

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

NETWORK-1 TECHNOLOGIES, INC.,
Patent Owner.

IPR2026-00115
Patent 11,606,204

DECLARATION OF DR. KONSTANTINOS PSOUNIS

Signed: 

Dr. Konstantinos Psounis

February 20, 2026

I. Introduction

1. My name is Konstantinos Psounis. I am over eighteen years of age, of sound mind, and qualified to make the statements set forth in this Declaration. With the exception of the legal principles counsel has supplied to me, all the facts and statements contained herein are within my personal knowledge and are in all respects true and correct.

2. I have been asked by Network-1 Technologies, Inc. (“Network-1” or “Patent Owner”) to submit this declaration in response to a Petition in IPR2026-00115 from Samsung Electronics Co. Ltd., and Samsung Electronics, America, Inc., (“Samsung” or “Petitioner”) regarding U.S. Patent No. 11,606,204 (“the ’204 Patent”).

3. I am being compensated for my time at my current standard rate of \$950 per hour for the services that I provide in connection with this case. That compensation is not contingent upon my performance, the outcome of the case, or any issues involved in or related to this case.

4. I declare under penalty of perjury that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. I further understand that willful false statements and the like are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code.

II. Qualifications

5. I have summarized in this section my educational background, career history, publications, and other relevant qualifications. My full *curriculum vita* is attached as Exhibit 2027 to this declaration.

6. I am a Professor and prior Associate Chair of Electrical and Computer Engineering and Professor of Computer Science at the University of Southern California. I joined the University of Southern California in 2003, after completing my PhD at Stanford University as a Stanford Graduate Fellow.

7. My professional career spans more than 20 years. As set forth in Exhibit 2027, I have extensive experience in the field of networked distributed systems, including the Internet and the web, Wi-Fi and cellular wireless systems, spectrum sharing wireless systems, sensor and IoT wireless systems, mobile ad hoc and delay tolerant wireless systems, data centers and cloud systems, peer to peer systems, and autonomous vehicles/drones systems.

8. I have published more than 100 technical papers in these fields, which have been cited tens of thousands of times. I have also been awarded numerous grants and significant funding from the government and industry leaders to advance these fields. As a result, I have been named an Institute of Electrical and Electronics Engineers (IEEE) Fellow, the highest grade of membership, for “fundamental

contributions in the theory and practice of wireless networks,” and a Distinguished Member of the Association of Computing Machinery (ACM).

9. Throughout my career, I have analyzed, designed, and developed efficient networked distributed systems for the Internet and the Web, Wi-Fi and cellular wireless systems, spectrum sharing wireless systems, sensor and IoT wireless systems, mobile ad hoc and delay tolerant wireless networks, data centers and cloud systems, peer to peer systems, and autonomous vehicles/drones systems. As such, I have acquired extensive expertise in the analysis and development of those systems and associated products.

10. I have extensive experience with and made contributions specifically towards analyzing and designing efficient Wi-Fi, cellular and other wireless systems. In particular, I have received multiple funding awards from the National Science Foundation (NSF), the leading governmental agency for funding computer engineering and computer science research, to work on wireless systems, including Wi-Fi systems. I have also received multiple funding awards from the industry leaders in the area of networking and in particular wireless networking, to work on these systems. I have published several papers in the most selective academic journals and conferences on wireless systems. I have also been the faculty in charge of the entire networking curriculum at the Electrical and Computer Engineering

department at USC for more than a decade and teach networking classes and in particular the graduate wireless networking class yearly.

11. I also have extensive practical experience with networked distributed systems. For example, I was a co-founder of SpaceMUX, Inc. (whose IP was later acquired by Quantenna Communications, Inc.), where I designed and developed systems to increase the speed of wireless networked systems using modern wireless networking technologies and techniques. Also, I was the Technology Architect for Fineground Networks (later acquired by Cisco Systems, Inc.), where I designed and developed systems to accelerate the delivery of content over the World Wide Web. In addition, for over 20 years both at Stanford University and at the University of Southern California I have designed and implemented efficient algorithms, protocols, and systems for a variety of distributed networked systems, and I have consulted for industrial leaders, and produced prototype systems. I have also applied for and been granted numerous patents, which are owned by network industry leaders and prestigious academic institutions.

12. In sum, I have extensive experience in and familiarity with the fields of networked distributed systems and in particular with wireless networking systems including Wi-Fi and cellular wireless systems, and extensive experience and contributions towards the analysis, design, and implementation of such systems.

III. Materials Considered

13. Among the materials I have reviewed in forming my opinions are the '204 Patent, its prosecution history, as well as the patents, references, and other materials cited in this expert declaration.

14. I have also reviewed the Petition and its exhibits, including the declaration of Dr. Christina Pöpper, Ph.D. (Exhibit 1002).

IV. Legal Principles

15. I am not a lawyer. In forming my opinions as set forth in this Declaration, I have relied upon legal principles supplied to me by attorneys for Atlas. In forming my opinions, I have not relied upon Patent Owner's attorneys for any purpose other than the following legal principles.

A. Claim Construction

16. I understand that determining whether a patent claim is valid requires a two-step analysis. First, the claim must be construed. Second, the properly construed claim must be compared to the prior art.

17. With respect to the first step, I understand that claims are construed from the perspective of a person of ordinary skill in the art ("POSITA") at the time of the purported invention. I understand that, absent a disclaimer or express definition, claim terms are given their plain and ordinary meaning to a POSITA in view of the specification and file history and the knowledge of a POSITA. Unless

otherwise noted, I have applied what I consider to be the plain and ordinary meaning of all terms as understood by a POSITA at the time of the invention.

B. Anticipation

18. I understand that, although not expressly disclosed, subject matter may be inherently disclosed in a prior art reference where that subject matter is necessarily present in the subject matter disclosed and would be understood to be so by those of ordinary skill in the art. I understand that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic.

19. I understand that a claim is invalid if each and every element of the claim is disclosed in a single prior art reference with the elements arranged as specified in the claim, either expressly or inherently. I understand that invalidity based on the disclosure of a single prior art reference in this manner is called anticipation.

C. Obviousness

20. I understand that a claim would have been obvious under 35 U.S.C. § 103 if one or more prior art references disclose every claim limitation in such a way so as to render the claim, as a whole, obvious to a person of ordinary skill in the art at the time the purported invention was made.

21. In determining whether or not a patented invention would have been obvious, the following factors should be considered: (a) the scope and content of the prior art; (b) the differences between the prior art and the claims at issue; (c) the level of ordinary skill in the art; and (d) whatever “secondary considerations” may be present.

22. I understand that certain “secondary considerations” may be relevant in determining whether or not an invention would have been obvious, and that these secondary considerations may include commercial success of a product using the invention, if that commercial success is due to the invention; long-felt but unsolved need for the invention; evidence of copying of the claimed invention by others; industry acceptance; initial skepticism of the invention; failure of others to solve the problem; praise of the invention by others; the taking of licenses under the patents by others; and simultaneous invention by others (which may be an indication that the claimed invention was the result of ordinary skill in the art).

23. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. While multiple prior art references or elements may, in some circumstances, be combined to render a patent claim obvious, I understand that I should consider whether there is an apparent reason to combine the prior art references or elements in the way the patent claims. To determine whether such an

apparent reason exists to combine the prior art references or elements in the way a patent claims, it will often be necessary to look to the interrelated teaching of multiple patents, to the effects of demands known to the design community or present in the marketplace, and to the background knowledge possessed by a person having ordinary skill in the art.

24. I also understand that when the prior art teaches away from combining prior art references or certain known elements, discovery of a successful means of combining them is more likely to be non-obvious. A prior art reference may be said to teach away from a patent when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the patent or would be led in a direction divergent from the path that was taken by the patent.

25. I also understand that it is not permissible to use hindsight in assessing whether a claimed invention is obvious. Rather, I understand that, to assess obviousness, you must place yourself in the shoes of a person having ordinary skill in the relevant field of technology at the time the inventions were made who is trying to address the issues or solve the problems faced by the inventor and ignore the knowledge you currently now have of the inventions.

26. I also understand that there are numerous ways in which to articulate the legal standard for obviousness, including: (1) combining prior art elements according to known methods to yield predictable results, (2) simple substitution of

one known element for another to obtain predictable results, (3) use of a known technique to improve similar devices (methods, or products) in the same way, (4) applying a known technique to a known device, method, or product ready for improvement to yield predictable results, (5) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success, (6) known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art, and (7) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

D. Person of Ordinary Skill in the Art

27. I understand that the meaning of claim terms and a patent's validity are to be determined from the vantage point of one of ordinary skill in the art at the time of the invention (a "POSITA"). In determining who would be one of such ordinary skill, I understand it is appropriate to consider criteria such as: (a) the type of problems encountered in the art; (b) prior art solutions to those problems; (c) the rapidity with which innovations are made; (d) the sophistication of the technology; and (e) the education level of active workers in the field.

V. The Level of Ordinary Skill in the Art

28. For the purposes of this declaration supporting the Patent Owner's Preliminary Response, I have been asked to apply the same POSITA definition as Dr. Pöpper and assume that a POSITA "would have had at least a bachelor's degree in electrical engineering, computer engineering, computer science, or a similar field and 2-3 years of experience with cellular/WLAN security and mobile devices, with additional education substituting for experience and vice versa." EX1002 ¶ 17. I understand that if trial is instituted, I will have the opportunity to propose my own definition of a POSITA.

VI. Analysis

29. I have been asked to opine on a limited number of issues for the purpose of supporting the Patent Owner's Preliminary Response. I understand that if trial is instituted, then I will have the opportunity to submit additional analysis on these and other issues.

A. Technological background.

30. Cellular networks need to identify and authenticate users on their network to ensure they only provide access to authorized users or devices. *See* EX2025, 1-3. One tool used to provide this authorization is the international mobile subscriber identity ("IMSI"). EX1005 ¶26. The IMSI can be provided on a SIM card and uniquely identifies every user of a cellular network and allows a cellular network

to acquire other information and details about the mobile device from the home location register (“HLR”), such as the unique secret key(s) shared between the mobile device and the HLR, also known as key K. *Id.* This information can be used for various purposes, including authenticating a mobile device and establishing encrypted communications. *Id.*; *see also* EX2025, 3-5.

31. Various approaches to authenticating a mobile device have been described by standards setting bodies such as the European Telecommunications Standards Institute (“ETSI”) and the 3rd Generation Partnership Project (“3GPP”). *See* EX2025, 1-6; EX1005 ¶9. These systems use the IMSI to identify a key K or K_i and derive further keys used to secure transmissions between the device and the network. *Id.* The key K serves an important function in this process. EX1006 ¶33. It can be provided on a mobile device’s SIM card and serves as a unique key that can be used to generate the authentication vectors and response parameters used to authenticate a mobile device. *Id.*

32. But, a cellular network cannot receive this information until it first obtains the mobile devices IMSI. *See* EX2025, 4-6. Historically, this required the IMSI to be transmitted “in the clear” and unencrypted from a mobile device to a cellular network. EX1006 ¶5; EX2025, 5-6. By transmitting “in the clear” third parties could intercept the IMSI and track a mobile device, creating serious privacy and security concerns. EX2025, 6.

33. The '204 Patent solves this problem by creating a system that enables encrypted transmission of the IMSI and subsequent authentication between the mobile device and mobile network. Claim 1, the only independent claim of the '204 Patent, is quoted below:

1. A mobile device comprising:

(a) at least one processor; and

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

- (1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;
- (2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;
- (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;
- (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;
- (5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and
- (6) authenticating with the wireless network using a message digest with the pre-shared secret key.

EX1001, 100:31-67 (claim 1).

B. Summary of Petitioner's Arguments

34. In the Petition and the nearly identical declaration of Dr. Christina Pöpper, Petitioner and Dr. Pöpper assert eight grounds of obviousness. Pet. 3-4; EX1002 ¶20. Only Grounds 1 and 5 address the independent claim of the '204 Patent. *Id.* Ground 5 only addresses element 1(b)(3) and otherwise refers back to the arguments of Ground 1. EX1002 ¶¶154-155. For the purposes of this declaration

submitted in support of Patent Owner's Preliminary Response, I have focused my analysis on the arguments presented in Ground 1 with respect to claim 1, but these arguments apply to all Grounds raised in the Petition.

35. Petitioner and Dr. Pöpper assert that claim 1 of the '204 Patent is obvious in view of "Semple" and "Wang." EX1002 ¶20. Semple is U.S. Patent Publication No. 2010/0174907, titled "Secure bootstrapping for wireless communications." EX1005, cover. Wang is International Publication Number WO 2008/005162 titled "Method and apparatus for security protection of an original user identity in an initial signaling message." EX1006, cover. Both are directed in relevant part towards mutual authentication between a mobile device and a cellular network. *See* EX1005, Abstract; EX1006, Abstract. I discuss both in more detail, below.

36. Petitioner and Dr. Pöpper do not appear to assert that either document teaches or suggests every element of Claim 1 of the '204 Patent. Instead, they describe a Semple-Wang system, which at a high level, modifies Semple to include an encrypted IMSI as described in Wang. *See* EX1002 ¶¶61-62. For reasons I explain below, a POSITA would never modify Semple in this way, and the Petitioner and Dr. Pöpper's arguments can only be explained by hindsight used to re-create claim 1 of the '204 Patent.

C. Dr. Pöpper's Proposed "Semple-Wang" System Reduces Security.

1. The Semple-Wang System

37. Petitioner and Dr. Pöpper propose that a POSITA would modify Semple and Wang by modifying the process described in Semple's Figure 6:

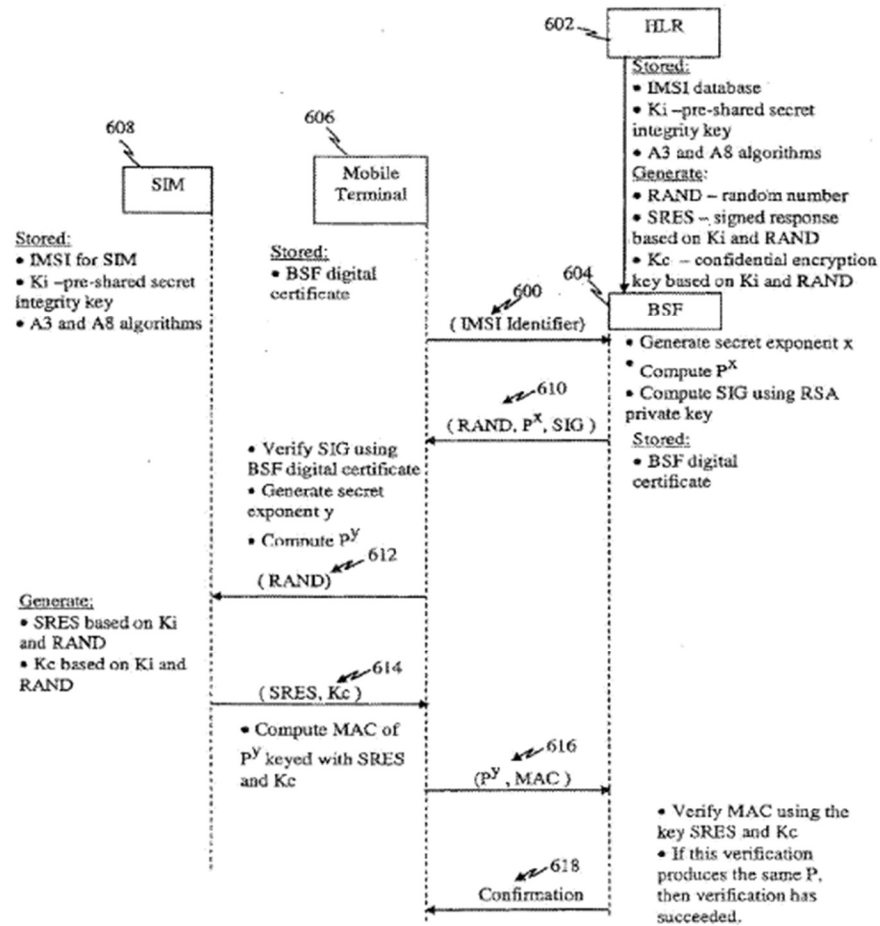
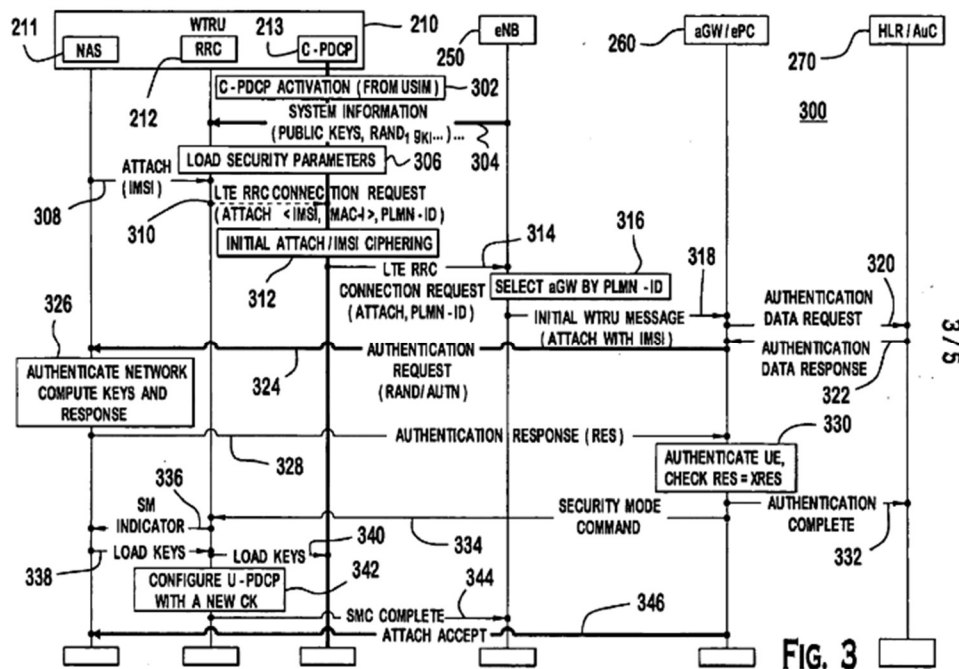


Figure 6

EX1005, Fig. 6; *see, e.g.*, EX1002 ¶¶86-88. The proposed modification changes step 616 of Semple, and Petitioner and Dr. Pöpper contend that a POSITA would look to Wang when changing this step. *Id.*

38. As described by Semple, step 616 transmits two items: 1) a public key of a mobile terminal, P_y , and 2) a MAC of P_y keyed with SRES and key K_c . EX1005 ¶49. This transmission allows the BSF to generate a shared key P_{xy} , that may be used in later communications. *Id.* ¶51. Wang, in the relevant discussion, teaches steps 312 and 314 that send a “attach message” including a ciphered IMSI along with a MAC-I from a WTRU (a mobile device) to an eNode-B (a base station). EX1006 ¶31. This step is illustrated in Figure 3 of Wang:



Id. Fig. 3.

39. Note that both Semple and Wang send an IMSI as part of an initial connection step, step 600 in Semple and step 314 in Wang. EX1005 ¶48; EX1006 ¶31. As I explain further below, this order of operations is a key part of the security systems described by both references. It is also clear that neither reference sends an

IMSI (encrypted or otherwise) in the same message as a public key for the mobile device, as required by claim 1 of the '204 Patent. *See, e.g., id.* And as the Petitioner and Dr. Pöpper appear to recognize, neither reference suggests encrypting an IMSI using a symmetric key generated using an elliptic curve integrated encryption scheme. EX1002 ¶¶87-88. For those reasons alone, Semple-Wang does not render the claims obvious.

40. To solve this failure in the art, Petitioner and Dr. Pöpper do not simply propose inserting the encryption technique from Wang into Semple. Instead, they propose completely changing the system described by Semple such that step 600 (sending the unencrypted IMSI) is moved into step 616, and the IMSI is transmitted with the Py and MAC. *Id.* ¶88. But, since Semple does not suggest encrypting the IMSI at this point, Petitioner and Dr. Pöpper further modify Semple to use a shared key Pxy to encrypt the IMSI when it is transmitted in step 616. *Id.* This change also includes Wang's MAC-I in step 616, resulting in two MACs sent in a single message. *Id.* The modification is allegedly supported by Semple's teaching that, after step 616, both the mobile terminal and BSF of Semple can have a shared key Pxy that can use to compute "[a] key for further communications." EX1002 ¶¶88-89; EX1006 ¶51.

41. Dr. Pöpper illustrates this modification in paragraph 88 of her declaration:

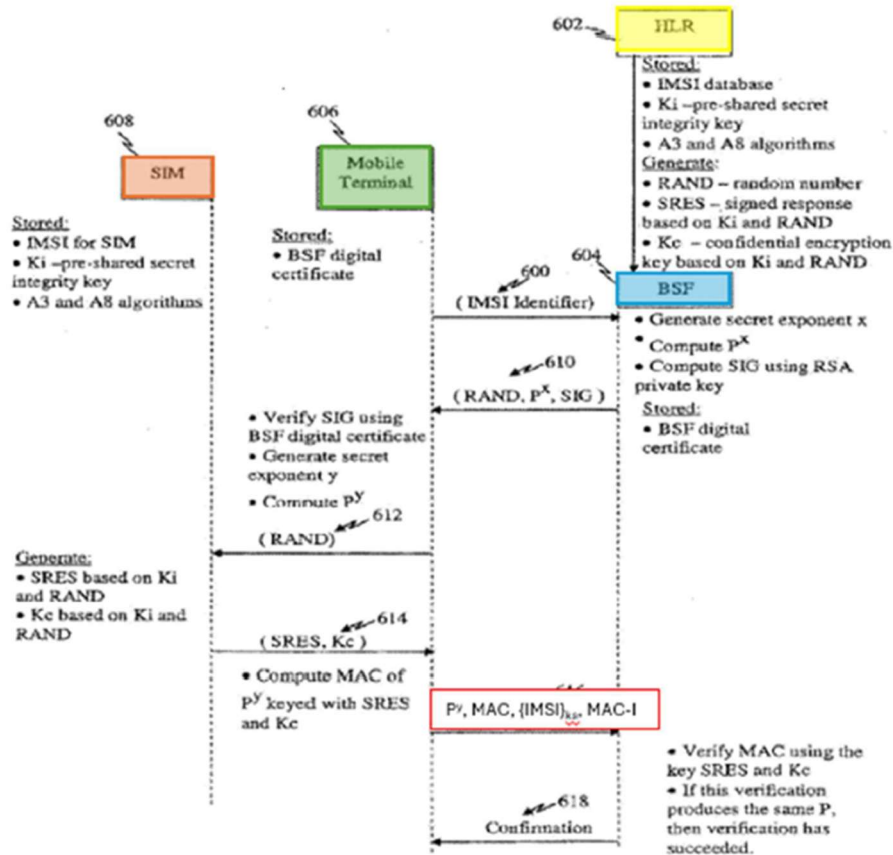


Figure 6

EX1002 ¶88. I note that though the above figure leaves step 600 in place, Petitioner and Dr. Pöpper appear to propose removing step 600 as “it not necessary since computing x and P^x does not depend on IMSI or the pre-shared key associated with it.” EX1002 ¶87. Certainly, neither Petitioner nor Dr. Pöpper argue that the IMSI would be sent twice in the modified Semple-Wang system. Regardless, I address the Semple-Wang combination both with and without step 600, below.

2. Semple and Wang use the same order of operations

42. Petitioner and Dr. Pöpper’s Semple-Wang system can only be explained by hindsight. Neither reference suggests of the proposed modification, and

a POSITA would understand that making this change would, at best, provide no additional security over Semple (if the IMSI were still transmitted in step 600), or, at worse, make Semple less secure (if the IMSI were not transmitted in step 600).

43. As an initial matter, neither Semple nor Wang suggest transmitting the IMSI as part of an authentication response step, and much less with the module public key, as claimed by the '204 Patent. As I noted above, both require that the IMSI be transmitted at the initial connection phase and separate from the authentication response. In Semple's step 600 and Wang's step 314, the mobile device sends its IMSI to the cellular network, which eventually arrives at the bootstrapping server function ("BSF") and then the home location register ("HLR") of the device's home network. EX1005 ¶48; EX1006 ¶¶31-33. With the IMSI, the HRL can identify the corresponding keys, generate a random number to use during the authentication process ("RAND"), and using the key(s) and RAND, generate a response value that will be used to authenticate the mobile device (SRES in Semple and XRES in Wang). EX1005 ¶48; EX1006 ¶¶33-34.

44. Both systems then send a form of authentication request back to the mobile device that includes RAND (Semple step 610 and Wang step 324). EX1005 ¶48-49; EX1006 ¶¶33-34. But, Semple and Wang transmit slightly different information with the RAND in this step. Semple sends a SIG value, which is a digital signature of Semple's BSF (not the HLR) computed using the BSF's RSA private

kye. EX1005 ¶48. Wang send a AUTN value, which is an authentication token generated by the HLR and comprises “a sequence number (SQN) hidden by an anonymity key (AK), an authentication management field (AMP) which specifies certain authentication components, (such as algorithms to be used, key lifetime, etc.), and a message authentication code (MAC) which is functionally dependent on the SQN, the AMF, and the RAND.” EX1006 ¶7, 33-34.

45. In the un-modified systems of Semple and Wang, the mobile device can use the authentication request to verify the authenticity of the mobile network and generate its own authentication response. In Semple, a digital certificate is used to verify the BSF. EX1005 ¶48-49. In Wang, the mobile device “authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC” of the AUTN. EX1006 ¶34.

46. In both Semple and Wang, the mobile device then uses RAND and their own keys to compute a response (SRES or RES). EX1005 ¶49; EX1006 ¶35. This response is transmitted back to the mobile network, which confirms that the response received by the mobile device matches the previously calculated one. EX1005 ¶50; EX1006 ¶35.

47. A POSITA would not re-order these steps to send the IMSI *after* the authentication request, as Petitioner and Dr. Pöpper propose. Both systems rely on their order of operations, and there is simply no teaching that suggests such a change.

The Semple-Wang system created by Petitioner and Dr. Pöpper is a completely new system that can only be explained with the hindsight of the '204 Patent.

3. A POSITA would not be motivated to create the Semple-Wang system proposed by Petitioner and Dr. Pöpper.

48. Not only is there no teaching for this change, but the proposed change creates an un-secure system that is vulnerable to attack.

49. As an initial matter, the '204 Patent improves security of the IMSI by performing the encryption at the very beginning of the transmissions between the mobile device and the network. Thus, the IMSI is encrypted throughout the communications. Neither Semple nor the Semple-Wang combination accomplish this. Semple sends the IMSI in the clear, because HLR needs to first identify that the mobile terminal belongs to the network prior to generating RAND and providing it to the BSF. EX1005 ¶48. And as explained below, the Semple-Wang combination introduces new vulnerabilities that a POSITA would seek to avoid.

50. To briefly dispense with Wang, Petitioner and Dr. Pöpper do not argue that Wang itself would be modified to send the IMSI after the authentication request. Regardless, Wang's AUTN cannot be generated without first receiving the IMSI, so there is no way that change could be made in Wang. EX1006 ¶7-8, 33-34.

51. Turning back to Semple, sending the IMSI prior to receiving the authentication message in step 610 is a key security feature of Semple's system. *See* EX1005 ¶53. As I noted above, Semple describes authenticating the mobile network

to the mobile device using a SIG in message 610 that is generated based on the RSA private key of the BSF, which can be authenticated by the mobile device using a pre-store digital certificate. EX1005 ¶¶48-49. Wang, on the other hand, uses an AUTN generated using the shared secret keys of the HLR. EX1006 ¶¶7-8, 33-34.

52. Petitioner and Dr. Pöpper's modified Semple-Wang system is illustrated again below, for reference:

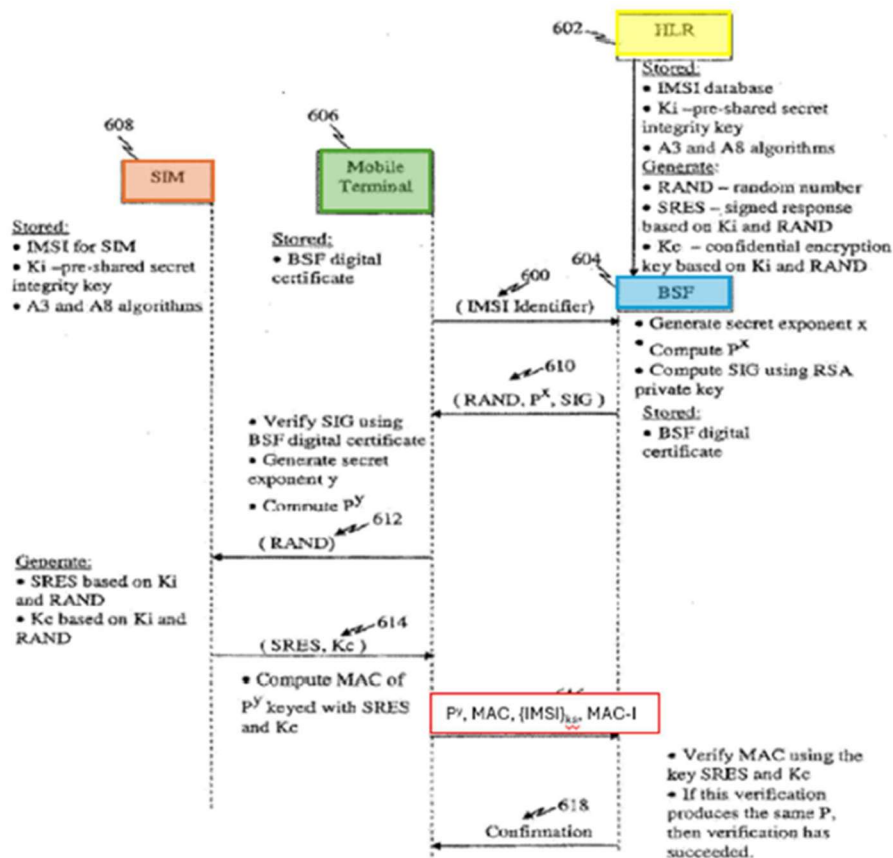


Figure 6

EX1002 ¶88. As Semple explains, the message 610 is only sent in response to receiving a valid IMSI. EX1005 ¶48. A POSITA would understand that this timing provides necessary security to the SIG and that changing it creates vulnerabilities in

the system. Indeed, Semple itself recognizes the importance of this timing. EX1005 ¶53.

53. Assuming that Petitioner and Dr. Pöpper propose removing step 600, broadcasting RAND, Px, and SIG to any device attempting to connect to the network (whether it has a valid IMSI or not) opens those values and the underlying keys to attack by providing time for an attacker to either compromise the keys or identify vulnerabilities. In one example, it increases the chance of an attacker intercepting and replaying messages between the BSF and mobile device, possibly tricking the BSF into communicating with an imposter device.

54. The modified Semple-Wang system also increases the risks of a compromised digital certificate at the BSF or an otherwise compromised BSF because it does not rely on the security of the HLR as both Wang and Semple do. In that situation, a mobile device would not be able to identify that the BSF was fraudulent because the mobile device cannot confirm that the BSF had its key K. That fraudulent BSF could then send its own forged message 610 to a mobile device with its own RAND, its own key Px, and a forged SIG that the mobile device would not be able to detect. The fraudulent BSF would then be able to intercept the Py, encrypted IMSI, and MAC of the mobile device. Because Py is not generated with the shared secret key, the fraudulent BSF will be able to generate Pxy and decrypt the IMSI. This allows the IMSI to be intercepted, as if it were transmitted in the

clear. But now, the fraudulent BSF could respond with a fraudulent confirmation message 618. This way, the fraudulent BSF can set up communications that appear secure and authentic to the mobile terminal, but in fact, are directly to a fraudulent system. No POSITA would modify Semple to create these security vulnerabilities.

55. By transmitting message 610 only in response to message 600, Semple reduces these problems. Indeed, Semple explains that with its system—only sending a response to a valid IMSI—various security improvements can be implemented, including using a new RAND with each instance of the protocol and ensuring that the Py and MAC are received within a short time frame. EX1005 ¶53.

56. To the extent that Petitioner and Dr. Pöpper suggest leaving step 600 in the Semple-Wang system but modifying it to include an encrypted IMSI in message 616, no POSITA would make that change. First, it provides no extra security, because the IMSI is still transmitted in the clear in step 600. Instead, an entirely redundant block of encrypted data is simply added to message 616 only for the purpose of manufacturing the claims of the '204 Patent from hindsight. Neither Semple nor Wang suggest sending the IMSI twice. And as I noted above, neither even suggest sending the IMSI with the authentication response message.

57. In sum, Petitioner and Dr. Pöpper's proposed Semple-Wang system would not function in use. Not only do Semple and Wang fail to disclose certain

elements of the claims of the '204 patent entire, but neither Semple nor Wang support such the combination proposed by Petitioner and Dr. Pöpper.

4. The '204 Patent Solved a long-felt need.

58. As I noted above, the need to securely transmit the IMSI was a long-recognized challenge in cellular communications. EX2025, 1-6. Sending the IMSI in the clear creates serious privacy concerns and potential weaknesses in communication security. *Id.*, 6. Various techniques were developed to offer some protection. *Id.* For example, GUTI could temporarily be used instead of the IMSI, but that technology still required the IMSI to be periodically transmitted in the clear. *Id.* The inventors of Wang also recognized that transmitting the IMSI unprotected was a problem, EX1006 ¶5.

59. The invention of the '204 Patent solves this long felt need. The invention of the '204 Patent encrypts the IMSI from the beginning of the communications between the mobile device and the network while ensuring that the mobile device and network are able to reliably authenticate each other. Despite the long felt need, this solution did not exist in the art prior to the invention of the '204 Patent.