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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 April 2006 (06.04.2006)

PCT

(10) International Publication Number
WO 2006/036521 A1

(51) International Patent Classification:
H04Q 7/32 (2006.01)

(21) International Application Number:
PCT/US2005/032337

(22) International Filing Date:
6 September 2005 (06.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/608,305	8 September 2004 (08.09.2004)	US
Not furnished	2 September 2005 (02.09.2005)	US

(71) Applicant *(for all designated States except US)*: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SEMPLE, James** [CA/GB]; 7 Queensgate Place, Flat 4, London South Wales SW7 5NU (GB). **ROSE, Gregory Gordon** [AU/US]; 3234 North Star Drive, San Diego, CA 92117 (US). **PADDON, Michael** [AU/AU]; 31 Armine Way, Kellyville, NSW 2155 (AU). **HAWKES, Philip Michael** [AU/AU]; 18-20 Knocklayde St, Unit 30, Ashfield, NSW 2131 (AU).

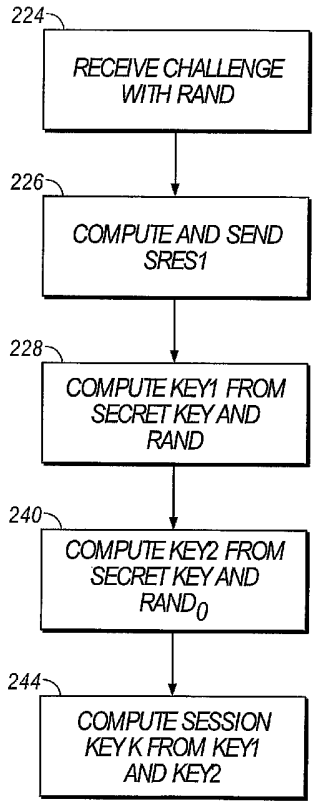
(74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, CA 92121 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: BOOTSTRAPPING AUTHENTICATION USING DISTINGUISHED RANDOM CHALLENGES



(57) Abstract: A communications system and method of bootstrapping mobile station authentication and establishing a secure encryption key are disclosed. In one embodiment of the communications network, a distinguished random challenge is reserved for generation of a secure encryption key, wherein the distinguished random challenge is not used for authentication of a mobile station. The distinguished random challenge is stored at a mobile station's mobile equipment and used to generate a secure encryption key, and a bootstrapping function in the network uses a normal random challenge to authenticate the mobile station and the distinguished random challenge to generate the secure encryption key.

WO 2006/036521 A1

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BOOTSTRAPPING AUTHENTICATION USING DISTINGUISHED RANDOM CHALLENGES

Claim of Priority under 35 U.S.C. § 119

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/608,305 entitled "BOOTSTRAPPING GSM AUTHENTICATION AND DISTINGUISHED RANDS" and filed on September 8, 2004. The disclosure of the above-described filed application is hereby incorporated by reference in its entirety.

BACKGROUND

Field

[0002] The application relates generally to authentication in cellular communication networks, and more particularly to the derivation of encryption keys for application security.

Background

[0003] Mobile communication applications generally share a need for authentication of a subscriber (user equipment or mobile station) by a communication server before communication is initiated or a transaction is carried out. One authentication mechanism is based on a secret shared between the communicating entities, and there are a number of authentication protocols that rely on this pre-shared secret.

[0004] In a mobile communications network based on the Global System for Mobile Communications (GSM), for example, the identity of a subscriber is authenticated before the subscriber is allowed to access the communications network. In order for a subscriber's mobile station (or user equipment UE) to establish a communication session with a network element, the mobile station authenticates itself to the network element by responding to a random number challenge. The random number challenge and a shared secret key are used to establish a session encryption key for encrypting communication transmissions between the mobile station and the network element.

[0005] The communications system features described herein can be implemented in a variety of communications networks requiring authentication and encrypted communication between communicating entities. Figure 1 is a block diagram of the communication network entities involved in authentication of a subscriber in a GSM

network. A subscriber's mobile station 30 comprises a secure IC 32 and mobile equipment (ME) 34 (e.g., a cellular telephone handset). The mobile equipment 34 includes a processor 36 configured to perform authentication functions at the mobile station 30 in conjunction with the secure IC 32.

[0006] Stored on the secure IC 32 is subscriber identity and subscription related information, information for performing authentication functions with the communications network, an International Mobile Subscriber Identity (IMSI), preferred language, and IC card identification. The secure IC may be referred to as a SIM card or a smart card. Also stored at the secure IC 32 is a secret key Ki 38 which is used to authenticate the mobile station 30 to a network element 40 of the serving network for access to the network. The secret key Ki 38 is also stored at the mobile subscriber's home network at an authentication center (AuC) 42. The authentication center 42 uses the secret key Ki 38 to generate authentication data specific to the subscriber using the secret key Ki 38, and sends the authentication data to the network element 40.

[0007] An authentication and key generation process for mobile station authentication and encrypted communication is illustrated in Figures 1-3, wherein Figure 2 is a flow diagram illustrating a method of authentication and encryption key generation at the mobile station 30, and Figure 3 is a signal flow diagram illustrating a method of mobile station authentication and encryption key generation in the communications network. In reference to Figure 3, the mobile station 30 requests a communication session with a network element 40 in a step 102. If the network element 40 does not already have security information stored for that subscriber to authenticate the mobile station 30, the network element 40 sends a request for security information to the authentication center 42 in the mobile station's home network in a step 104. In response to the security information request, the authentication center 42 generates one or more authentication vectors comprising a random number challenge RAND, an expected authentication response XRES, and a encryption key Kc. The expected response XRES and the encryption key Kc are determined based on the RAND and the secret key Ki 38. In a step 108, the authentication center 42 sends the authentication vector(s) (RAND, XRES, Kc) to the network element 40.

[0008] The network element 40 selects an authentication vector (RAND, XRES, Kc) to use in authenticating the identity of the mobile station 30 and sends the random challenge RAND of the selected authentication vector to the mobile station 30 in a step

112. Referring to Figure 2, the mobile station 30 receives the authentication challenge with the challenge RAND in step 112, and computes and sends an authentication response in a step 114. The mobile station 30 also computes a session key in a step 115 using the secret key Ki 38 and RAND.

[0009] To produce the response and the session key, the mobile equipment 34 at the mobile station 30 passes the RAND to the secure IC in a step 113. In steps 114 and 115, the secure IC 32 computes a set of one or more values using the received random challenge RAND and the stored secret key Ki. These values generally include an authentication response SRES as shown in step 114. In step 115, the secure IC 32 computes a second value comprising a session encryption key Kc using the received random challenge RAND, the stored secret key Ki 38. In a step 116, the secure IC 32 sends the generated response SRES and the encryption key Kc to the mobile equipment 34 in a step 116. The mobile equipment 34 sends the generated authentication response SRES to the network element 40 in a step 117, and stores the key Kc at the mobile equipment in a step 118. The network element 40 compares the mobile station generated authentication response SRES to the expected response XRES of the selected authentication vector in a step 119. If the authentication parameters do not match, the authentication procedure is terminated. If the parameters do match, the mobile station 30 is considered authenticated in a step 120 and the network element 40 begins communication with the mobile unit using the encryption key Kc in step 122.

[0010] GSM authentication and key agreement procedures are subject to replay and cryptanalytic attack. For example, the conventional algorithms used by the GSM system to encrypt communications are weak. Methods have been devised to determine the encryption key Kc and determine the contents of a subscriber's communications. There is therefore a need in the art for a method of improving application security using the current capabilities of deployed mobile stations, especially as mobile communications become used for more sensitive data or require stronger authentication.

SUMMARY

[0011] In one aspect, the invention includes a mobile station configured for communicating in a wireless communications network. The mobile station comprises a receiver configured to receive at least one authentication data parameter from the wireless communications network and a memory storing a fixed authentication data

parameter. A first processing circuit is configured to generate a first key based on the at least one received authentication data parameter, and to generate a second key based on the fixed authentication data parameter. A second processing circuit is configured to generate a third key using at least the first and second keys.

[0012] In another aspect, a mobile element of a wireless communications network is provided. The wireless communications network comprises a plurality of mobile elements and a plurality of network elements communicating with the mobile elements. The mobile element is configured to authenticate itself to the communications network by responding to a challenge value presented to the mobile element by a network element of the communications network during an authentication procedure. Furthermore, the mobile element comprises a memory storing a reserved challenge value that is not used to authenticate mobile elements in authentication procedures between any network element and any mobile element.

[0013] In another aspect, the invention includes a method of communication between a mobile station and a communications network element. The method includes selecting an authentication challenge at a network element and transmitting the authentication challenge to a mobile station. The method further includes generating a first value comprising an authentication response at the mobile station using at least the authentication challenge and a stored key; generating a second value at the mobile equipment using at least the authentication challenge and the stored key; generating a third value at the mobile equipment using at least a fourth value different from the authentication challenge and the stored key; and generating a key using at least the second and third values.

[0014] In another aspect, a method of creating keys in a communication network that uses a challenge-response authentication procedure comprises reserving at least one challenge value for use in generating session keys for use in communication between mobile units and network elements within the communication network. The reserved challenge value is not used for mobile unit authentication.

[0015] In another aspect, a method of generating a key at a mobile station for securing communication between the mobile station and a network element is provided. In this aspect, the method includes receiving an authentication challenge value from a network element at the mobile station and sending the authentication challenge value to a processing circuit. The method further includes generating a first set of one or more

values using at least the authentication challenge value, sending at least one value from the first set to the network element for authentication. The method continues by sending a second authentication challenge value to the processing circuit and generating a second set of one or more values using at least the second authentication challenge. A key is generated using at least one value of the first set and at least one value of the second set.

[0016] In another aspect, a mobile station in a communications network includes means for receiving an authentication challenge value from the communications network, means for generating a first set of values in response to the received authentication challenge, means for generating a second set of values in response to a distinguished authentication challenge value, and means for generating a key using at least one of the first set of values and at least one of the second set of values.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1 is a block diagram of the communication network entities involved in authentication of a subscriber for communication in a GSM network;

[0018] FIG. 2 is a flow chart illustrating an authentication and key generation process performed at a mobile station according to GSM;

[0019] FIG. 3 is a signal flow diagram illustrating an authentication and key agreement procedure for authentication of a subscriber to a network element in GSM;

[0020] FIG. 4 is a block diagram of one embodiment of the communication network entities involved in authentication of a subscriber using distinguished authentication data;

[0021] FIG. 5 is a flow chart illustrating one embodiment of an authentication and distinguished key generation process performed at a mobile station using distinguished authentication data; and

[0022] FIG. 6 is a signal flow diagram illustrating one embodiment of a method of establishing a secure communication session between a mobile station and a communications network using distinguished authentication data.

DETAILED DESCRIPTION

[0023] As discussed above, the GSM encryption algorithms A5/1 and A5/2 are subject to attack, and methods have been found to obtain knowledge of an encryption key and thereby obtain unauthorized information from the mobile station 30. Thus, an improved authentication and key generation procedure is herein described, wherein the authentication and key generation procedure is implemented in one embodiment wherein the functions performed by a mobile subscriber's secure IC 32 remain the same as in the procedure illustrated in Figures 2-3, but the functions performed by the mobile equipment ME are different. Specifically, embodiments of the authentication and key generation procedure described herein can be implemented in new mobile station terminals using already deployed secure IC's 32, in order to derive keys for use in application security which are not compromised by the weaknesses of the GSM radio interface encryption.

[0024] Figure 4 is a block diagram of one embodiment of the communication network entities involved in authentication of a subscriber using distinguished authentication data. The communications network illustrated in Figure 4 comprises a mobile station 202, which is similar to the mobile station 30 of Figure 1, wherein the mobile station 202 of Figure 3 comprises the secure IC 32 which stores the secret key 38. However, mobile equipment 204 of the mobile station 202 is different from the mobile equipment 34 of the mobile station 30 of Figure 1 in that mobile equipment 204 stores distinguished or reserved authentication data in its memory, such as a distinguished random number challenge RAND 206. The mobile equipment 204 also comprises a processor 208.

[0025] The mobile equipment 204 uses the distinguished RAND 206 to generate a second set of values in addition to the set of values produced in response to a RAND received from the network as part of an authentication process. The mobile station computes a "distinguished" session key K using values produced from the challenge RAND received from the network and values produced from the distinguished RAND stored in the mobile station. The distinguished RAND has a predetermined fixed value known to the network and the mobile device. It may, for example, have an all-zero value, and is designated herein as $RAND_0$. The authentication center 42 also stores the distinguished RAND so that the network can also compute the distinguished key K. The distinguished key K can be used for a variety of purposes after it is generated, including

encrypting or keying a message authentication code in future communications, transactions, or the like. It may be used to secure communications between the mobile station 202 and a network element for applications requiring increased security, such as banking applications, over a variety of bearers such as GPRS, Bluetooth or WLAN. The distinguished RAND is reserved by the system for use in generating the distinguished key K, and is not used for initial authentication procedures, so that neither $RAND_0$ or the signed response to $RAND_0$ ($SRES_0$) are transferred over the wireless communication link.

[0026] Figures 5-6 illustrate an authentication and secure key generation process for the network entities of Figure 4, wherein Figure 5 is a flow diagram illustrating one embodiment of a method of authentication and secure key generation at the mobile station 202, and Figure 6 is a signal flow diagram illustrating one embodiment of an authentication and secure key generation process for establishing secure communication in a network.

[0027] In reference to Figure 6, the network element 40 obtains authentication data specific to the subscriber from the authentication center (AuC) 42 in the subscriber's home network. In a step 214, the authentication center 42 uses a random challenge RAND and the secret key Ki to generate one or more authentication vectors (RAND, XRES, Kc). The authentication center 42 also generates one or more distinguished authentication vectors ($RAND_0$, $XRES_0$, Kc_0) using the distinguished random challenge $RAND_0$ 206 and the secret key Ki. In a step 216, the authentication center computes a distinguished session key K using Kc, Kc_0, XRES, and $XRES_0$. In one embodiment, the distinguished key K is a hash of Kc, Kc_0, XRES, and $XRES_0$. In a step 220, the authentication center 42 sends both the authentication vector(s) and distinguished authentication vector(s) to the network element 40. With this information, the network element can also compute the distinguished key K based on the information provided by the authentication center.

[0028] As will be appreciated by those skilled in the art, the distinguished key K may be generated based on a plurality of combinations of values and is not limited to those described herein. For example, the distinguished key K may be generated based on RAND and $RAND_0$ in addition to or in place of Kc, Kc_0, XRES, and $XRES_0$. Also, a variety of variants may be used to provide the network element with the information necessary to communicate with the mobile station using the key K. The network

element 40 may directly receive the hash value forming the distinguished key K from the authentication center rather than the above described distinguished authentication vector. Alternately, the network element could keep a database of $XRES_0$ and Kc_0 for different subscriber identities (e.g. the IMSI).

[0029] Figure 4 is a signal flow diagram illustrating one embodiment of a bootstrapped method of authenticating a mobile subscriber using distinguished authentication data. Some of the procedures performed by the network elements according to the method illustrated in Figure 4 are similar to the procedures performed according to the method illustrated in Figure 2.

[0030] For authentication of the mobile station and generation of a session key, the network element 40 sends an authentication request to the mobile subscriber's mobile equipment 204 in a step 220, wherein the authentication request comprises only the random number challenge RAND, and the distinguished $RAND_0$ is not transmitted over the radio network from the network element 40 to the mobile station 202. In reference to Figure 5, the authentication and session key generation process performed at the mobile station 202 begins in step 224 in which the mobile equipment 204 receives the authentication challenge with the challenge RAND. In a step 226, the secure IC 32 computes the authentication response SRES1 and the mobile equipment 204 sends the response to the network element 40. In a step 228, the secure IC computes a first key KEY1 using the stored secret key Ki and the challenge RAND. In a step 240, the secure IC 32 computes a second key KEY2 using the distinguished challenge $RAND_0$ stored at the mobile equipment 204 and the secret key Ki stored at the secure IC 32. In a step 244, the mobile equipment 204 computes a session key K from KEY1 and KEY2. This key may be used in future communications or transactions.

[0031] The authentication and key generation process performed at the secure IC 32 and mobile equipment 204 is illustrated in more detail in reference to the network element 40 in Figure 6. Upon receipt of the random number challenge RAND, the mobile equipment 204 sends RAND to the secure IC 32 in step 224. In step 226, the secure IC generates the authentication or signed response SRES using RAND and the secret key Ki 38, and the secure IC computes the cipher key Kc in step 228 using the RAND and the secret key Ki. The secure IC 32 sends both the authentication response SRES and the cipher key Kc to the mobile equipment 204 in a step 230, and the mobile equipment 204 transmits the authentication response SRES to the network element 40 in a step 230.

The network element 40 compares the authentication response SRES from the mobile equipment 204 to the expected response XRES in the selected authentication vector in a step 234, similar to step 119 in Figure 3.

[0032] In a step 236, the mobile equipment 204 sends the distinguished random challenge $RAND_0$ 206, stored at the mobile equipment 204, to the secure IC 32, which computes a distinguished authentication response $SRES_0$ based on the distinguished $RAND_0$ in step 238, similar to step 226, using the secret key Ki. The secure IC 32 also computes the distinguished cipher key Kc_0 in step 240 using the secret key Ki. The secure IC 32 then transmits the distinguished authentication response $SRES_0$ and distinguished cipher key Kc_0 to the mobile equipment 204 in a step 242. Thus, the same secure IC used in the authentication process of Figure 3 can be used to generate the distinguished cipher key Kc_0 according to the embodiment of the invention illustrated in Figure 6.

[0033] In response to receipt of the distinguished authentication response $SRES_0$ and distinguished cipher key Kc_0, the mobile equipment 204 generates a distinguished session key K in step 244. In one embodiment, the distinguished key K is generated based on the cipher key Kc and authentication response SRES generated by the secure IC 32 in steps 226 and 228 using RAND, and the distinguished cipher key Kc_0 and distinguished authentication response $SRES_0$ generated by the secure IC 32 in steps 238 and 240 using $RAND_0$. The mobile equipment stores the distinguished key K in a step 246. With the distinguished key K stored at both the mobile equipment 204 and the network element 40, the key K can be used in future communications and transactions. In some embodiments, the mobile equipment 204 is configured to reject an authentication request including the distinguished RAND value to ensure that the signed response to the reserved RAND value is never sent over the wireless communication link and the resulting enciphering key Kc0 is not used to encrypt over the radio link.

[0034] Thus, according to the authentication and key generation process illustrated in Figures 4-6, a key K is agreed for use by applications, re-using the existing GSM SIM, Authentication Center, and interface between the mobile terminal and SIM, but the key is not exposed by security weaknesses in the GSM air interface.

[0035] In one embodiment, the mobile equipment 204 is configured to generate a distinguished authentication response DRES to replace the authentication response SRES for the authentication of the identity of the mobile station 202 to the network

element 40. For example, the mobile equipment 204 may be configured to generate a distinguished key DRES based on XRES, XRES0, Kc, Kc0. In such an embodiment the network element 40 either receives an expected distinguished authentication response DRES which is generated at the authentication center 42, or the network element 40 is configured to generate the expected distinguished response DRES based on the received parameters SRES, SRES0, Kc and Kc0. The network element 40 is further configured to compare the distinguished authentication data DRES generated by the mobile equipment 204 to the expected distinguished response for authentication of the mobile station 202.

[0036] In some embodiments, the authentication and key generation process discussed in reference to Figures 4-6 further employs a bootstrapping function in the mobile stations' home network for bootstrapping the authentication and key generation process. The bootstrapped process may be used for authentication and key generation in connection with communication sessions requiring heightened security, such as between the mobile station and an e-commerce network application function. In such embodiments, the mobile station 202 performs the authentication and key generation process in connection with the bootstrapping function instead of the network element 40, wherein the bootstrapping function receives the authentication vectors and session key K from the authentication center 42. Following authentication of the mobile station, the bootstrapping function then sends the session key K to the e-commerce network application function for encrypting communications with the mobile station.

[0037] In a communications network employing the bootstrapped process, the mobile equipment 204 may be configured to perform the authentication and key generation process with the secure IC 32 illustrated in Figures 2-3 for voice calls, wherein the cipher key Kc is used to encrypt communications with a network element. The mobile equipment 204 may further be configured to recognize a communication session type requiring increased security, such as e-commerce, and accordingly perform the authentication and key generation process with the secure IC 32 illustrated in Figures 5-6, wherein the session key K is used to encrypt communications. Regardless of the authentication and key generation process performed by the mobile equipment 204, the process performed by the secure IC 32 remains the same by receiving a random challenge and computing both a signed response and a cipher key based on the random challenge and the stored secret key Ki.

[0038] An exemplary implementation of the authentication and key generation process illustrated in Figures 4-6 is a communication session between a mobile station and a banking institution, wherein a mobile subscriber desires to exchange sensitive information with a network application and therefore desires increased communication security. In the present example, a mobile station requests communication with the bank network application function by transmitting a request to the bootstrapping function in the mobile station's home network. The bootstrapping function obtains standard (RAND, XRES, Kc) and distinguished authentication vectors ($RAND_0$, $XRES_0$, Kc_0) and a session key K from the authentication center for use in authenticating the identity of the mobile station requesting communication. The bootstrapping function sends the random challenge RAND to the mobile station's mobile equipment. The mobile equipment sends the random challenge RAND to its secure IC for computation of the response SRES and cipher key Kc. In response to receipt of the response SRES and cipher key Kc from the secure IC, the mobile equipment sends the response SRES to the bootstrapping function, which determines whether the key used to generate SRES is the same as the key used to generate the expected response XRES by comparing SRES to XRES. If the two parameters do match, the authentication of the mobile station is considered successful and the bootstrapping function sends the session key to the network application function (bank).

[0039] After sending the generated response SRES to the bootstrapping function, the mobile equipment sends the distinguished $RAND_0$, stored at the mobile equipment, to the secure IC for computation of the distinguished response $SRES_0$ and distinguished cipher key Kc_0. The mobile equipment then uses Kc, SRES, Kc_0, $SRES_0$ to compute the distinguished session key K. The mobile station and the network application function can then begin secure communications using the distinguished session key K to encrypt their communication transmissions.

[0040] As will be appreciated by those skilled in the art, the above-described systems and methods are directed to only a few specific embodiments, and the invention can be practiced in many ways. Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be

represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0041] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0042] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0043] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the

processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[0044] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

What is claimed is:

CLAIMS

1. A mobile station for communicating in a wireless communications network, comprising:

a receiver configured to receive at least one authentication data parameter from said wireless communications network;

a memory storing a fixed authentication data parameter;

a first processing circuit configured to generate a first key based on said at least one received authentication data parameter, and to generate a second key based on said fixed authentication data parameter; and

a second processing circuit configured to generate a third key using at least said first and second keys.

2. The mobile station of Claim 1, wherein said second processing circuit is configured to encrypt communication transmissions using said third key.

3. The mobile station of Claim 1, wherein the at least one received authentication data parameter comprises a random or pseudo-random number that changes for different communication sessions between said mobile station and said communications network.

4. The mobile station of Claim 3, wherein the mobile equipment is configured to reject an authentication request containing said fixed authentication data parameter.

5. The mobile station of Claim 1, wherein the first processing circuit is configured to generate an authentication response using at least one received authentication data parameter and a secret key.

6. The mobile station of Claim 5, wherein the mobile station is configured to send the authentication response over said wireless communication channel for authentication of the mobile station.

7. The mobile station of Claim 1, wherein the first processing circuit comprises a secure integrated circuit.

8. The mobile station of Claim 7, wherein the first integrated circuit comprises a subscriber identity module (SIM).

9. A mobile element of a wireless communications network, said wireless communications network comprising a plurality of mobile elements and a plurality of network elements communicating with said mobile elements, wherein said mobile element is configured to authenticate itself to said communications network by responding to a challenge value presented to the mobile element by a network element of said communications network during an authentication procedure, and wherein said mobile element comprises a memory storing a reserved challenge value that is not used to authenticate mobile elements in authentication procedures between any network element and any mobile element.

10. The mobile element of Claim 9, comprising a processing circuit configured to generate sets of one or more values in response to challenge values using at least a stored key.

11. The mobile element of Claim 10, wherein said processing circuit is configured to generate a signed response and an encryption key in response to a challenge value.

12. The mobile element of Claim 11, wherein said processing circuit comprises a subscriber identity module (SIM).

13. The mobile element of Claim 12, wherein said mobile unit is configured to communicate in a GSM communications network.

14. The mobile element of Claim 12, wherein said mobile unit is configured to communicate in a local area network.

15. A method of communication between a mobile station and a communications network element, comprising:

selecting an authentication challenge at a network element;

transmitting the authentication challenge to a mobile station;

generating a first value comprising an authentication response at the mobile station using at least the authentication challenge and a stored key;

generating a second value at the mobile equipment using at least the authentication challenge and said stored key;

generating a third value at the mobile equipment using at least a fourth value different from said authentication challenge and said stored key; and

generating a key using at least said second and third values.

16. The method of Claim 15, wherein the first authentication challenge comprises a random or pseudo-random number.

17. The method of Claim 15, comprising transmitting said authentication challenge from an authentication center to said network element.

18. The method of Claim 15, comprising transmitting said key from an authentication center to said network element.

19. The method of Claim 15, wherein said fourth value comprises a reserved authentication challenge.

20. The method of Claim 15, further comprising rejecting an authentication request at the mobile station when the authentication challenge is the same as said fourth value.

21. A method of creating keys in a communication network that uses a challenge- response authentication procedure, said method comprising reserving at least one challenge value for use in generating session keys for use in communication between mobile units and network elements within the communication network, wherein the reserved challenge value is not used for mobile unit authentication.

22. A method of generating a key at a mobile station for securing communication between said mobile station and a network element, said method comprising:

receiving an authentication challenge value from a network element at said mobile station;

sending said authentication challenge value to a processing circuit;

generating a first set of one or more values using at least said authentication challenge value;

sending at least one value from said first set to the network element for authentication;

sending a second authentication challenge value to said processing circuit;

generating a second set of one or more values using at least said second authentication challenge;

generating said key using at least one value of said first set and at least one value of said second set.

23. The method of Claim 22, wherein a value of said first set of values sent to a network element comprises a signed response (SRES).

24. The method of Claim 22, wherein one of said first set of values comprises an encryption key.

25. The method of Claim 22, wherein one of said second set of values comprises an encryption key.

26. The method of Claim 22, wherein comprising generating, with said processing circuit, a signed response and an encryption key for each authentication challenge value sent to said processing circuit.

27. The method of Claim 22, wherein the first authentication challenge is a random or pseudo-random number.

28. A mobile station in a communications network, said mobile station comprising:

means for receiving an authentication challenge value from said communications network;

means for generating a first set of values in response to said received authentication challenge;

means for generating a second set of values in response to a distinguished authentication challenge value; and

means for generating a key using at least one of said first set of values and at least one of said second set of values.

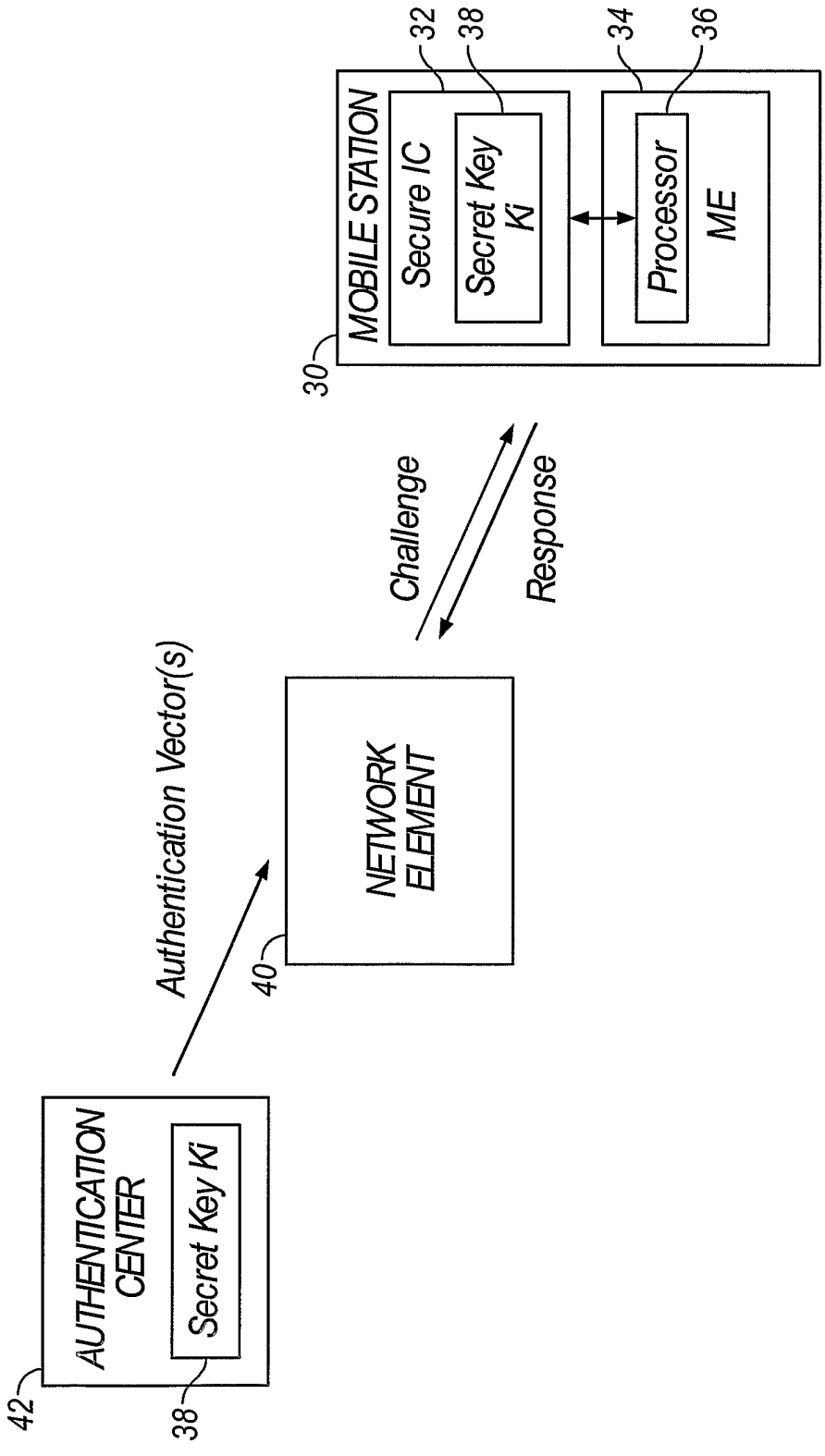

MOBILE STATION
Secure IC
Secret Key Ki
Processor ME
32
38
34
36
30
Challenge
Response
Authentication Vector(s)
NETWORK ELEMENT
40
AUTHENTICATION CENTER
Secret Key Ki
42
38

FIG. 1

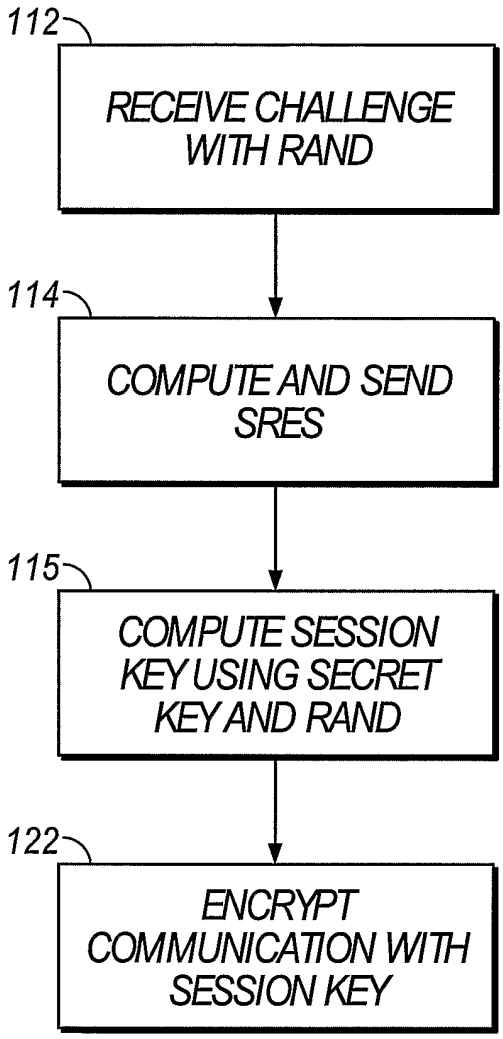

112
RECEIVE CHALLENGE WITH RAND
114
COMPUTE AND SEND SRES
115
COMPUTE SESSION KEY USING SECRET KEY AND RAND
122
ENCRYPT COMMUNICATION WITH SESSION KEY

FIG. 2

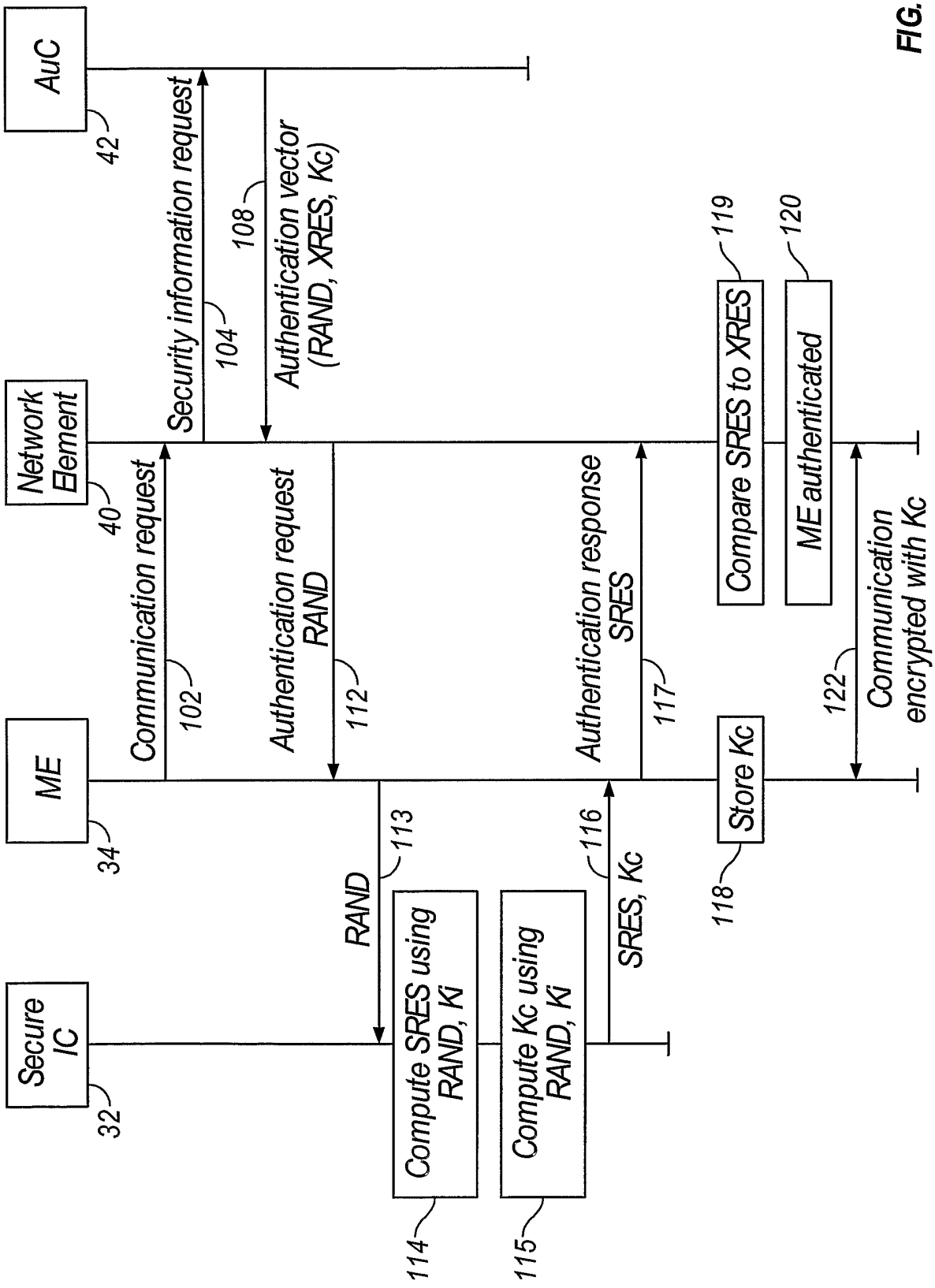

AuC
42
Network Element
40
ME
34
Secure IC
32
Security information request
104
Authentication vector (RAND, XRES, Kc)
108
Communication request
102
Authentication request RAND
112
RAND
113
Compute SRES using RAND, Ki
114
Compute Kc using RAND, Ki
115
Authentication response SRES
117
SRES, Kc
116
Compare SRES to XRES
119
ME authenticated
120
Store Kc
118
Communication encrypted with Kc
122

FIG. 3

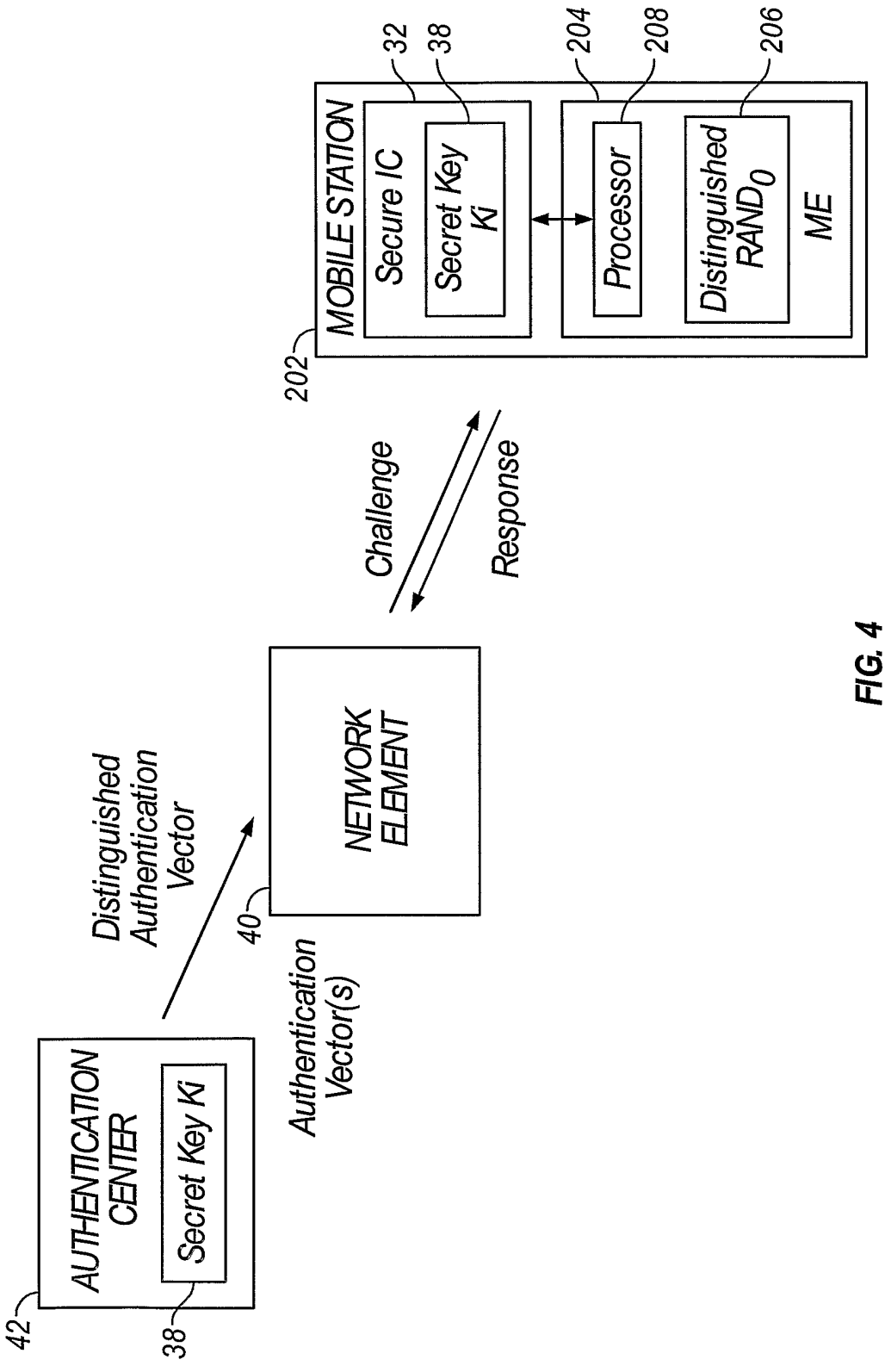

AUTHENTICATION CENTER
Secret Key Ki
42
38
Distinguished Authentication Vector
Authentication Vector(s)
NETWORK ELEMENT
40
Challenge
Response
MOBILE STATION
Secure IC
Secret Key Ki
Processor
Distinguished RAND0
ME
202
32
38
204
208
206

FIG. 4

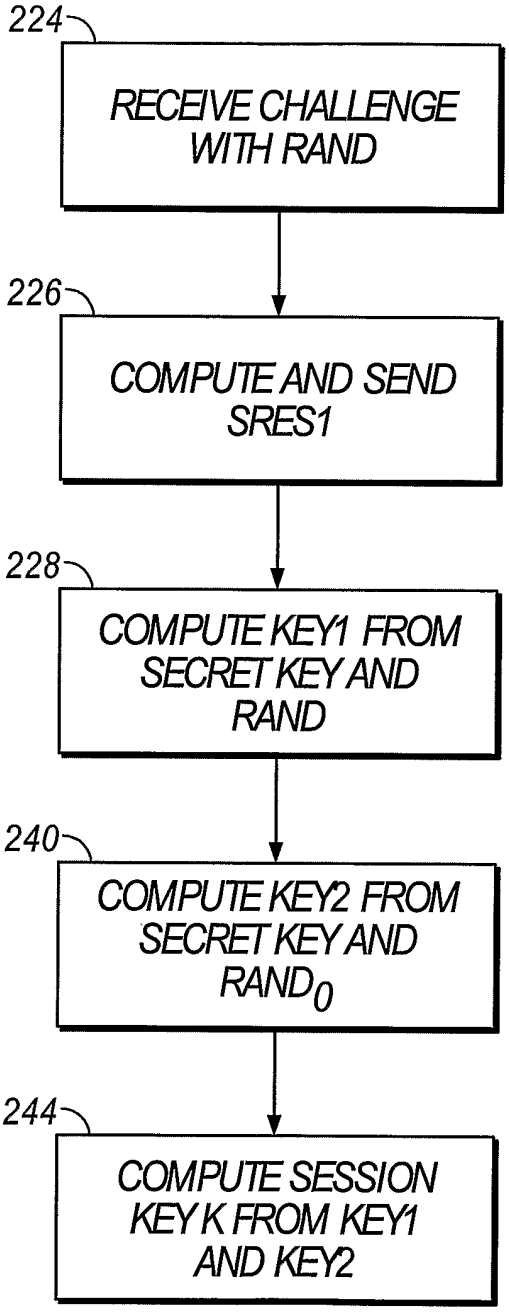

224
RECEIVE CHALLENGE WITH RAND
226
COMPUTE AND SEND SRES1
228
COMPUTE KEY1 FROM SECRET KEY AND RAND
240
COMPUTE KEY2 FROM SECRET KEY AND RAND0
244
COMPUTE SESSION KEY K FROM KEY1 AND KEY2

FIG. 5

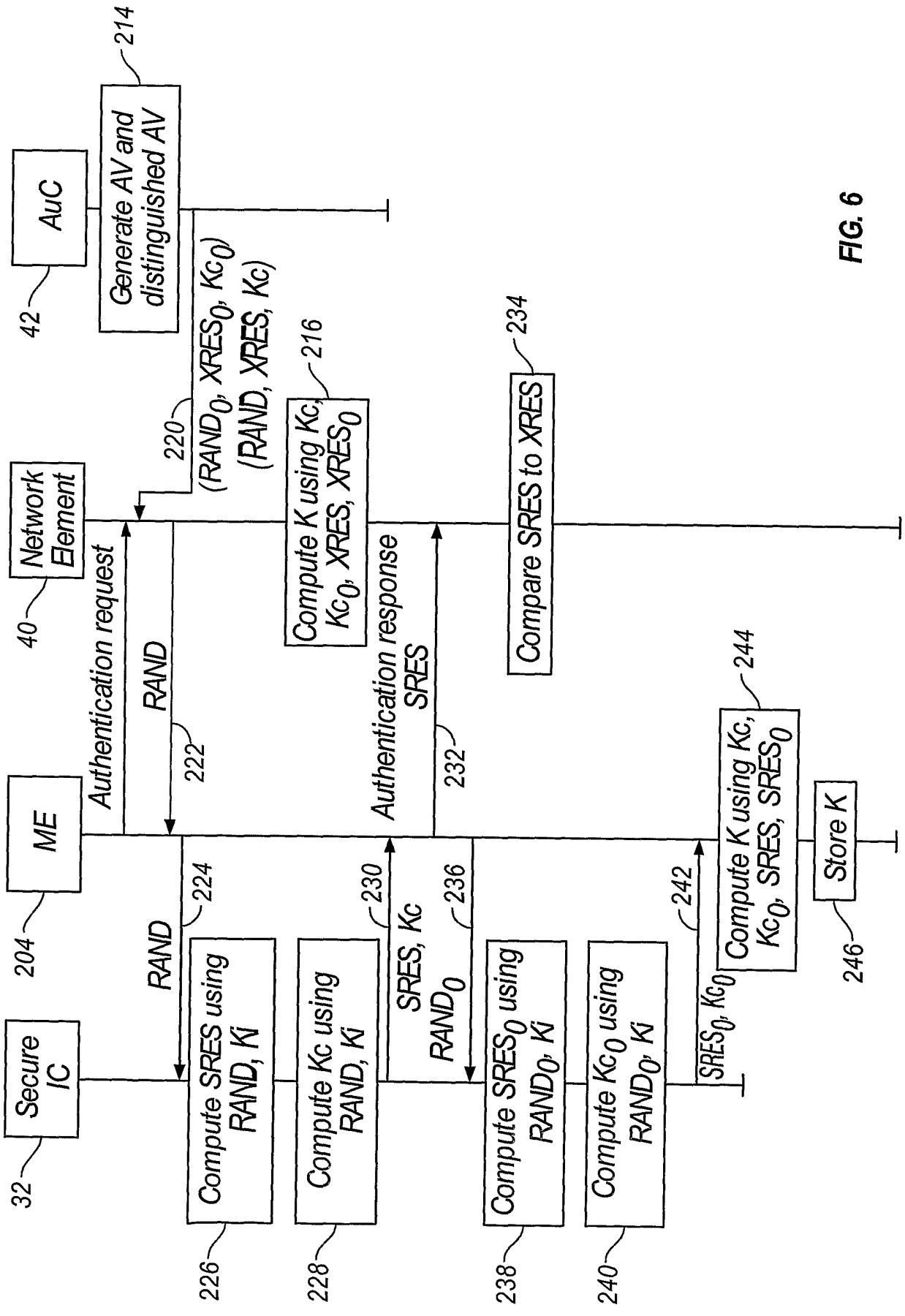

AuC
42
Generate AV and distinguished AV
214
Network Element
40
220
(RAND0, XRES0, Kc0)
(RAND, XRES, Kc)
Compute K using Kc0, XRES, XRES0
216
Compare SRES to XRES
234
ME
204
Authentication request
RAND
222
Authentication response
SRES
232
Secure IC
32
RAND
224
Compute SRES using RAND, Ki
226
Compute Kc using RAND, Ki
228
SRES, Kc
RAND0
230
236
Compute SRES0 using RAND0, Ki
238
Compute Kc0 using RAND0, Ki
240
SRES0, Kc0
242
Compute K using Kc, Kc0, SRES, SRES0
244
Store K
246

FIG. 6

INTERNATIONAL SEARCH REPORT

I · tional application No
/US2005/032337

A. CLASSIFICATION OF SUBJECT MATTER
H04Q7/32

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 101 28 300 A1 (GIESECKE & DEVRIENT GMBH) 9 January 2003 (2003-01-09) paragraph '0022! - paragraph '0032! paragraph '0040! paragraph '0042! paragraph '0048! - paragraph '0051! paragraph '0054! figure 3	1-8, 15-20, 22-28
A	US 6 711 400 B1 (AURA TUOMAS) 23 March 2004 (2004-03-23) column 5, line 21 - line 51 column 6, line 16 - column 7, line 46 figure 4	1-28

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 February 2006	16/02/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Müller, N

INTERNATIONAL SEARCH REPORT

I tional application No
/US2005/032337

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/14895 A (DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH; HAKE, JENS; THELEN, JOERG) 16 March 2000 (2000-03-16) page 2, line 6 - page 3, line 26 page 4, line 9 - line 29	1-28
A	US 5 661 806 A (NEVOUX ET AL) 26 August 1997 (1997-08-26) column 1, line 58 - column 2, line 50 column 4, line 40 - line 65 figure 2	1-28
P,X	WO 2005/048638 A (QUALCOMM INCORPORATED; ROSE, GREGORY G; PADDON, MICHAEL; HAWKES, PHILI) 26 May 2005 (2005-05-26) paragraph '0035! paragraph '0039! figures 5a,6	15-18, 22-28

INTERNATIONAL SEARCH REPORT

International application No
US2005/032337

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 10128300 A1	09-01-2003	WO 02102103 A2	19-12-2002
		EP 1400142 A2	24-03-2004
US 6711400 B1	23-03-2004	AU 6733198 A	24-11-1998
		EP 0976219 A2	02-02-2000
		FI 971620 A	17-10-1998
		WO 9849855 A2	05-11-1998
WO 0014895 A	16-03-2000	AU 1259200 A	27-03-2000
		CA 2343180 A1	16-03-2000
		DE 19840742 A1	09-03-2000
		EP 1112666 A2	04-07-2001
		PL 347024 A1	11-03-2002
		US 6934531 B1	23-08-2005
US 5661806 A	26-08-1997	EP 0675615 A1	04-10-1995
		FR 2718312 A1	06-10-1995
		JP 8008899 A	12-01-1996
WO 2005048638 A	26-05-2005	US 2005100165 A1	12-05-2005