. 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.

F. Grounds 6-8

153. In my opinion, 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.

XII. CONCLUSION

154. For the reasons above, it is my opinion that Claims 1-20 of the '864 Patent are obvious based on each of the grounds specified in my Declaration.

155. I declare that all statements made in my Declaration of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: November 7, 2025

Dr. Christina Pöpper

Petitioner Samsung Ex-1002, 0104