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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2024 (28.11.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/242541 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/KR2024/095830

(22) International Filing Date:
22 May 2024 (22.05.2024)

(25) Filing Language: English

(26) Publication Language: English

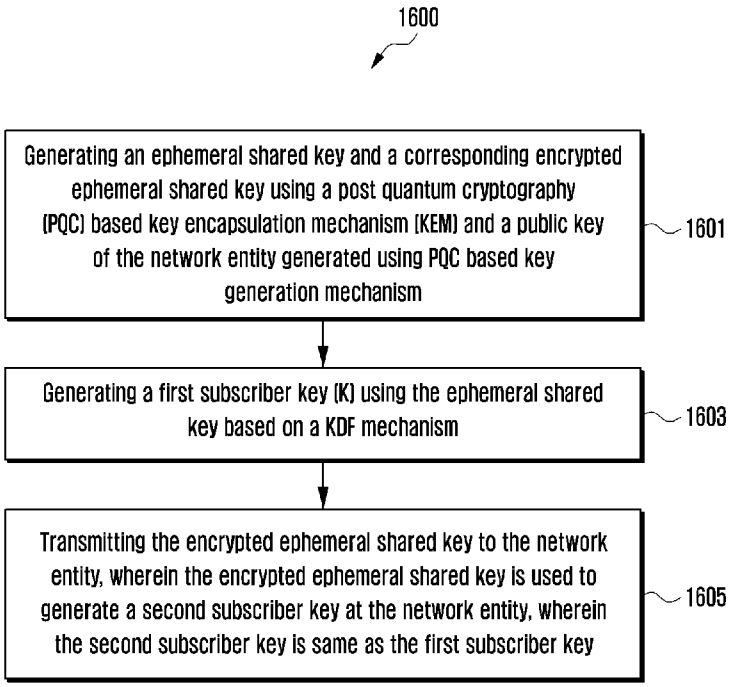
(30) Priority Data:
202341035704 23 May 2023 (23.05.2023) IN
202341035704 15 May 2024 (15.05.2024) IN

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(72) Inventors: **VUPPALA, Ramesh Chandra**; # 2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanakundi Circle, Marathahalli Post, Bangalore 560037 (IN). **SHARMA, Neha**; # 2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanakundi Circle, Marathahalli Post, Bangalore 560037 (IN). **JE, Donghyun**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR). **NIGAM, Anshuman**; # 2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanakundi Circle, Marathahalli Post, Bangalore 560037 (IN). **KIM, Dongmyung**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(74) Agent: **YOON & LEE INTERNATIONAL PATENT & LAW FIRM**; 3rd Fl, Ace Highend Tower-5, 226, Gasan Digital 1-ro, Geumcheon-gu, Seoul 08502 (KR).

(54) **Title:** METHODS AND SYSTEMS FOR PERFORMING AUTHENTICATION AND KEY AGREEMENT



(57) **Abstract:** The present disclosure relates to a 5G communication system or a 6G communication system for supporting higher data rates beyond a 4G communication system such as long term evolution (LTE). Disclosed is a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises generating (1601) an ephemeral shared key and a corresponding encrypted ephemeral shared key using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism. Further, the method comprises generating (1603) a first subscriber key (K) using the ephemeral shared key based on a KDF mechanism. Further, the method comprises transmitting (1605) the encrypted ephemeral shared key to the network entity, wherein the encrypted ephemeral shared key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key.

WO 2024/242541 A1

[Continued on next page]

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

Description

Title of Invention: METHODS AND SYSTEMS FOR PERFORMING AUTHENTICATION AND KEY AGREEMENT

Technical Field

[1] The present disclosure relates to the field of wireless communication networks, and more particularly relates to methods and systems performing authentication and key agreement (AKA) in wireless communication networks.

Background Art

[2] Considering the development of wireless communication from generation to generation, the technologies have been developed mainly for services targeting humans, such as voice calls, multimedia services, and data services. Following the commercialization of 5G (5th-generation) communication systems, it is expected that the number of connected devices will exponentially grow. Increasingly, these will be connected to communication networks. Examples of connected things may include vehicles, robots, drones, home appliances, displays, smart sensors connected to various infrastructures, construction machines, and factory equipment. Mobile devices are expected to evolve in various form-factors, such as augmented reality glasses, virtual reality headsets, and hologram devices. In order to provide various services by connecting hundreds of billions of devices and things in the 6G (6th-generation) era, there have been ongoing efforts to develop improved 6G communication systems. For these reasons, 6G communication systems are referred to as beyond-5G systems.

[3] 6G communication systems, which are expected to be commercialized around 2030, will have a peak data rate of tera (1,000 giga)-level bps and a radio latency less than 100μsec, and thus will be 50 times as fast as 5G communication systems and have the 1/10 radio latency thereof.

[4] In order to accomplish such a high data rate and an ultra-low latency, it has been considered to implement 6G communication systems in a terahertz band (for example, 95GHz to 3THz bands). It is expected that, due to severer path loss and atmospheric absorption in the terahertz bands than those in mmWave bands introduced in 5G, technologies capable of securing the signal transmission distance (that is, coverage) will become more crucial. It is necessary to develop, as major technologies for securing the coverage, radio frequency (RF) elements, antennas, novel waveforms having a better coverage than orthogonal frequency division multiplexing (OFDM), beamforming and massive multiple input multiple output (MIMO), full dimensional MIMO (FD-MIMO), array antennas, and multiantenna transmission technologies such as large-scale antennas. In addition, there has been ongoing discussion on

new technologies for improving the coverage of terahertz-band signals, such as metamaterial-based lenses and antennas, orbital angular momentum (OAM), and reconfigurable intelligent surface (RIS).

[5] Moreover, in order to improve the spectral efficiency and the overall network performances, the following technologies have been developed for 6G communication systems: a full-duplex technology for enabling an uplink transmission and a downlink transmission to simultaneously use the same frequency resource at the same time; a network technology for utilizing satellites, high-altitude platform stations (HAPS), and the like in an integrated manner; an improved network structure for supporting mobile base stations and the like and enabling network operation optimization and automation and the like; a dynamic spectrum sharing technology via collison avoidance based on a prediction of spectrum usage; an use of artificial intelligence (AI) in wireless communication for improvement of overall network operation by utilizing AI from a designing phase for developing 6G and internalizing end-to-end AI support functions; and a next-generation distributed computing technology for overcoming the limit of UE computing ability through reachable super-high-performance communication and computing resources (such as mobile edge computing (MEC), clouds, and the like) over the network. In addition, through designing new protocols to be used in 6G communication systems, developing mecahnisms for implementing a hardware-based security environment and safe use of data, and developing technologies for maintaining privacy, attempts to strengthen the connectivity between devices, optimize the network, promote softwarization of network entities, and increase the openness of wireless communications are continuing.

[6] It is expected that research and development of 6G communication systems in hyper-connectivity, including person to machine (P2M) as well as machine to machine (M2M), will allow the next hyper-connected experience. Particularly, it is expected that services such as truly immersive extended reality (XR), high-fidelity mobile hologram, and digital replica could be provided through 6G communication systems. In addition, services such as remote surgery for security and reliability enhancement, industrial automation, and emergency response will be provided through the 6G communication system such that the technologies could be applied in various fields such as industry, medical care, automobiles, and home appliances.

[7] In recent years, Fifth Generation (5G) wireless communication system has been developed to provide high-speed data services The development of 5G has revolutionized several industries, such as autonomous vehicles, healthcare, and manufacturing by enabling ultra-reliability and ultra-low-latency applications. However, the development of 5G implicates potential security vulnerabilities that threaten mobile user privacy. Said potential security vulnerabilities include lack of full

protection against compromised/impersonated home networks or serving networks (SNs). A major component of the specification associated with the standardization of 5G describes Authentication and Key Agreement (AKA) protocol in 5G, as depicted in FIG. 1.

[8] FIG. 1 is a schematic diagram 100 depicting an Authentication and Key Agreement (AKA) in 5G, in accordance with the existing art. As shown in the figure, the representation of authentication and key agreement consists of a user authentication function in the Universal Subscriber Identity Module (USIM) and a construction of Authentication String (AUTS) parameters at a user equipment (UE). A static subscriber long term key K is provisioned to the UE during the SIM provisioning and the random number (RAND) is shared with the UE by the network during the AKA procedure. Further, all the authentication vectors are generated at the UE using K and RAND values.

[9] In 5G AKA provides user identity protection using public-key cryptography, i.e., Elliptical curve based integrated encryption scheme (ECIES). In an implementation of ECIES as depicted in FIG. 2, firstly elliptical curve based ephemeral key generation happens at a user equipment (UE) and home network (HN). HN public key is configured at SIM provisioning. Ephemeral UE private key and HN public key are used to generate ephemeral shared key at UE.

[10] However, 3rd Generation Partnership Project (3GPP) standards do not mention any specific authentication and key agreement methodology for 5G, beyond 5G, and/ or sixth generation (6G) wireless communication system to protect against threats posed by quantum machines. With the rise in research and development of quantum machines, currently used cryptography techniques such as ECIES may not remain efficient. In a scenario an attacker (i.e., an eavesdropper) may use quantum machine to launch resource intensive attack could recover a static subscriber long-term key.

[11] Recovery of the static subscriber long-term key would allow the attacker to pose as the subscriber to the home network or the serving network. The attacker can combine the recovered static subscriber long-term key with random number (RAND) and use key derivation functions (KDF) to generate Ciphering Key (CK), Integrity Key (IK). Consequently, complete key hierarchy gets compromised, since all the authentication vectors are generated from the subscriber long-term key as depicted in FIG. 3.

[12] FIG. 3 is a schematic diagram 300 depicting an exemplary representation of the key hierarchy in the 5G wireless communication system and the generation of the authentication vectors at the network, in accordance with the existing art. As shown in the figure, K is the long-term subscriber key or Universal Subscriber Identity Module (USIM) individual key, which is provided to the UE during Subscriber Identity Module (SIM)/Universal Integrated Circuit Card (UICC) provisioning. All keys for

access security and core network security entities derive from this long-term subscriber key 'K'. A random number (RAND) is generated for providing different authentication vectors for every session between the UE and the network. The authentication vectors include a cipher key, integrity key, anonymity key, expected response (XRES), and a Message Authentication Code (MAC).

[13] Thus, the attacker is enabled to launch fake base stations to communicate with UE compromising user location, privacy and all communication between UE and HN. The attacker would need to use resource intensive attack to recover the static subscriber long-term key. Thereafter, the attacker would be required to know parameters related to the home network or the serving network, to model a key derivation algorithm and the inputs to the KDF in the key hierarchy. The attacker may leverage quantum machines to recover the key hierarchy. Further, with the leverage of quantum machines and complete hierarchy, the attacker would be able to decrypt all traffic belonging to that subscriber which was not encrypted at the application layer. Moreover, recovery of the subscriber long-term key would also allow the attacker to pose as the subscriber to the network.

[14] Further, in the 6G wireless communication systems, quantum machines are widely used which is a threat to current wireless security systems. The quantum machines make use of quantum-mechanical effects which allows quantum bits (qubits) to exist in a combination of several states at once, and entanglement, which further allows connections between separate quantum systems such that they cannot be described independently. There exist quantum algorithms that use the quantum-mechanical effects to solve certain cryptographic problems more efficiently than they may be solved on a classical computer. Shor's quantum algorithm for integer factorization runs in polynomial time on a quantum computer. A variant of Shor's algorithm enables a quantum computer to calculate discrete logarithms in polynomial time, both over finite fields and elliptic curves. The variant of Shor's algorithm renders several other public-key cryptosystems insecure, including Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH).

[15] Further, the generated RAND is shared in an unencrypted form over the air in authentication request message from network to UE, as shown in FIG. 4. FIG. 4 is a schematic diagram 400 depicting AKA procedure between the network and the UE, in accordance with the existing art. As shown in the figure, Security Anchor Function (SEAF), Authentication Server Function (AUSF), and Unified Data Management (UDM) are network functions that are involved in the AKA procedure. Further, as depicted in the figure, the RAND is generated at step 1, and is shared unencrypted with the UE in the authentication request message at step 6.

[16] Furthermore, FIG. 5 is a schematic diagram 500 depicting a sequence flow diagram of the Authentication and Key Agreement (AKA) procedure highlighting unprotected authentication request messages, in accordance with existing art. During the AKA procedure at present, authentication parameters like RAND, AUTN (Authentication Token), and like are shared with the UE via the authentication request message. This authentication request message is shared via an unsecured channel to the UE as Non-Access Stratum (NAS) and Access Stratum (AS) security context is not yet established between the UE and the network. The attacker may easily read the authentication parameters and use them in quantum circuit modelling as per 3GPP 33.841 and try to decode the USIM individual key or the long term key to generate authenticate vectors.

[17] Recovery of the long term key may also make the attacker to derive all the keys in the hierarchy using key derivation functions. Attacker can create a false base station and communicate with the UE. Thereafter, all privacy and sensitive information from the user, for example, location information, user identity, and others is compromised.

[18] The recovery of the long term key may also allow the attacker to pose as the subscriber to the network. Attackers may also perform spoofing, Denial of service (DoS), Distributed denial of service (DDoS), and replay attacks on the network.

[19] Therefore, there lies a need to address the above-described limitations and provide a methodology to counter the threats of quantum computing to asymmetric cryptography to secure the AKA procedures.

Disclosure of Invention

Technical Problem

[20] The purpose of this application is to be able to solve at least one of the drawbacks of the prior art. There is a need to provide a methodology to counter the threats of quantum computing to asymmetric cryptography to secure the authentication and key agreement (AKA) procedures.

Solution to Problem

[21] In an embodiment, the present disclosure refers to a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises generating an ephemeral shared key and a corresponding encrypted ephemeral shared key using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism, generating a first subscriber key (K) using the ephemeral shared key based on a KDF mechanism, and transmitting the encrypted ephemeral shared key to the network entity, wherein the encrypted ephemeral shared key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key.

[22] In an embodiment, the present disclosure refers to a method at a network entity in communication with a UE for authentication and key agreement. The method comprises receiving the encrypted ephemeral shared key from the UE, wherein the encrypted ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism, decrypting (1609) the received encrypted ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using the PQC based key generation mechanism, to obtain the decrypted ephemeral shared key, and generating (1611) a second subscriber key (K) using the ephemeral shared key based on a KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[23] In an embodiment, the present disclosure refers to a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises generating an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism, generating a first ephemeral key (s1) using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method, generating a second ephemeral shared key (s2) and a corresponding encrypted second ephemeral shared key using the post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and the public key of the network entity generated using PQC based key generation mechanism, combining the first ephemeral key (s1) and the second ephemeral shared key (s2) to generate a first hybrid ephemeral shared key, generating a first subscriber key (K) using the first hybrid ephemeral shared key based on a KDF mechanism, and transmitting the ephemeral public key and the encrypted second ephemeral shared key to the network entity, wherein the ephemeral public key and the encrypted second ephemeral shared key are used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key.

[24] In an embodiment, the present disclosure refers to a method at a network entity in communication with a UE for authentication and key agreement. The method comprises receiving the ephemeral public key and the encrypted second ephemeral shared key from the UE, wherein the ephemeral public key is generated using an elliptical curve (EC) based key generation mechanism, wherein the encrypted second ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and the public key of the network entity generated using PQC based key generation mechanism; generating a first ephemeral key (s1) using the ephemeral public key received from UE and the ephemeral private key generated at the HN based on a predetermined key agreement method; decrypting

the received encrypted second ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using PQC based key generation mechanism, to obtain the decrypted second ephemeral shared key (s2); combining the generated first ephemeral key (s1) and the decrypted second ephemeral shared key (s2) to generate a second hybrid ephemeral shared key, wherein the second hybrid ephemeral shared key is same as the first hybrid ephemeral shared key; and generating a second subscriber key (K) using the second hybrid ephemeral shared key based on the KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[25] In an embodiment, the present disclosure refers to a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises generating an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism; generating an ephemeral shared key using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method; generating a first subscriber key (K) based on the ephemeral shared key using a predefined KDF mechanism; and transmitting the ephemeral public key generated at the UE to the network entity, wherein the ephemeral public key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key.

[26] In an embodiment, the present disclosure refers to a method at a network entity, comprising a public key and a private key, in communication with a UE for authentication and key agreement. The method comprises receiving the ephemeral public key from the UE, wherein the ephemeral public key is generated using an elliptical curve (EC) based key generation mechanism, generating an ephemeral shared key using a private key of the network entity and the ephemeral public key of the UE using the predetermined key agreement method, and generating a second subscriber key (K) based on the ephemeral shared key using the predefined KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[27] In an embodiment, the present disclosure refers to a method at a network entity in communication with a UE for authentication and key agreement. The method comprises generating an authentication parameter using a predetermined technique; encrypting the authentication parameter using a private key of the network entity based on a PQC based encryption technique; signing the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature to generate a digitally signed encrypted authentication parameter and transmitting the digitally signed encrypted authentication parameter to a user equipment (UE), wherein the digitally signed encrypted authentication parameter is verified and decrypted at the UE.

[28] In an embodiment, the present disclosure refers to a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises obtaining the digitally signed encrypted authentication parameter, wherein the digitally signed encrypted authentication parameter is generated by encrypting authentication parameter using a private key of the network entity based on a PQC based encryption technique, wherein the digitally signed encrypted authentication parameter is further generated by signing the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature; and decrypting, upon verifying the digital signature, the encrypted authentication parameter using a public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique.

[29] In an embodiment, the present disclosure refers to a method at a network entity in communication with a UE for authentication and key agreement. The method comprises generating an ephemeral shared key using a key generation mechanism; generating an ephemeral encryption key from an ephemeral shared key using a key derivation function; generating an authentication parameter using a predetermined technique; encrypting the authentication parameter using the ephemeral encryption key using a symmetric encryption technique; and transmitting the encrypted authentication parameter to a user equipment (UE), wherein the encrypted authentication parameter is decrypted at the UE.

[30] In an embodiment, the present disclosure refers to a method at a user equipment (UE) in communication with a network entity for performing authentication and key agreement. The method comprises obtaining the encrypted authentication parameter in an authentication request message, wherein the encrypted authentication parameter is generated at the network entity by encrypting an authentication parameter using an ephemeral encryption key using a symmetric encryption technique; generating an ephemeral decryption key corresponding to the ephemeral encryption key generated at the network entity using the key generation mechanism; and decrypting the authentication parameter using the ephemeral decryption key using a symmetric decryption technique corresponding to the symmetric encryption technique.

[31] In an embodiment, the present disclosure refers to a user equipment (UE) and a network entity configured to perform the methods as described in the present disclosure.

Advantageous Effects of Invention

[32] Embodiments of the present disclosure provides methods and apparatus for securely performing authentication and key agreement procedure to prevent various attacks on the network.

Brief Description of Drawings

[33] These and other features, aspects, and advantages of the present disclosure will become better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

[34] FIG. 1 is a schematic diagram depicting an Authentication and Key Agreement (AKA) in 5G, in accordance with the existing art;

[35] FIG. 2 illustrates an exemplary implementation Elliptical curve based integrated encryption scheme, in accordance with existing art;

[36] FIG. 3 is a schematic diagram depicting an exemplary representation of the key hierarchy in the 5G wireless communication system and the generation of the authentication vectors at the network, in accordance with the existing art;

[37] FIG. 4 is a schematic diagram depicting AKA procedure between the network and the UE, in accordance with the existing art;

[38] FIG. 5 is a schematic diagram depicting a sequence flow diagram of the Authentication and Key Agreement (AKA) procedure highlighting unprotected authentication request messages, in accordance with existing art;

[39] FIG. 6 is a block diagram depicting an exemplary system for performing authentication and key agreement (AKA), in accordance with one or more embodiments of the present disclosure;

[40] FIG. 7 is a schematic diagram depicting a part of registration request from UE 601 to HN 603 using PQC-KEM, in accordance with one or more embodiments of the present disclosure;

[41] FIG. 8 is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on PQC KEM based ephemeral shared key, in accordance with one or more embodiments of the present disclosure;

[42] FIG. 9a is a schematic diagram depicting an exemplary implementation of the system for performing AKA based on hybrid ephemeral shared key at UE side, in accordance with one or more embodiments of the present disclosure;

[43] FIG. 9b is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on hybrid ephemeral shared key at HN side, in accordance with one or more embodiments of the present disclosure;

[44] FIG. 10a is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on EC based ephemeral shared key at UE side, in accordance with one or more embodiments of the present disclosure;

[45] FIG. 10b is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on EC based ephemeral shared key at HN side, in accordance with one or more embodiments of the present disclosure;

[46] FIG. 11a is a schematic diagram depicting an exemplary impact of using ephemeral shared key instead of static subscriber key on key generation at HN side, according to embodiments of the present disclosure;

[47] FIG. 11b is a schematic diagram depicting an exemplary impact of using ephemeral shared key instead of static subscriber key on key generation at UE side, according to embodiments of the present disclosure;

[48] FIG. 12a is a schematic diagram depicting encryption of authentication parameters using ephemeral shared key at HN side, in accordance with one or more embodiments of the present disclosure;

[49] FIG. 12b is a schematic diagram depicting decryption of authentication parameters using ephemeral shared key at UE side, in accordance with one or more embodiments of the present disclosure;

[50] FIG. 13 is a schematic diagram depicting an impact of using encrypted authentication parameters in AKA, in accordance with one or more embodiments of the present disclosure;

[51] FIG. 14a is a schematic diagram depicting authentication parameters encryption at HN side, in accordance with one or more embodiments of the present disclosure;

[52] FIG. 14b is a schematic diagram depicting authentication parameters encryption at UE side, in accordance with one or more embodiments of the present disclosure;

[53] FIG. 15 is a schematic diagram depicting an impact of using authentication parameters encryption in AKA, in accordance with one or more embodiments of the present disclosure;

[54] FIGS. 16a-16b are flow diagrams depicting a method for performing AKA, according to an embodiment of the present disclosure;

[55] FIGS. 17a-17b are flow diagrams depicting another method for performing AKA, according to an embodiment of the present disclosure;

[56] FIGS. 18a-18b are flow diagrams depicting another method for performing AKA, according to an embodiment of the present disclosure;

[57] FIGS. 19a-19b are flow diagrams depicting another method for performing AKA, according to an embodiment of the present disclosure; and

[58] FIGS. 20a-20b are flow diagrams depicting another method for performing AKA, according to an embodiment of the present disclosure.

[59] Further, skilled artisans will appreciate that those elements in the drawings are illustrated for simplicity and may not have necessarily been drawn to scale. For example, the flow charts illustrate the method in terms of the most prominent steps

involved to help to improve understanding of aspects of the present invention. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

Mode for the Invention

[60] It will be understood by those skilled in the art that the foregoing general description and the following detailed description are explanatory of the disclosure and are not intended to be restrictive thereof.

[61] Reference throughout this specification to "an aspect", "another aspect" or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. Thus, appearances of the phrase "in an embodiment", "in another embodiment", "in one embodiment", and similar language throughout this specification may but do not necessarily, all refer to the same embodiment.

[62] The terms "comprises", "comprising", "includes", "comprise", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a process or method that comprises a list of steps does not include only those steps but may include other steps not expressly listed or inherent to such process or method.

[63] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skilled in the art to which this disclosure belongs. The system, method, and examples provided herein are illustrative only and not intended to be limiting.

[64] Embodiments of the present invention will be described below in detail with reference to the accompanying drawings.

[65] The embodiments disclosed herein describe the methods and systems for performing authentication and key agreement.

[66] Embodiments disclosed herein relate to techniques for securing the authentication and key agreement (AKA) procedure from quantum machines in both the 5G and the 6G wireless communication systems. Embodiments herein define a mechanism for preserving forward secrecy in generating key hierarchy in both the 5G and the 6G wireless communication systems. Embodiments herein further define a mechanism for utilizing shared key generated from crypto algorithms to replace the long term key. Embodiments disclosed herein further define a mechanism for utilizing shared key generated from crypto algorithms to secure random numbers generated during the

AKA procedure. The crypto algorithm as disclosed herein refers to either legacy crypto algorithms, post quantum cryptography algorithms, or any hybrid algorithm. In an exemplary embodiment, the post quantum cryptography algorithms are preferred over other crypto algorithms. The post quantum cryptography algorithms are safe against quantum attacks and offer fast key generation mechanism.

[67] The currently used authentication and key agreement procedures use the same long term key (K) for generating authentication vectors throughout multiple sessions for each subscriber. Technical specification (TS) 33.841 in 3GPP standard states that quantum circuit modelling can be performed by an attacker using quantum machines and can recover the subscriber's long term key. Recovery of the long term key also makes the attacker to derive all the keys in the hierarchy using key derivation functions. The attacker may create false base stations and communicate with the UE. Thereafter all privacy and sensitive information from the user for example, location information, user identity, or like gets compromised.

[68] Moreover, the attacker may also pose as the subscriber to the network. The attacker can also perform spoofing, Denial of service (DoS), Distributed denial of service (DDoS), and replay attacks on the network. Preserving the forward secrecy with post quantum security in the 6G wireless communication system mitigates such kinds of attacks as keys keep on changing for each session.

[69] Forward secrecy is a feature of a specific key agreement that gives assurance that shared keys will not be compromised even if a private key or long-term secrets used in the shared key exchange are compromised. Forward secrecy may be achieved by generating ephemeral public and private session keys for each session. Therefore, even if an attacker or adversary hacks any private key (for example, the most recent private key), only a minimal amount of sensitive data is exposed which is valid for only that particular session for which the key is hacked and keeping past communications secure.

[70] FIG. 6 is a block diagram depicting an exemplary system 600 for performing authentication and key agreement (AKA), in accordance with one or more embodiments of the present disclosure. The system 600 comprises a user equipment (UE) 601, and a network entity 603 communicatively coupled with each other over a network 611. According to embodiments of the present disclosure, the network entity 603 may be associated with a home network (HN). The network entity 603 includes a processor 605, a memory 607, and a communication unit 609.

[71] In an example, the processor 605 may be a single processing unit or a number of units, all of which could include multiple computing units. The processor 605 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, logical processors, virtual

processors, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the processor 605 is configured to fetch and execute computer-readable instructions and data stored in memory 607.

[72] The memory 607 may include any non-transitory computer-readable medium known in the art including, for example, volatile memory or Random Access Memory (RAM), such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read-only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes.

[73] The communication unit 609 may be configured to provide network connectivity and enable communication with coupled devices such as the UE 601. The network connectivity may be provided via a wireless connection or a wired connection. For example, the network connectivity may be provided via cellular technology, such as, 5G, beyond 5G, or 6G.

[74] The functions of the processing unit 613, the memory unit 615, and the network interface 617 are analogous to the functions of the processor 605, the memory 607, and the communication unit 609, and are not described here again for the sake of brevity.

[75] Further, each of the UE 601 and the network entity 603 may be configured to perform AKA in one or more possible manners as described in greater detail in the foregoing paragraphs.

[76] According to the embodiments of the present disclosure, the system 600 may utilize post quantum cryptography (PQC) key encapsulation mechanism (KEM) based shared key generation instead of conventional ECIES.

[77] FIG. 7 is a schematic diagram 700 depicting a part of registration request from UE 601 to HN 603 using PQC-KEM, in accordance with one or more embodiments of the present disclosure. Firstly, PQC based key generation happens at HN. PQC HN public key may be configured at SIM provisioning. Further, a random number may be used, and ephemeral shared key may be generated using PQC KEM. Finally, the ephemeral shared key may be encrypted using PQC HN Public key to generate encrypted shared key and sent to HN in registration request. Thereafter, the network entity HN may receive the encrypted shared key and decrypt the received encrypted shared key using PQC HN private key to derive the same ephemeral shared key as UE.

[78] In an implementation of the system may be configured to perform AKA based on PQC KEM based ephemeral shared key, as depicted in FIG. 8.

[79] FIG. 8 is a schematic diagram 800 depicting an exemplary implementation of the system 600 for performing AKA based on PQC KEM based ephemeral shared key, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the UE 601 in communication with a network entity 603 may be configured

to generate an ephemeral shared key and a corresponding encrypted ephemeral shared key using the post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity 603 generated using PQC based key generation mechanism. Further, the UE 601 may be configured to generate a first subscriber key (K) using the ephemeral shared key based on a predefined KDF mechanism and transmit the encrypted ephemeral shared key to the network entity 603.

[80] Further, the network entity 603 may be configured to receive the encrypted ephemeral shared key from the UE 601 and decrypt the received encrypted ephemeral shared key using the PQC-KEM and a private key of the network entity 603, generated using PQC based key generation mechanism, to obtain the decrypted ephemeral shared key. According to the embodiments of the present disclosure, the public key, and the private key of the network entity 603 may generated using PQC based key generation mechanism. Finally, the network entity 603 may be configured to generate a second subscriber key (K) using the ephemeral shared key based on the predefined KDF mechanism such that the second subscriber key is same as the first subscriber key.

[81] Consequent to the above-described mechanism for performing AKA, the subscriber key in the network entity may be derived from the PQC based ephemeral key created from PQC KEM and using private key of HN. According to the embodiments of the present disclosure, the subscriber key may be an ephemeral key generated for each user session. Further, the subscriber key in the UE may be derived from the PQC based ephemeral key created from PQC KEM and using public key of HN. According to the embodiments of the present disclosure, the subscriber key may be the ephemeral key generated for each user session. Since the PQC based ephemeral shared key are be generated for each session using public key of HN, the need to store a large number of long-term keys in the HN (for example, in Unified Data Management (UDM)) is eliminated, thereby reducing operational risks in the life cycle of key management.

[82] In another implementation of the system may be configured to perform AKA based on hybrid ephemeral shared key, as depicted in FIG. 9a and 9b.

[83] FIG. 9a is a schematic diagram 900 depicting an exemplary implementation of the system 600 for performing AKA based on hybrid ephemeral shared key at UE side, in accordance with one or more embodiments of the present disclosure. According to embodiments of the present disclosure, the hybrid ephemeral key may be obtained using a combination of elliptical curve (EC) based key generation mechanism, and PQC KEM.

[84] As depicted in the figure, the UE 601 in communication with a network entity 603 may be configured to generate an ephemeral public key and an ephemeral private key using an EC based key generation mechanism. Further, the UE 601 may be configured to generate a first ephemeral key (s1) using a public key of the network entity and the

ephemeral private key generated at the UE based on a predetermined key agreement method. In an embodiment, the public key of the network entity 603 may be generated using PQC based key generation mechanism.

[85] Further, the UE 601 may be configured to generate a second ephemeral shared key (s2) and a corresponding encrypted second ephemeral shared key using the PQC KEM, and the public key of the network entity generated using PQC based key generation mechanism. Furthermore, the UE 601 may be configured to combine the first ephemeral key (s1) and the second ephemeral shared key (s2) to generate a first hybrid ephemeral shared key and generate a first subscriber key (K) using the first hybrid ephemeral shared key based on a predefined KDF mechanism. Moreover, the UE 601 may be configured to transmit the ephemeral public key and the encrypted second ephemeral shared key to the network entity.

[86] FIG. 9b is a schematic diagram 900 depicting an exemplary implementation of the system 600 for performing AKA based on hybrid ephemeral shared key at HN side, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the network entity 603 may be configured to receive the ephemeral public key and the encrypted second ephemeral shared key from the UE 601 and generate the first ephemeral key (s1) using the ephemeral public key received from UE and the ephemeral private key generated at the HN based on a predetermined key agreement method. Further, the network entity 603 may be configured to decrypt the received encrypted second ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using PQC based key generation mechanism, to obtain the decrypted second ephemeral shared key (s2). In an embodiment, the private key of the network entity 603 may be generated using PQC based key generation mechanism.

[87] Further, the network entity 603 may combine the generated first ephemeral key (s1) and the decrypted second ephemeral shared key (s2) to generate a second hybrid ephemeral shared key, wherein the second hybrid ephemeral shared key is same as the first hybrid ephemeral shared key. Upon generating the second hybrid ephemeral shared key, the network entity 60 may be configured to generate a second subscriber key (K) using the second hybrid ephemeral shared key based on the predefined KDF mechanism, such that the second subscriber key is same as the first subscriber key.

[88] Consequent to the above-described mechanism for performing AKA, the subscriber key in the network entity may be derived from the hybrid shared key based on elliptical shared key and post quantum shared key using private key of HN. According to the embodiments of the present disclosure, the subscriber key may be an ephemeral key generated for each user session. Further, the subscriber key in the UE may be derived from the Hybrid shared key based on elliptical shared key and post quantum shared key using public key of HN. According to the embodiments of the present

disclosure, the subscriber key may be the ephemeral key generated for each user session.

[89] In yet another implementation of the system may be configured to perform AKA based on EC based ephemeral shared key, as depicted in FIGS. 10a and 10b.

[90] FIG. 10a is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on EC based ephemeral shared key at UE side, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the UE may be configured to generate an ephemeral public key and an ephemeral private key using the EC based key generation mechanism. Further, the UE 601 may be configured to generate an ephemeral shared key using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method. Furthermore, the UE 601 may be configured to generate a first subscriber key (K) based on the ephemeral shared key using a predefined KDF mechanism, and transmit the ephemeral public key generated at the UE to the network entity.

[91] FIG. 10b is a schematic diagram depicting an exemplary implementation of the system 600 for performing AKA based on EC based ephemeral shared key at HN side, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the network entity may be configured to receive the ephemeral public key from the UE, and generate an ephemeral shared key using a private key of the network entity and the ephemeral public key of the UE using the predetermined key agreement method. Further, the network entity may be configured to generate a second subscriber key (K) based on the ephemeral shared key using the predefined KDF mechanism, such that the second subscriber key is same as the first subscriber key.

[92] Consequent to the above-described mechanism for performing AKA, the subscriber key in the network entity may be derived from the elliptical shared key created from elliptical cryptography algorithms and using private key of HN. According to the embodiments of the present disclosure, the subscriber key may be an ephemeral key generated for each user session. Further, the subscriber key in the UE may be derived from the elliptical shared key created from elliptical cryptography algorithms and using public key of HN. According to the embodiments of the present disclosure, the subscriber key may be the ephemeral key generated for each user session.

[93] FIG. 11a is a schematic diagram depicting an exemplary impact of using ephemeral shared key instead of static subscriber key on key generation at HN side, according to embodiments of the present disclosure. FIG. 11b is a schematic diagram depicting an exemplary impact of using ephemeral shared key instead of static subscriber key on key generation at UE side, according to embodiments of the present disclosure. As depicted in the figure, the static subscriber key has been replaced with ephemeral

key generated for each new session. Therefore, since the long-term subscriber key is generated for each new session, the need for generation of RAND value is eliminated. Therefore, no RAND value is shared from the network entity to the UE during AKA.

[94] In addition to using at least one of the PQC KEM based ephemeral shared key, the hybrid ephemeral shared key, and the EC based ephemeral shared key, the system 600 may be configured to use authentication parameters for performing AKA, as described below in conjunction with FIGS. 12a - 14.

[95] FIG. 12a is a schematic diagram depicting encryption of authentication parameters using ephemeral shared key at the HN side, in accordance with one or more embodiments of the present disclosure. FIG. 12b is a schematic diagram depicting decryption of authentication parameters using ephemeral shared key at the UE side, in accordance with one or more embodiments of the present disclosure. As depicted in the Figure 12a, the network entity 603 may be configured to generate an ephemeral shared key using a predetermined key generation mechanism and generate an ephemeral encryption key from the ephemeral shared key using a predefined key derivation function. Further, the network entity 603 may be configured to generate an authentication parameter using a predetermined technique. Furthermore, the network entity may be configured to combine the encrypted authentication parameter with a MAC-tag value and transmit the encrypted authentication parameter, combined with a MAC-tag value, to the UE.

[96] In an embodiment, the authentication parameter is a random number (RAND) and/ or an authentication number (AUTN). In an embodiment, the random number is generated using predetermined number generation technique or by a quantum random number generator (QRNG).

[97] In an embodiment, the key generation mechanism comprises of at least one of the elliptical curve (EC) based key generation mechanism, and a post quantum cryptography (PQC) based key encapsulation mechanism (KEM). In an embodiment, the public key and the private key of the network entity are generated using PQC based key generation mechanism.

[98] As depicted in FIG. 12b, the UE may be configured to obtain the encrypted authentication parameter in an authentication request message, generate an ephemeral decryption key corresponding to the ephemeral encryption key generated at the network entity using the key generation mechanism, and decrypt the authentication parameter using the ephemeral decryption key using a symmetric decryption technique corresponding to the symmetric encryption technique.

[99] FIG. 13 is a schematic diagram 1300 depicting an impact of using encrypted authentication parameters in AKA, in accordance with one or more embodiments of the present disclosure. Consequent to using encrypted authentication parameters

in AKA, the UDM shall subsequently send this transformed authentication vector AV' (Encrypted RAND, Encrypted AUTN, Mac-tag value, XRES, CK', IK') to the AUSF from which it received the Nudm_UEAuthentication_Get Request together with an indication that the AV' is to be used for EAP-AKA' using a Nudm_UEAuthentication_Get Response message. Further, the SEAF shall transparently forward the EAP-Request/AKA'-Challenge message to the UE in a NAS message Authentication Request message. The ME shall forward the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM. Mac-tag value is verified upon reception of encrypted RAND and/or AUTN by the UE. USIM/ ME will decrypt the RAND and/or AUTN value upon reception from network using PQC/Hybrid/EC based key encapsulation algorithm.

[100] Moreover, synchronisation failure indication by UE to network is trigged by UE to network if decryption of RAND and/or AUTN is failed, or verification failure of MAC-tag value occurs.

[101] In yet another implementation, the system 600 may be configured to encrypt the authentication parameters using PQC based encryption and then digitally signing the encrypted the authentication parameters using PQC based digitally signature.

[102] FIG. 14a is a schematic diagram depicting authentication parameters encryption at HN side, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the network entity may be configured to generate an authentication parameter using a predetermined technique and encrypt the authentication parameter using a private key of the network entity based on PQC based encryption technique. According to embodiments of the present disclosure, the authentication parameter is a random number (RAND) and/or an authentication number (AUTN). According to embodiments of the present disclosure, the public key and the private key of the network entity are generated using PQC key generation mechanism. Further, the network entity may be configured to sign the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature to generate a digitally signed encrypted authentication parameter and transmit the digitally signed encrypted authentication parameter to the UE.

[103] FIG. 14b is a schematic diagram depicting authentication parameters encryption at UE side, in accordance with one or more embodiments of the present disclosure. As depicted in the figure, the UE may be configured to obtain the digitally signed encrypted authentication parameter, and decrypt, upon verifying the digital signature, the encrypted authentication parameter using a public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique.

[104] FIG. 15 is a schematic diagram 1500 depicting an impact of using authentication parameters encryption in AKA, in accordance with one or more embodiments of the present disclosure. Consequent to using encrypted authentication parameters in AKA, Consequent to using encrypted authentication parameters in AKA. Further, the SEAF shall transparently forward the EAP-Request/AKA'-Challenge message to the UE 601 in a NAS message Authentication Request message. The ME shall forward the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM. Signature value is verified upon reception of encrypted RAND and/or AUTN by the UE. USIM/ME will decrypt the RAND and/or AUTN value upon reception from network using PQC/Hybrid/EC based decryption algorithm.

[105] Further, synchronisation failure indication by UE to network is trigged by UE to network if decryption of RAND and/or AUTN is failed, or verification failure of digital signature has occurred.

[106] FIGS. 16a-16b illustrate flow diagrams depicting a method 1600 for performing AKA, according to an embodiment of the present disclosure. The method 1600 includes a series of operations 1601-1605 at the UE and 1607-1611 at the network entity.

[107] Referring to FIG. 16a, at step 1601, the processing unit 613 generates an ephemeral shared key and a corresponding encrypted ephemeral shared key using the post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism.

[108] At step 1603, the processing unit 613 generates a first subscriber key (K) using the ephemeral shared key based on a KDF mechanism.

[109] At step 1605, the processing unit 613 transmits the encrypted ephemeral shared key to the network entity.

[110] Referring to FIG. 16b, at step 1607, the processor 605 receives the encrypted ephemeral shared key from the UE.

[111] At step 1609, the processor 605 decrypts the received encrypted ephemeral shared key using the PQC-KEM and the private key of the network entity, generated using PQC based key generation mechanism, to obtain the decrypted ephemeral shared key.

[112] At step 1611, the processor 605 generates a second subscriber key (K) using the ephemeral shared key based on a KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[113] FIGS. 17a-17b illustrate flow diagrams depicting another method 1700 for performing AKA, according to an embodiment of the present disclosure. The method 1700 includes a series of operations 1701-1711 at the UE and 1713-1721 at the network entity.

[114] In FIG. 17a, at step 1701, the processing unit 613 generates an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism.

[115] At step 1703, the processing unit 613 generates a first ephemeral key (s1) using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method.

[116] At step 1705, the processing unit 613 generates a second ephemeral shared key (s2) and a corresponding encrypted second ephemeral shared key using the post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and the public key of the network entity generated using PQC based key generation mechanism.

[117] At step 1707, the processing unit 613 combines the first ephemeral key (s1) and the second ephemeral shared key (s2) to generate a first hybrid ephemeral shared key.

[118] At step 1709, the processing unit 613 generates a first subscriber key (K) using the first hybrid ephemeral shared key based on a KDF mechanism.

[119] At step 1711, the processing unit 613 transmits the ephemeral public key and the encrypted second ephemeral shared key to the network entity.

[120] In FIG. 17b, at step 1713, the processor 605 receives the ephemeral public key and the encrypted second ephemeral shared key from the UE.

[121] At step 1715, the processor 605 generates the first ephemeral key (s1) using the ephemeral public key received from UE and the ephemeral private key generated at the HN based on a predetermined key agreement method.

[122] At step 1717, the processor 605 decrypts the received encrypted second ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using PQC based key generation mechanism, to obtain the decrypted second ephemeral shared key (s2).

[123] At step 1719, the processor 605 combines the generated first ephemeral key (s1) and the decrypted second ephemeral shared key (s2) to generate a second hybrid ephemeral shared key, wherein the second hybrid ephemeral shared key is same as the first hybrid ephemeral shared key.

[124] At step 1721, the processor 605 generates a second subscriber key (K) using the second hybrid ephemeral shared key based on the KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[125] FIGS. 18a-18b illustrate flow diagrams depicting another method 1800 for performing AKA, according to an embodiment of the present disclosure. The method 1800 includes a series of operations 1801-1807 at the UE and 1809-1813 at the network entity.

[126] In FIG. 18a, at step 1801, the processing unit 613 generates an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism.

[127] At step 1803, the processing unit 613 generates an ephemeral shared key using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method.

[128] At step 1805, the processing unit 613 generates a first subscriber key (K) based on the ephemeral shared key using a predefined KDF mechanism.

[129] At step 1807, the processing unit 613 transmits the ephemeral public key generated at the UE to the network entity.

[130] In FIG. 18b, at step 1809, the processor 605 receives the ephemeral public key from the UE.

[131] At step 1811, the processor 605 generates an ephemeral shared key using a private key of the network entity and the ephemeral public key of the UE using the predetermined key agreement method.

[132] At step 1813, the processor 605 generates a second subscriber key (K) based on the ephemeral shared key using the predefined KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[133] FIGS. 19a-19b illustrate flow diagrams depicting another method 1900 for performing AKA, according to an embodiment of the present disclosure. The method 1900 includes a series of operations 1901-1909 at the network entity and 1911-1915 at the UE.

[134] In FIG. 19a, at step 1901, the processing unit 605 generates an ephemeral shared key using a key generation mechanism.

[135] At step 1903, the processing unit 605 generates an ephemeral encryption key from the ephemeral shared key using a predefined key derivation function.

[136] At step 1905, the processing unit 605 generates an authentication parameter using a predetermined technique.

[137] At step 1907, the processing unit 605 encrypts the authentication parameter using the ephemeral encryption key using a symmetric encryption technique.

[138] At step 1909, the processing unit 605 transmits the encrypted authentication parameter to UE.

[139] In FIG. 19b, at step 1911, the processor 613 obtains the encrypted authentication parameter in an authentication request message.

[140] At step 1913, the processor 613 generates an ephemeral decryption key corresponding to the ephemeral encryption key generated at the network entity using the key generation mechanism.

[141] At step 1915, the processor 613 decrypts the authentication parameter using the ephemeral decryption key using a symmetric decryption technique corresponding to the symmetric encryption technique.

[142] FIGS. 20a-20b illustrate flow diagrams depicting another method 2000 for performing AKA, according to an embodiment of the present disclosure. The method 2000 includes a series of operations 2001-2007 at the network entity and 2009-2011 at the UE.

[143] In FIG. 20a, at step 2001, the processor 605 generates an authentication parameter using a predetermined technique.

[144] At step 2003, the processor 605 encrypts the authentication parameter using a private key of the network entity based on PQC based encryption technique.

[145] At step 2005, the processor 605 signs the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature to generate a digitally signed encrypted authentication parameter.

[146] At step 2007, the processor 605 transmits the digitally signed encrypted authentication parameter to UE.

[147] In FIG. 20b, at step 2009, the processing unit 613 obtains the digitally signed encrypted authentication parameter.

[148] At step 2011, the processing unit 613 decrypts, upon verifying the digital signature, the encrypted authentication parameter using a public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique.

[149] At least by virtue of aforesaid, the present subject matter at least provides the following advantages:

[150] The system and method disclosed in the present disclosure provides post quantum-safe authentication and key agreement method between subscriber and network entity.

[151] Further, the system and method disclosed in the present disclosure helps to prevent recovery of the subscriber's long-term key, which in turn would also avoid the attacker to pose as the subscriber to the network.

[152] Further, the system and method disclosed in the present disclosure prevents attacker from being able to decrypt all traffic belonging to that subscriber which is not encrypted at the application layer. Hence, subscriber location, privacy and all communication between user equipment and a network entity is not compromised.

[153] Moreover, dynamic and ephemeral subscriber key per each session allows to decrease threat surface to limit to only one session if in case of compromised ephemeral subscriber's long-term key.

[154] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one ordinary skilled in the art to which this

invention belongs. The system, methods, and examples provided herein are illustrative only and not intended to be limiting.

[155] While specific language has been used to describe the present subject matter, any limitations arising on account thereto, are not intended. As would be apparent to a person in the art, various working modifications may be made to the method to implement the inventive concept as taught herein. The drawings and the forgoing description give examples of embodiments. Those skilled in the art will appreciate that one or more of the described elements may well be combined into a single functional element. Alternatively, certain elements may be split into multiple functional elements. Elements from one embodiment may be added to another embodiment.

Claims

[Claim 1] A method performed by a user equipment (UE) in communication with a network entity for performing authentication and key agreement, the method comprising:
generating an ephemeral shared key and a corresponding encrypted ephemeral shared key using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity;
generating a first subscriber key (K) using the ephemeral shared key based on a key derivation function (KDF) mechanism; and
transmitting the encrypted ephemeral shared key to the network entity, wherein the encrypted ephemeral shared key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key.

[Claim 2] The method of claim 1, wherein the public key of the network entity is generated using PQC based key generation mechanism.

[Claim 3] The method of claim 1, further comprising:
receiving, from the network entity, a digitally signed encrypted authentication parameter, wherein the digitally signed encrypted authentication parameter is generated by encrypting authentication parameter using a private key of the network entity based on a PQC based encryption technique, and signing the encrypted authentication parameter using a PQC based digital signature; and
decrypting, upon verifying the digital signature, the encrypted authentication parameter using the public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique

[Claim 4] The method of claim 3, wherein the authentication parameter is a random number (RAND) or an authentication number (AUTN).

[Claim 5] A method performed by a network entity in communication with a user equipment (UE) for authentication and key agreement, the method comprising:
receiving the encrypted ephemeral shared key from the UE, wherein the encrypted ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity;

decrypting the received encrypted ephemeral shared key using the PQC-KEM and a private key of the network entity; and

generating a second subscriber key (K) using the decrypted ephemeral shared key generated based on a KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

[Claim 6] The method of claim 5, wherein the private key of the network entity is generated using PQC based key generation mechanism.

[Claim 7] The method of claim 5, further comprising:

generating an authentication parameter using a predetermined technique;

encrypting the authentication parameter using the private key of the network entity based on a PQC based encryption technique;

signing the encrypted authentication parameter using a PQC based digital signature to generate a digitally signed encrypted authentication parameter; and

transmitting the digitally signed encrypted authentication parameter to the UE, wherein the digitally signed encrypted authentication parameter is verified and decrypted at the UE.

[Claim 8] The method of claim 7, wherein the authentication parameter is a random number (RAND) or an authentication number (AUTN).

[Claim 9] A user equipment (UE) in communication with a network entity, the UE comprising:

a transceiver; and

a controller configured to:

generate an ephemeral shared key and a corresponding encrypted ephemeral shared key using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity,

generate a first subscriber key (K) using the ephemeral shared key based on a key derivation function (KDF) mechanism, and

transmit the encrypted ephemeral shared key to the network entity, wherein the encrypted ephemeral shared key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key

[Claim 10] The UE of claim 9,

wherein the public key of the network entity is generated using PQC based key generation mechanism.

[Claim 11] The UE of claim 9,
wherein the controller is further configured to:
receive, from the network entity, a digitally signed encrypted authentication parameter, wherein the digitally signed encrypted authentication parameter is generated by encrypting authentication parameter using a private key of the network entity based on a PQC based encryption technique, and signing the encrypted authentication parameter using a PQC based digital signature, and
decrypt, upon verifying the digital signature, the encrypted authentication parameter using the public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique.

[Claim 12] The UE of claim 11, wherein the authentication parameter is a random number (RAND) or an authentication number (AUTN).

[Claim 13] A network entity in communication with a user equipment (UE), the network entity comprising:
a transceiver; and
a controller configured to:
receive the encrypted ephemeral shared key from the UE, wherein the encrypted ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity,
decrypt the received encrypted ephemeral shared key using the PQC-KEM and a private key of the network entity, and
generate a second subscriber key (K) using the decrypted ephemeral shared key generated based on a KDF mechanism, wherein the second subscriber key is same as the first subscriber key.

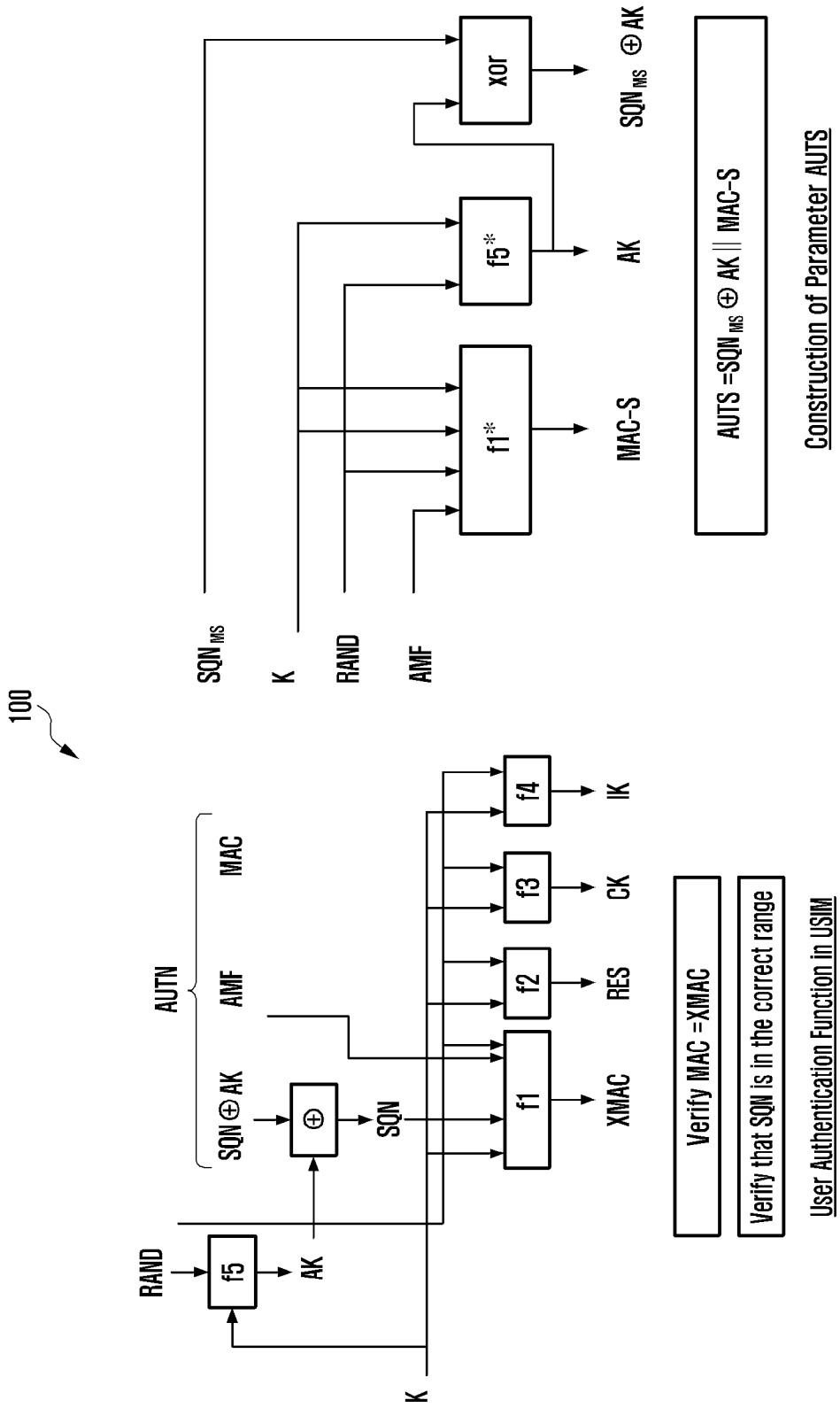
[Claim 14] The network entity of claim 13, wherein the private key of the network entity is generated using PQC based key generation mechanism.

[Claim 15] The network entity of claim 13,
wherein the controller is further configured to:
generate an authentication parameter using a predetermined technique,
encrypt the authentication parameter using the private key of the network entity based on a PQC based encryption technique,

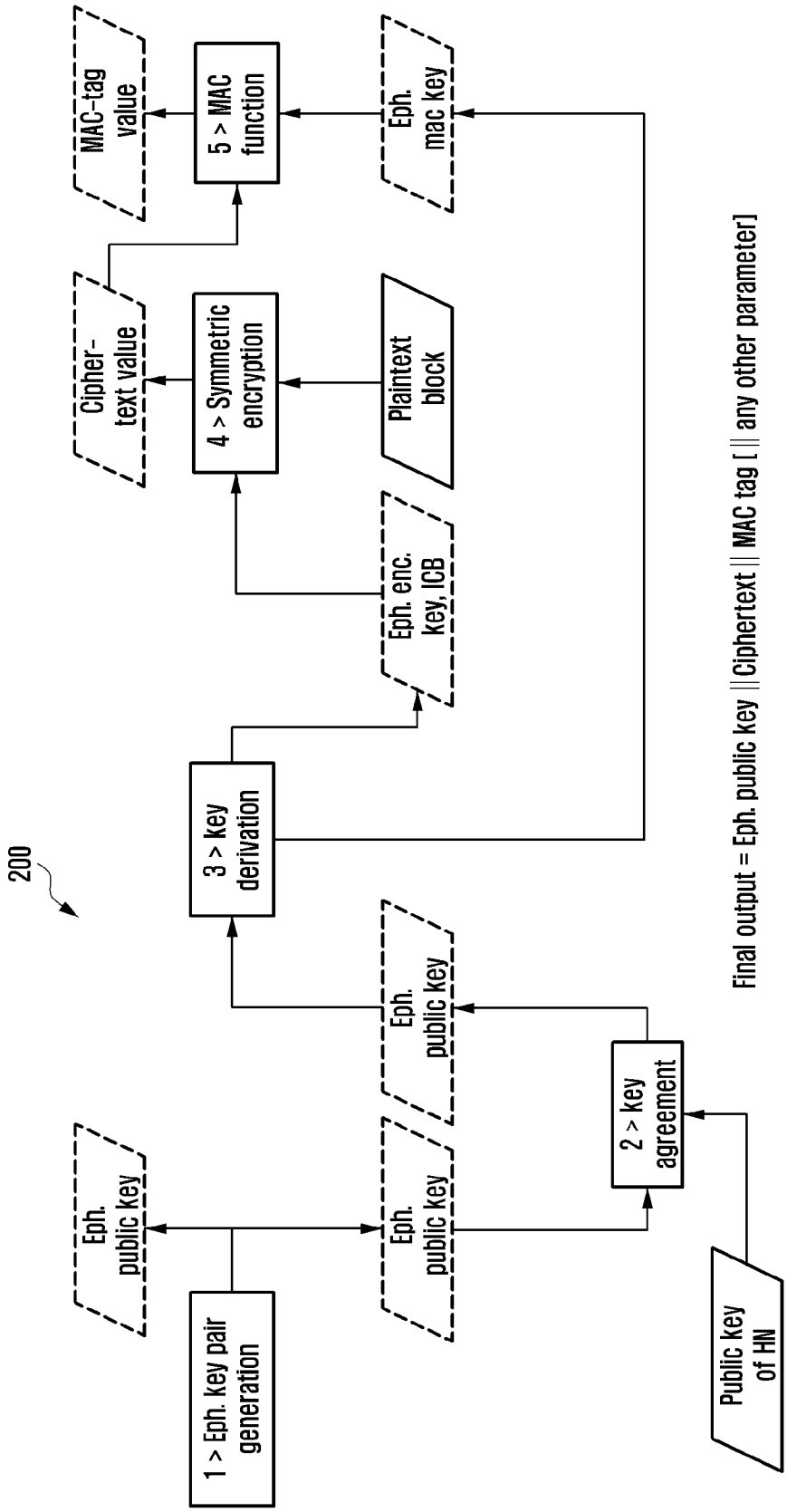
sign the encrypted authentication parameter using a PQC based digital signature to generate a digitally signed encrypted authentication parameter, and

transmit the digitally signed encrypted authentication parameter to the UE, wherein the digitally signed encrypted authentication parameter is verified and decrypted at the UE.

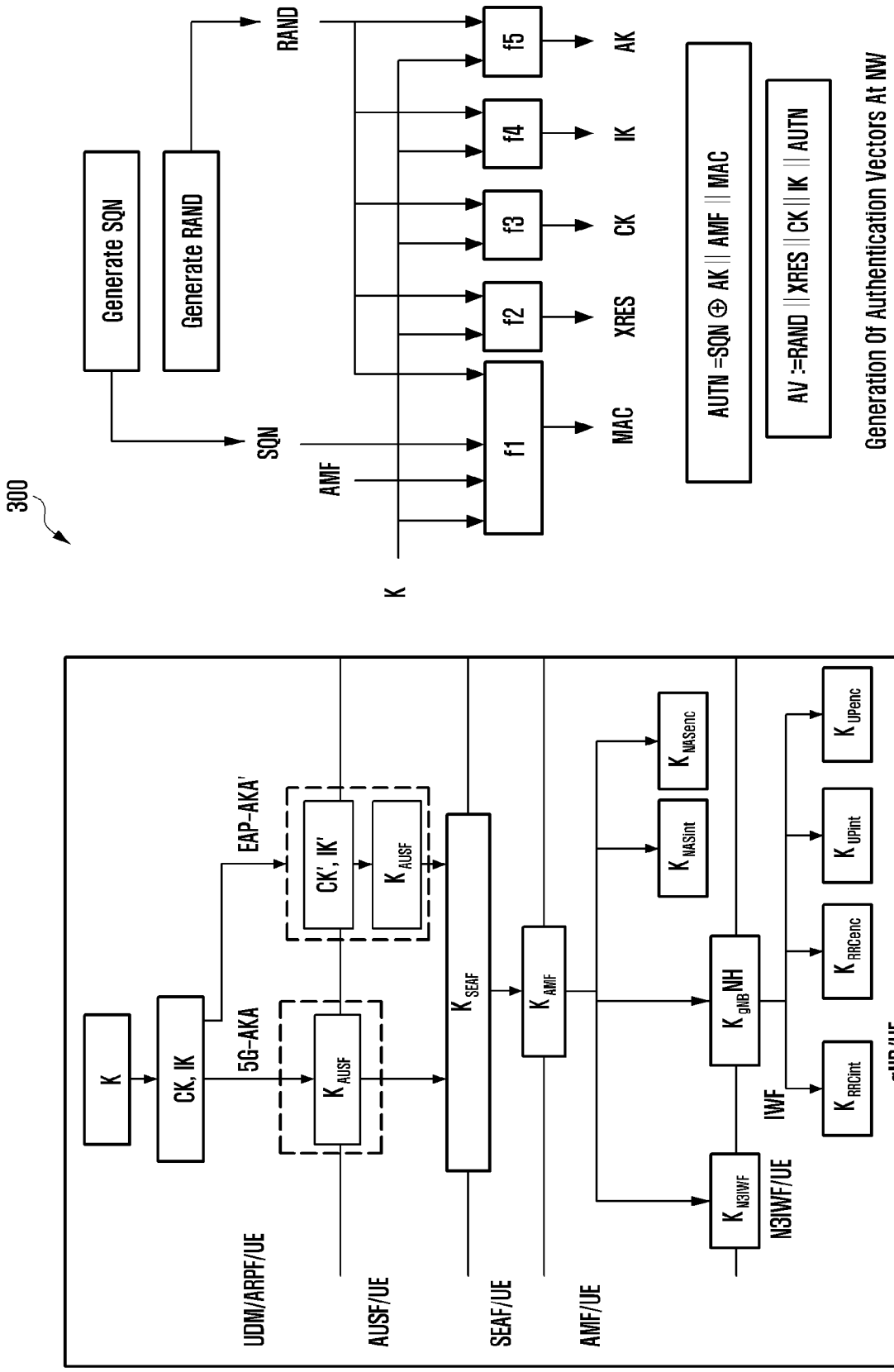
[Fig. 1]


100
SQN MS
K
RAND
AMF
f1*
f5*
xor
MAC-S
AK
SQN MS ⊕ AK
AUTS =SQN MS ⊕ AK || MAC-S
Construction of Parameter AUTS
AUTN
MAC
AMF
SQN ⊕ AK
SQN
RAND
f5
AK
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verify MAC =XMAC
Verify that SQN is in the correct range
User Authentication Function in USIM

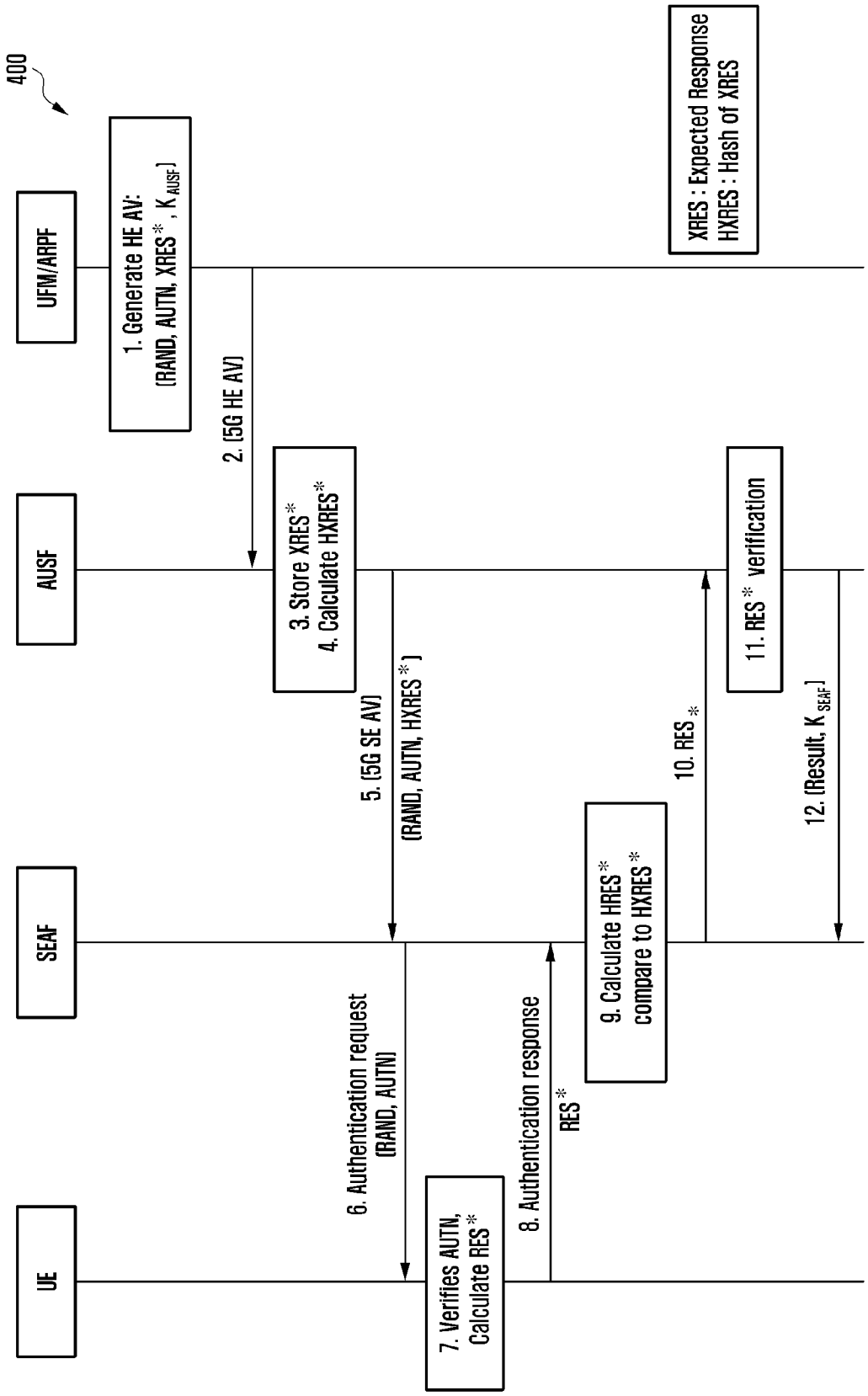
[Fig. 2]


200
1 > Eph. key pair generation
Eph. public key
Eph. public key
2 > key agreement
Public key of HN
Eph. public key
3 > key derivation
Eph. enc. key, ICB
Eph. mac key
4 > Symmetric encryption
Plaintext block
Cipher-text value
5 > MAC function
MAC-tag value
Final output = Eph. public key || Ciphertext || MAC tag [|| any other parameter]

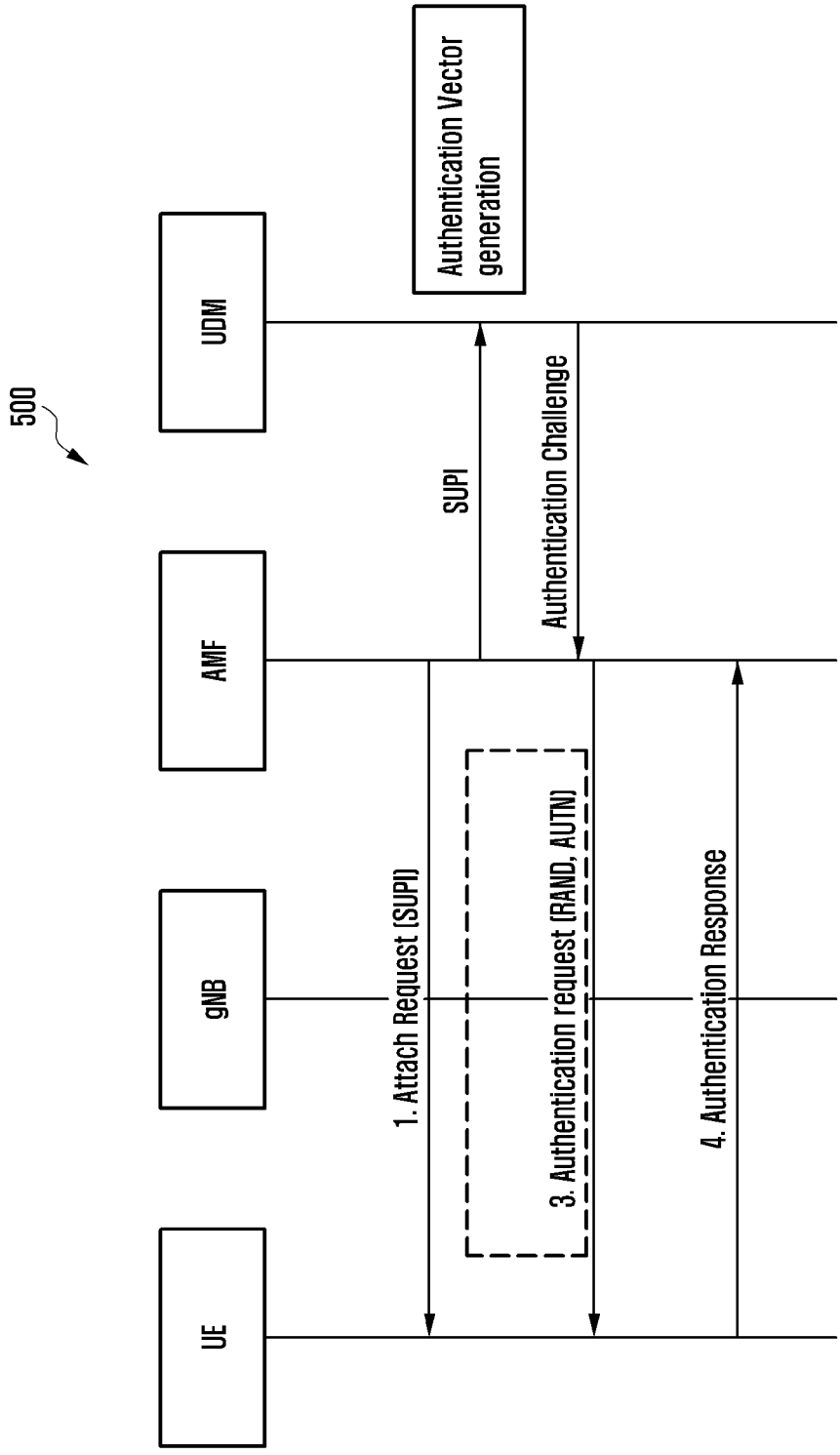
[Fig. 3]


300
Generate SQN
Generate RAND
RAND
SQN
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN =SQN ⊕ AK || AMF || MAC
AV :=RAND || XRES || CK || IK || AUTN
Generation Of Authentication Vectors At NW
K
CK, IK
5G-AKA
EAP-AKA'
CK', IK'
K AUSF
K AUSF
K SEAF
K AMF
K NASenc
K NASint
K gNB NH
K N3IWF
K RRCint
K RRCenc
K UPint
K UPenc
UDM/ARPF/UE
AUSF/UE
SEAF/UE
AMF/UE
N3IWF/UE
IWF
gNB/UE

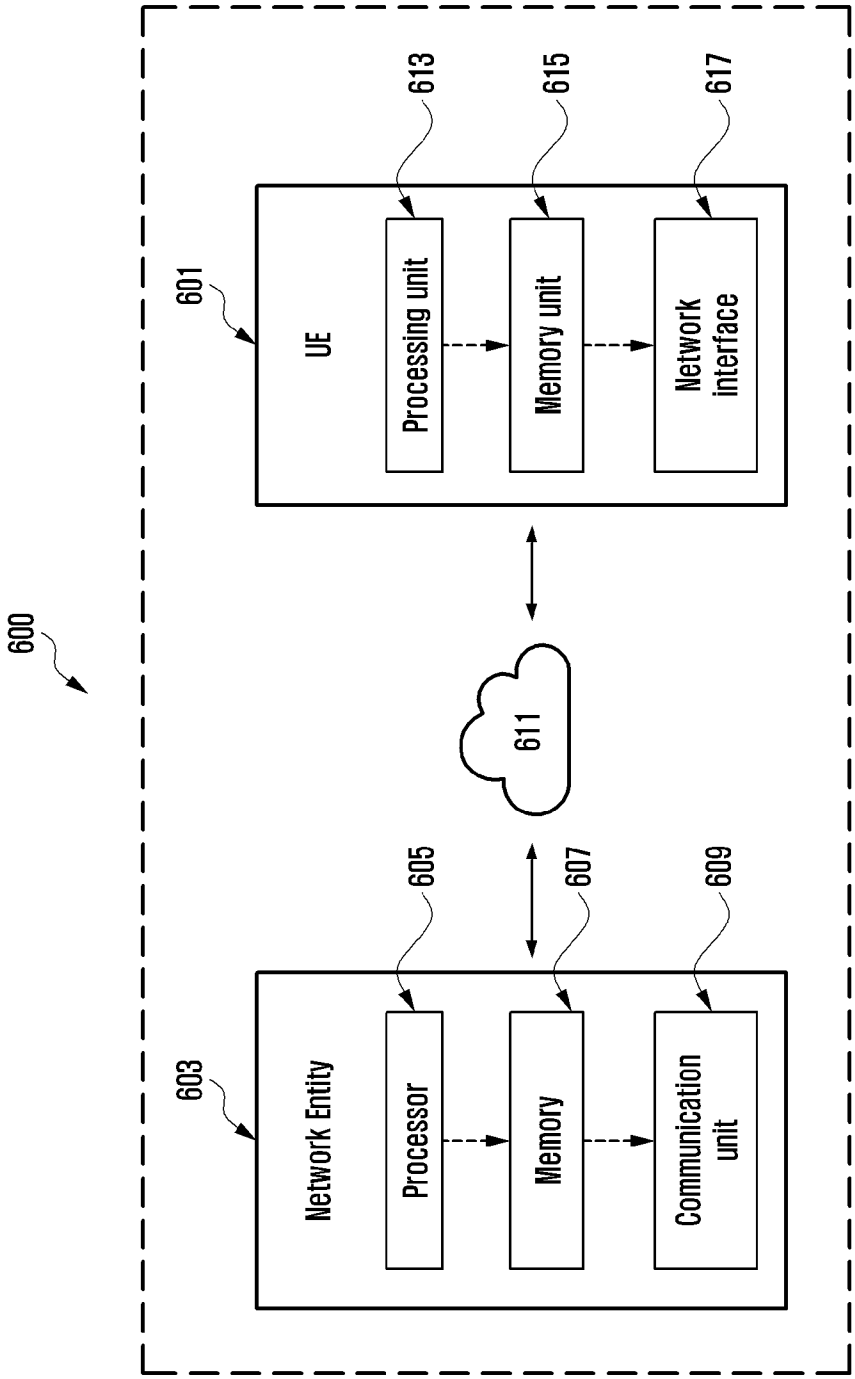
[Fig. 4]


400
UFM/ARPF
AUSF
SEAF
UE
1. Generate HE AV: (RAND, AUTN, XRES*, K_AUSF)
2. (5G HE AV)
3. Store XRES*
4. Calculate HXRES*
5. (5G SE AV) (RAND, AUTN, HXRES*)
6. Authentication request (RAND, AUTN)
7. Verifies AUTN, Calculate RES*
8. Authentication response RES*
9. Calculate HRES* compare to HXRES*
10. RES*
11. RES* verification
12. (Result, K_SEAF)
XRES : Expected Response
HXRES : Hash of XRES

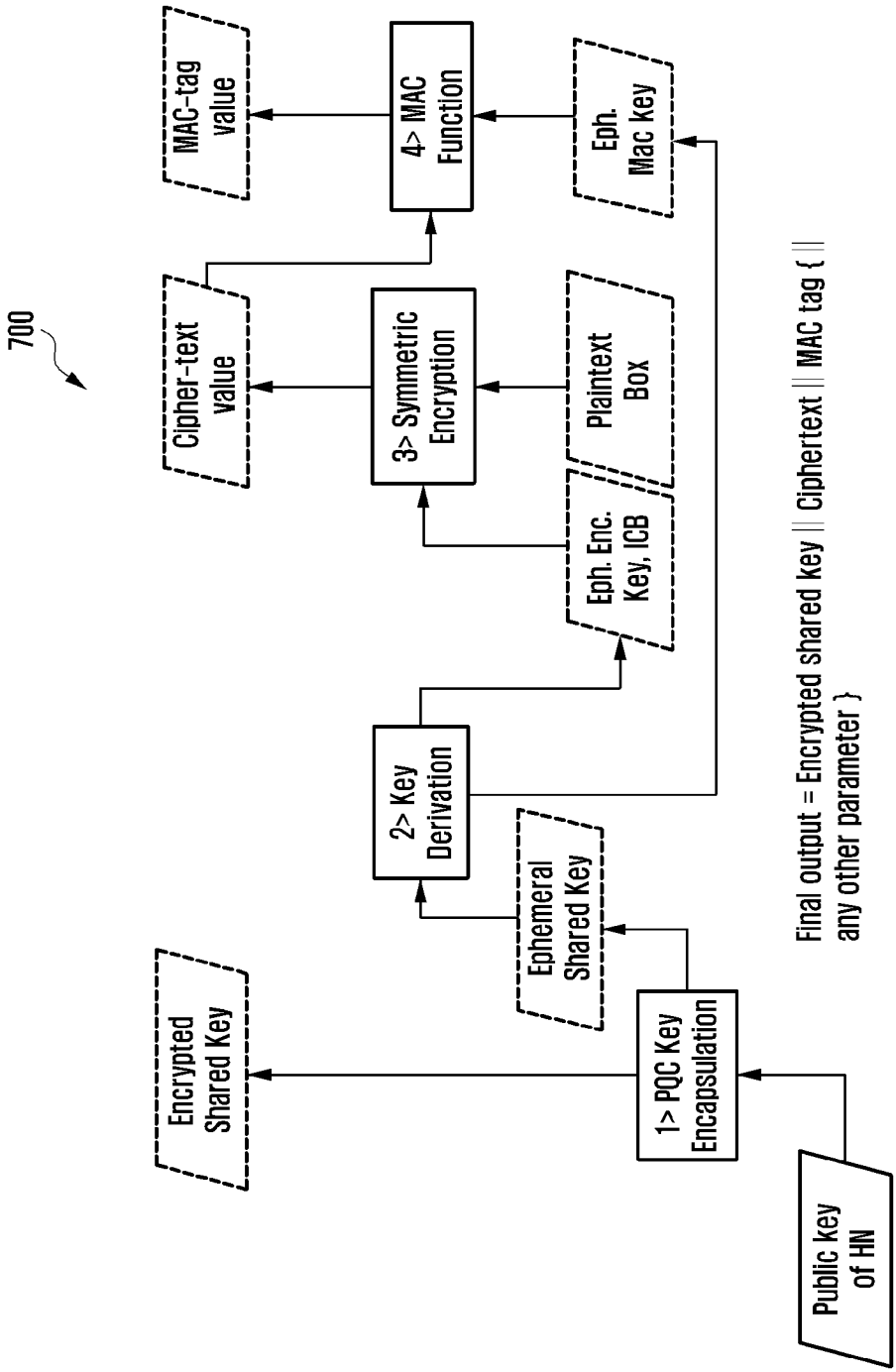
[Fig. 5]


500
UDM
AMF
gNB
UE
Authentication Vector generation
SUPI
Authentication Challenge
1. Attach Request (SUPI)
3. Authentication request (RAND, AUTN)
4. Authentication Response

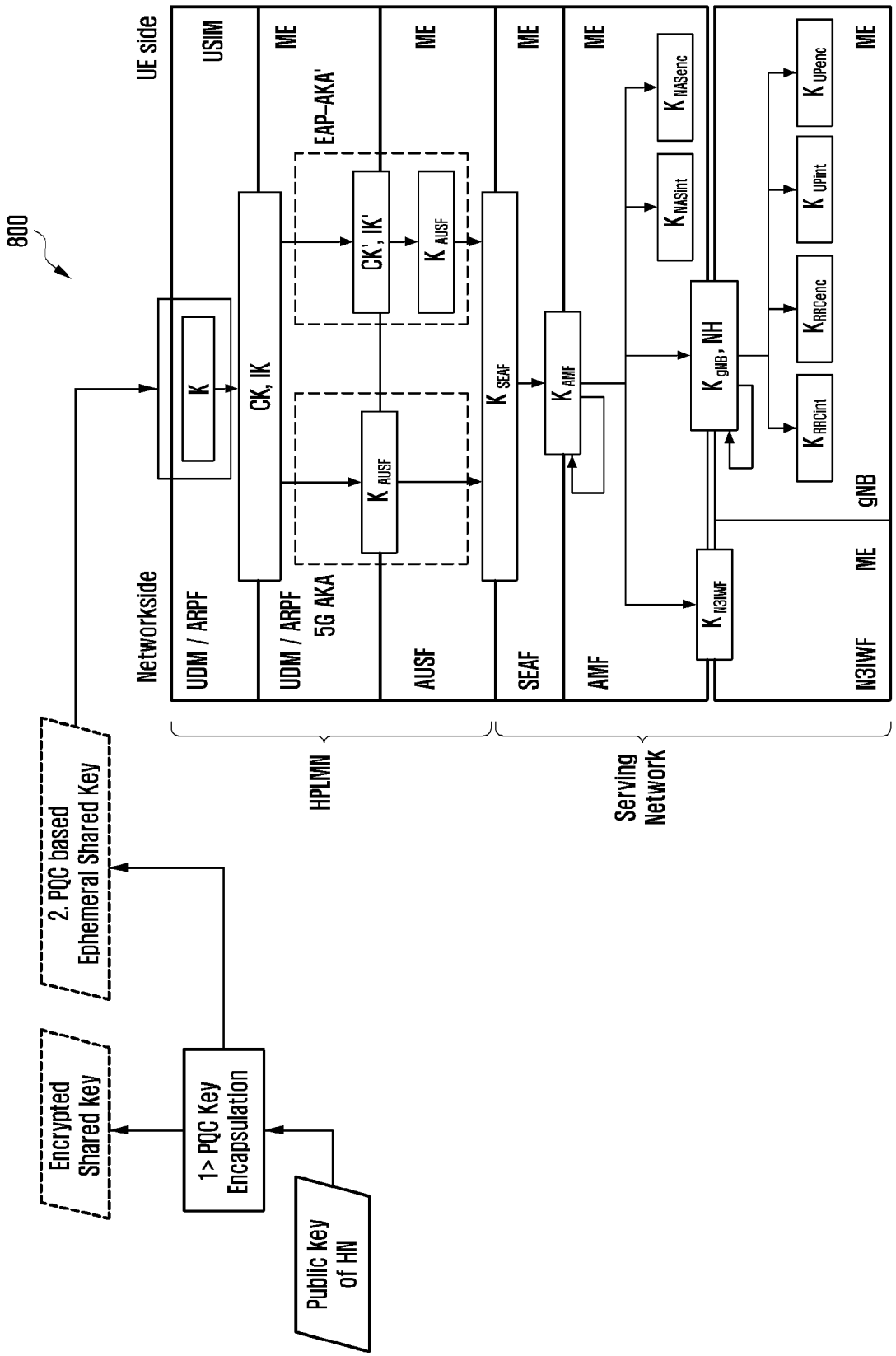
[Fig. 6]


600
601
UE
613
Processing unit
615
Memory unit
617
Network interface
611
603
Network Entity
605
Processor
607
Memory
609
Communication unit

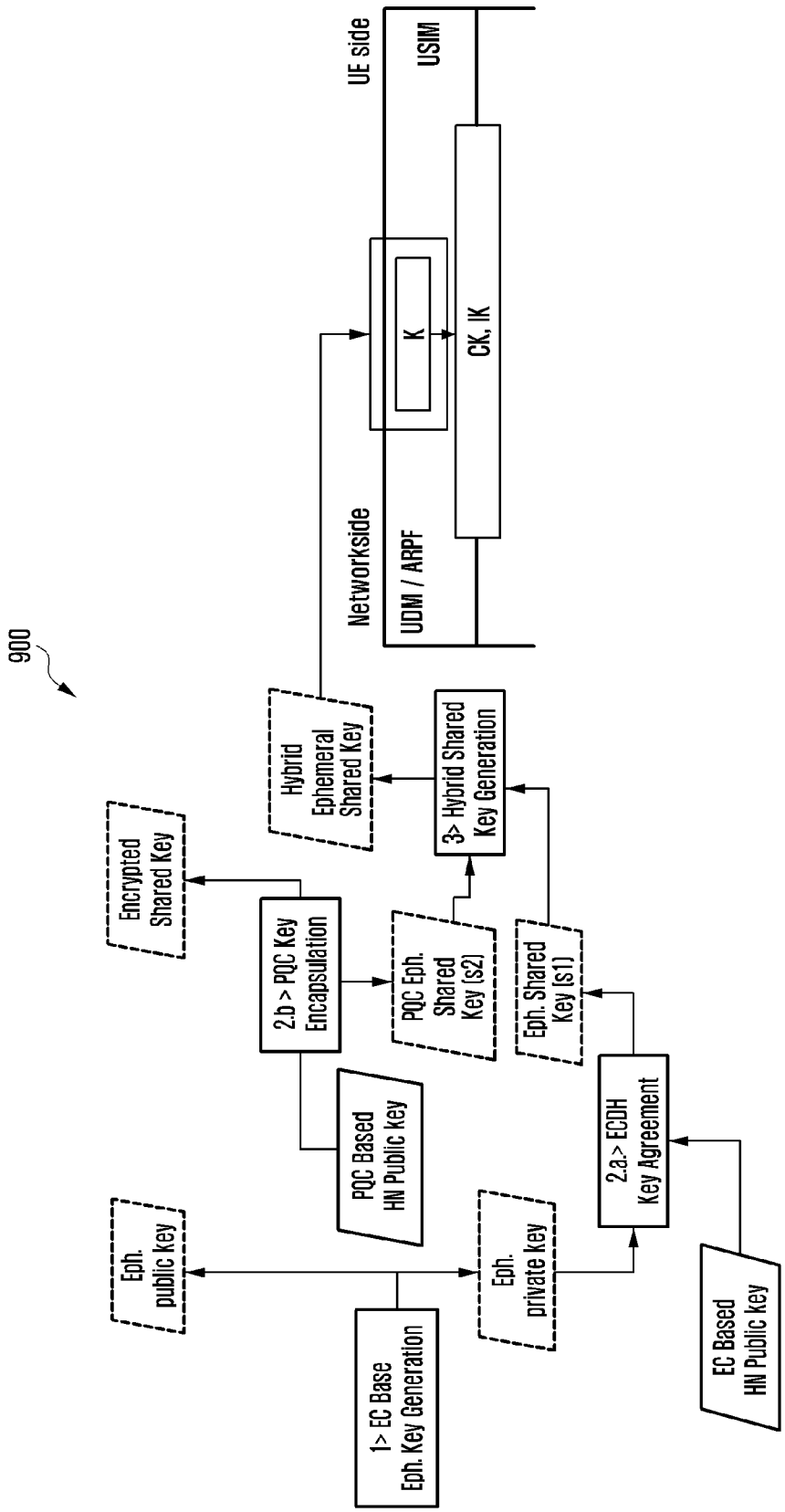
[Fig. 7]


700
Public key of HN
1> PQC Key Encapsulation
Encrypted Shared Key
Ephemeral Shared Key
2> Key Derivation
Eph. Enc. Key, ICB
Plaintext Box
3> Symmetric Encryption
Cipher-text value
Eph. Mac key
4> MAC Function
MAC-tag value
Final output = Encrypted shared key || Ciphertext || MAC tag { || any other parameter }

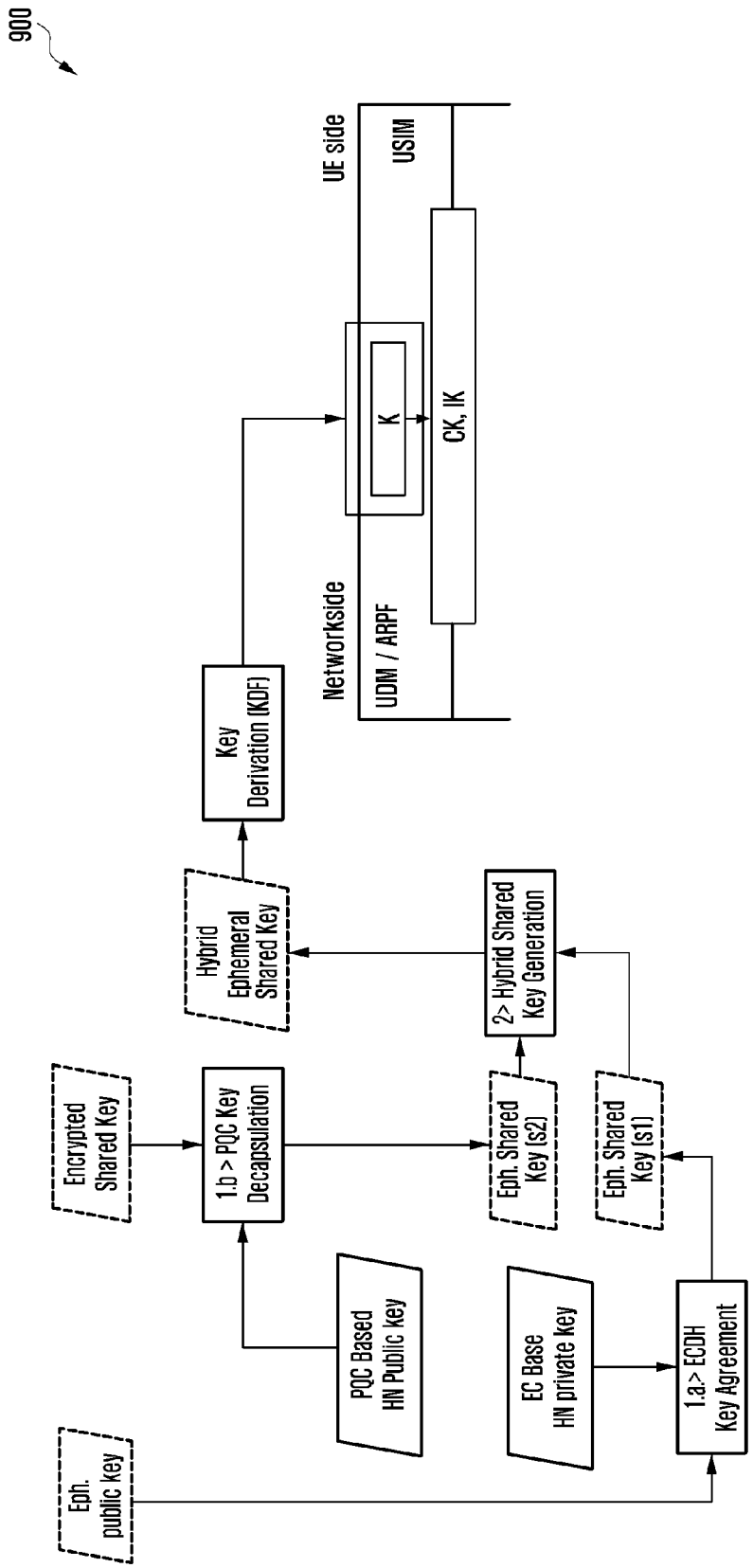
[Fig. 8]


800
UE side
USIM
ME
EAP-AKA'
CK', IK'
K AUSF
K SEAF
K AMF
K NASenc
K NASint
K gNB, NH
K UPenc
K UPint
K RRCenc
K RRCint
K N3IWF
K
CK, IK
K AUSF
Networkside
UDM / ARPF
UDM / ARPF
5G AKA
AUSF
SEAF
AMF
gNB
N3IWF
HPLMN
Serving Network
2. PQC based Ephemeral Shared Key
Encrypted Shared key
1> PQC Key Encapsulation
Public key of HN

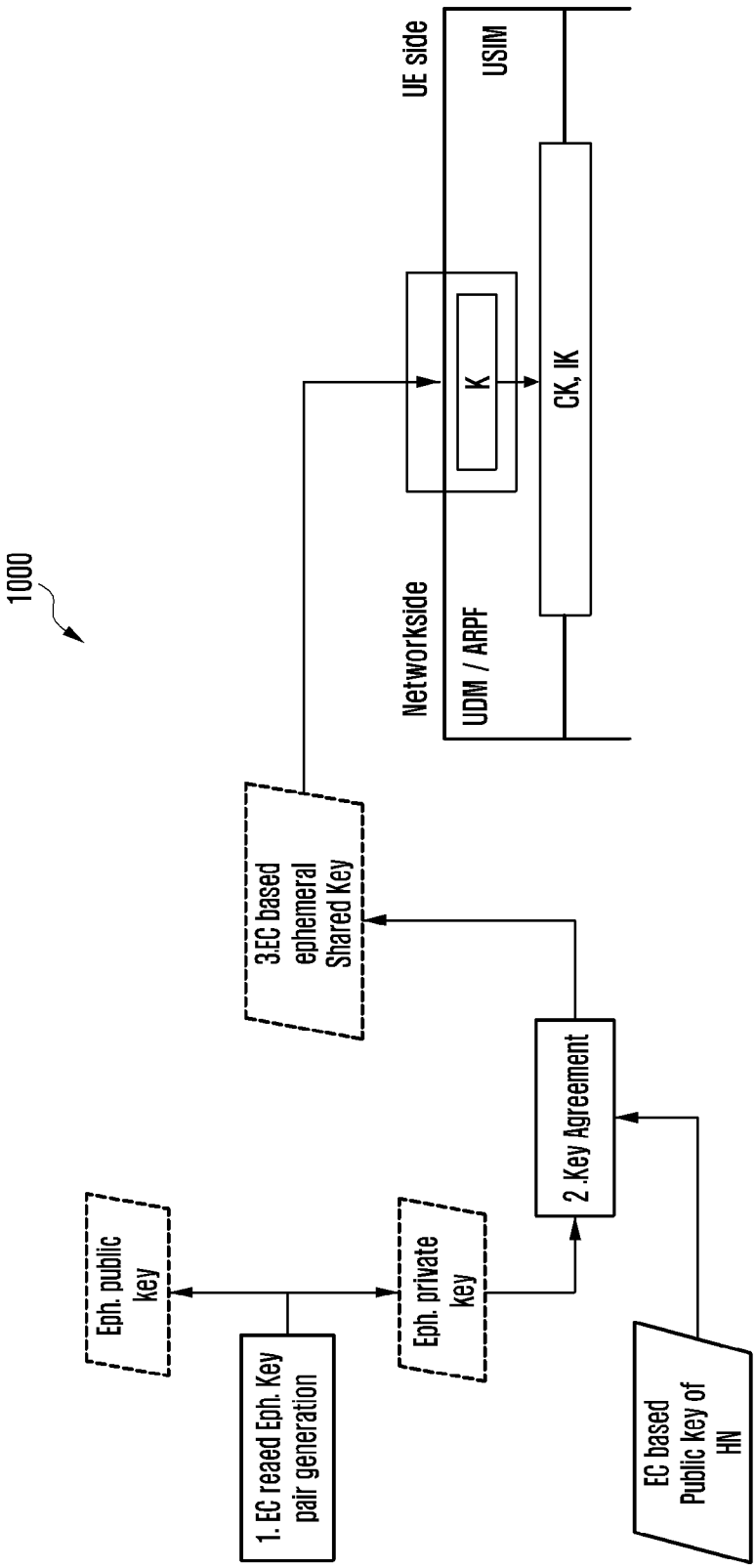
[Fig. 9a]


900
UE side
USIM
K
CK, IK
Networkside
UDM / ARPF
Hybrid Ephemeral Shared Key
3> Hybrid Shared Key Generation
Encrypted Shared Key
2.b > PQC Key Encapsulation
PQC Eph. Shared Key (s2)
Eph. Shared Key (s1)
PQC Based HN Public key
2.a.> ECDH Key Agreement
Eph. public key
Eph. private key
EC Based HN Public key
1> EC Base Eph. Key Generation

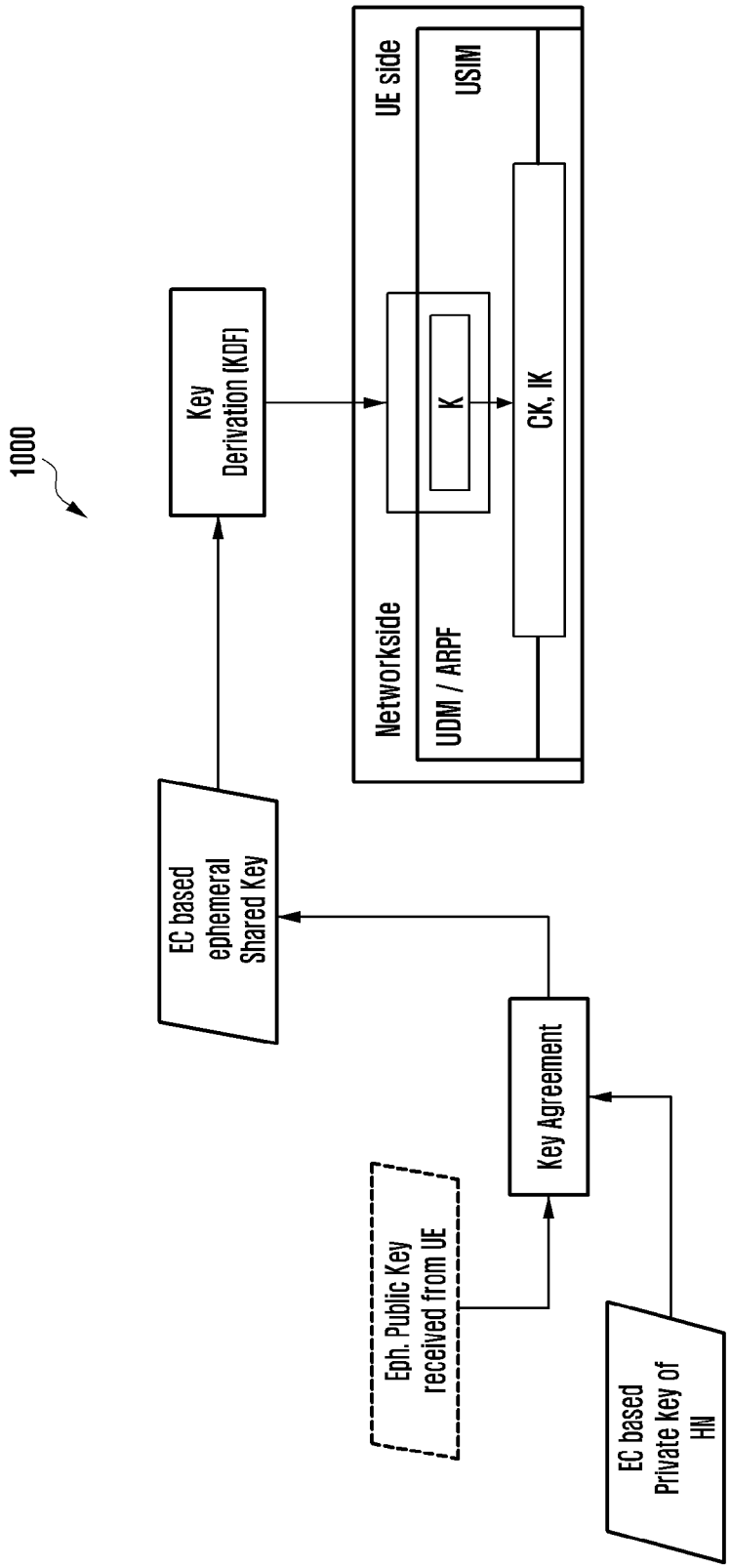
[Fig. 9b]


900
UE side
USIM
K
CK, IK
Networkside
UDM / ARPF
Key Derivation (KDF)
Hybrid Ephemeral Shared Key
2> Hybrid Shared Key Generation
Encrypted Shared Key
1.b > PQC Key Decapsulation
Eph. Shared Key (s2)
Eph. Shared Key (s1)
PQC Based HN Public key
EC Base HN private key
1.a> ECDH Key Agreement
Eph. public key

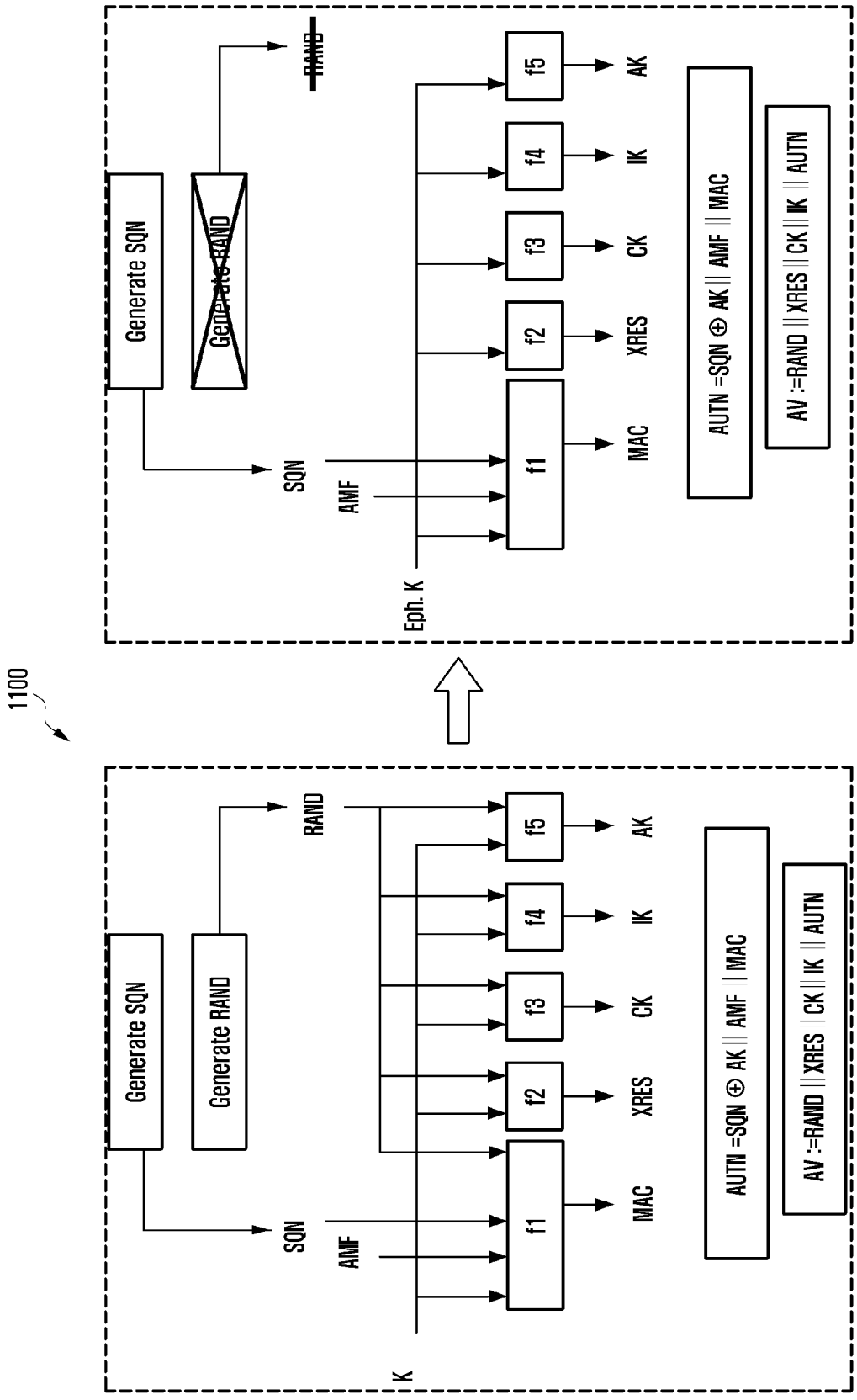
[Fig. 10a]


1000
UE side
USIM
Networkside
UDM / ARPF
K
CK, IK
3.EC based ephemeral Shared Key
2 .Key Agreement
Eph. public key
Eph. private key
1. EC reaed Eph. Key pair generation
EC based Public key of HN

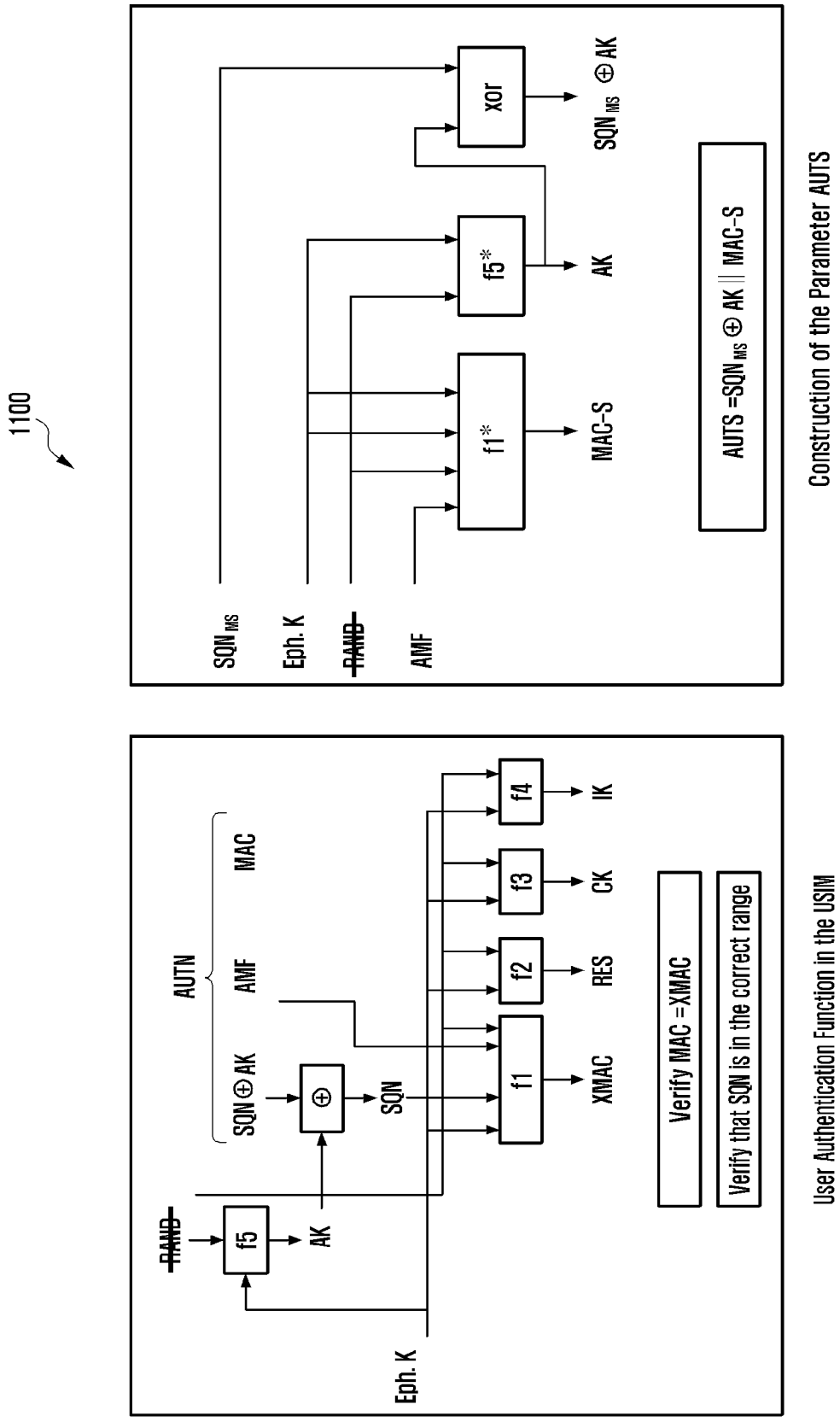
[Fig. 10b]


1000
Key Derivation (KDF)
UE side
USIM
K
CK, IK
Networkside
UDM / ARPF
EC based ephemeral Shared Key
Key Agreement
Eph. Public Key received from UE
EC based Private key of HN

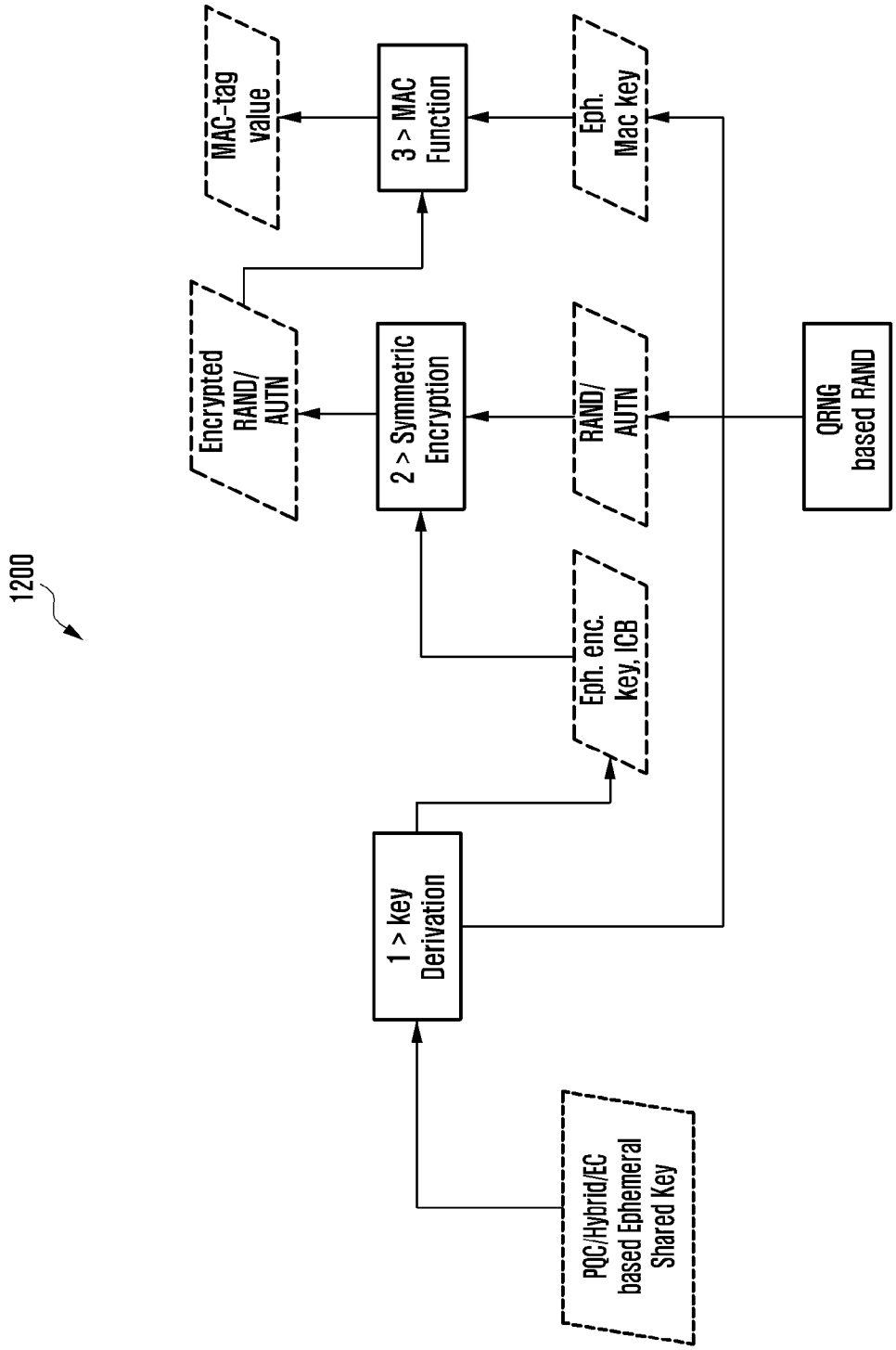
[Fig. 11a]


1100
Generate SQN
Generate RAND
RAND
SQN
AMF
Eph. K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN =SQN ⊕ AK || AMF || MAC
AV :=RAND || XRES || CK || IK || AUTN
Generate SQN
Generate RAND
RAND
SQN
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN =SQN ⊕ AK || AMF || MAC
AV :=RAND || XRES || CK || IK || AUTN

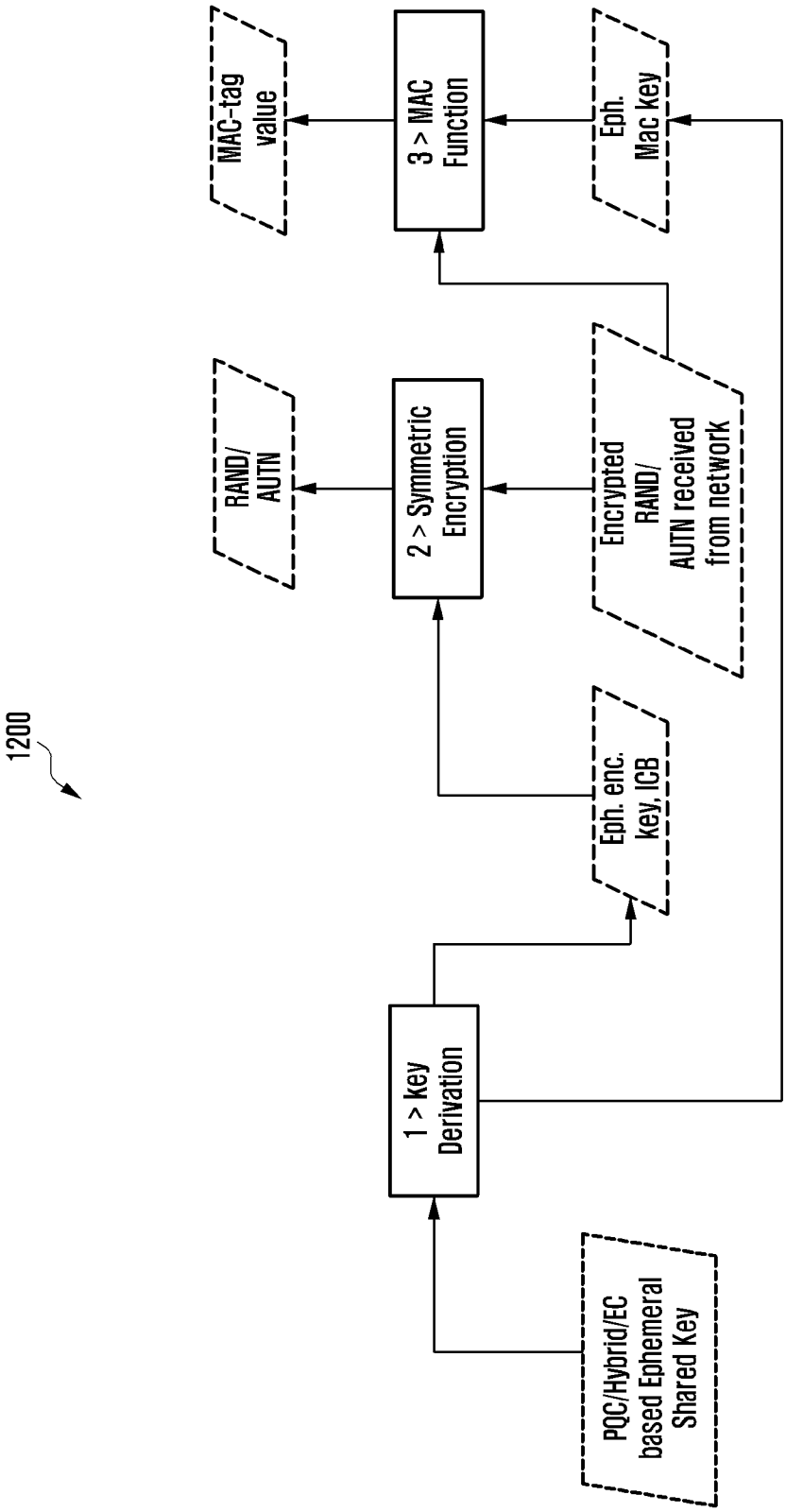
[Fig. 11b]


1100
SQN MS
Eph. K
RAND
AMF
f1*
f5*
xor
MAC-S
AK
SQN MS ⊕ AK
AUTS =SQN MS ⊕ AK || MAC-S
Construction of the Parameter AUTS
Eph. K
RAND
f5
AK
AUTN
SQN ⊕ AK
AMF
MAC
⊕
SQN
f1
f2
f3
f4
XMAC
RES
CK
IK
Verify MAC =XMAC
Verify that SQN is in the correct range
User Authentication Function in the USIM

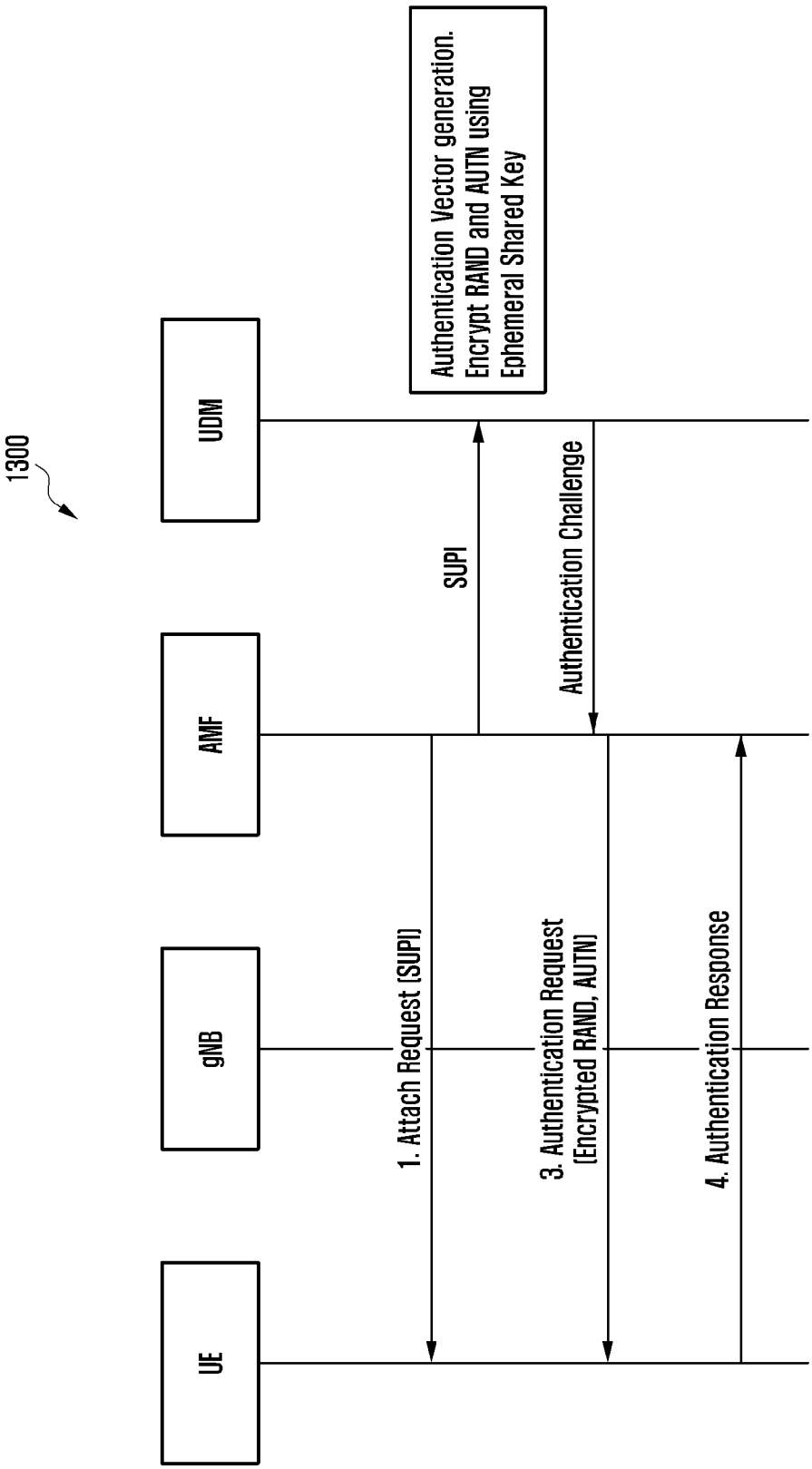
[Fig. 12a]


1200
PQC/Hybrid/EC based Ephemeral Shared Key
1 > key Derivation
Eph. enc. key, ICB
2 > Symmetric Encryption
RAND/ AUTN
QRNG based RAND
Encrypted RAND/ AUTN
3 > MAC Function
Eph. Mac key
MAC-tag value

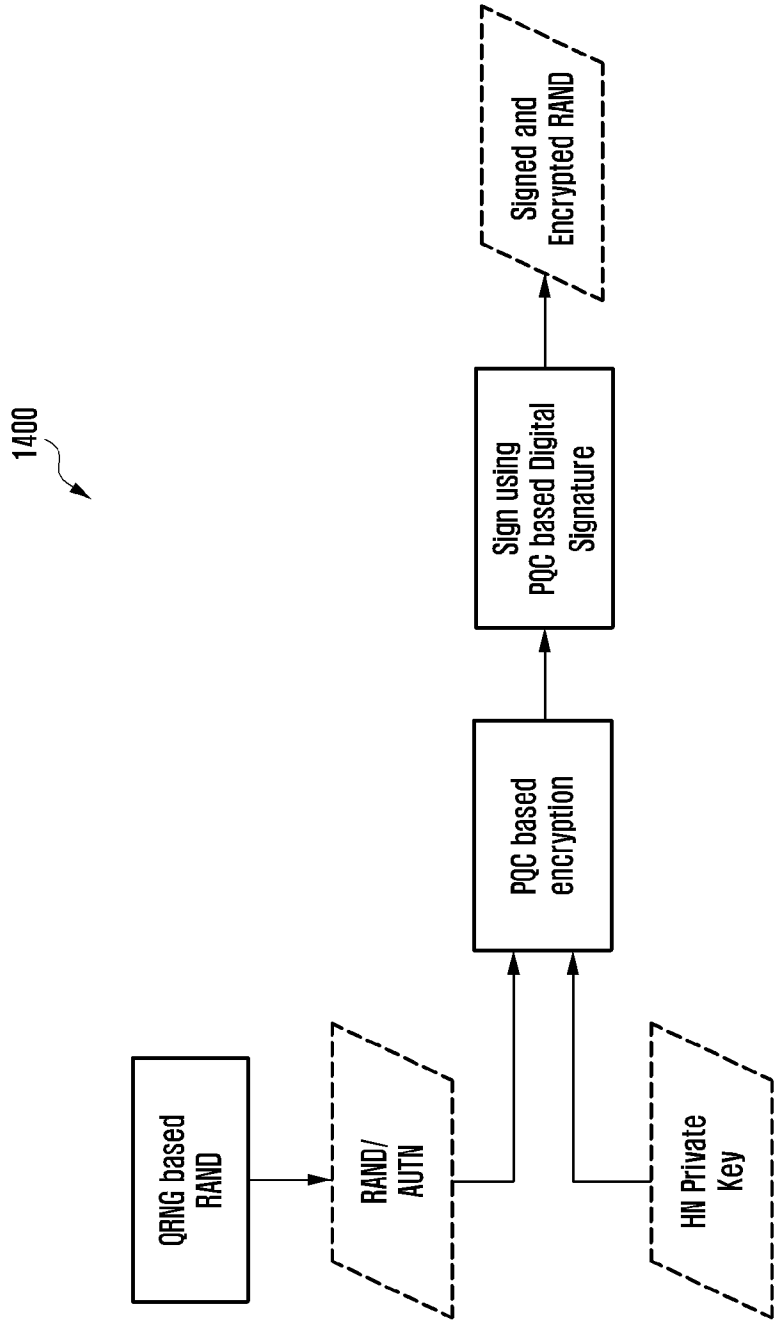
[Fig. 12b]


1200
PQC/Hybrid/EC based Ephemeral Shared Key
1 > key Derivation
Eph. enc. key, ICB
2 > Symmetric Encryption
Encrypted RAND/ AUTN received from network
RAND/ AUTN
3 > MAC Function
Eph. Mac key
MAC-tag value

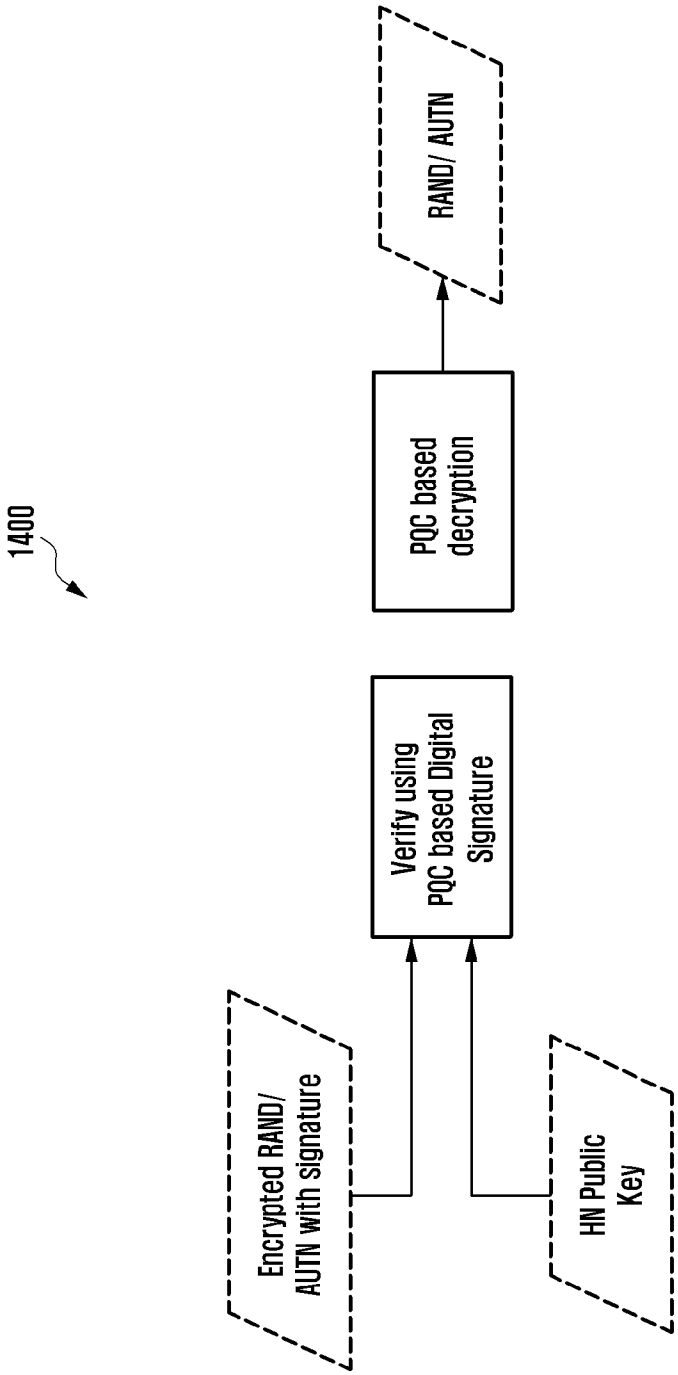
[Fig. 13]


1300
UDM
AMF
gNB
UE
Authentication Vector generation.
Encrypt RAND and AUTN using
Ephemeral Shared Key
SUPI
Authentication Challenge
1. Attach Request [SUPI]
3. Authentication Request
[Encrypted RAND, AUTN]
4. Authentication Response

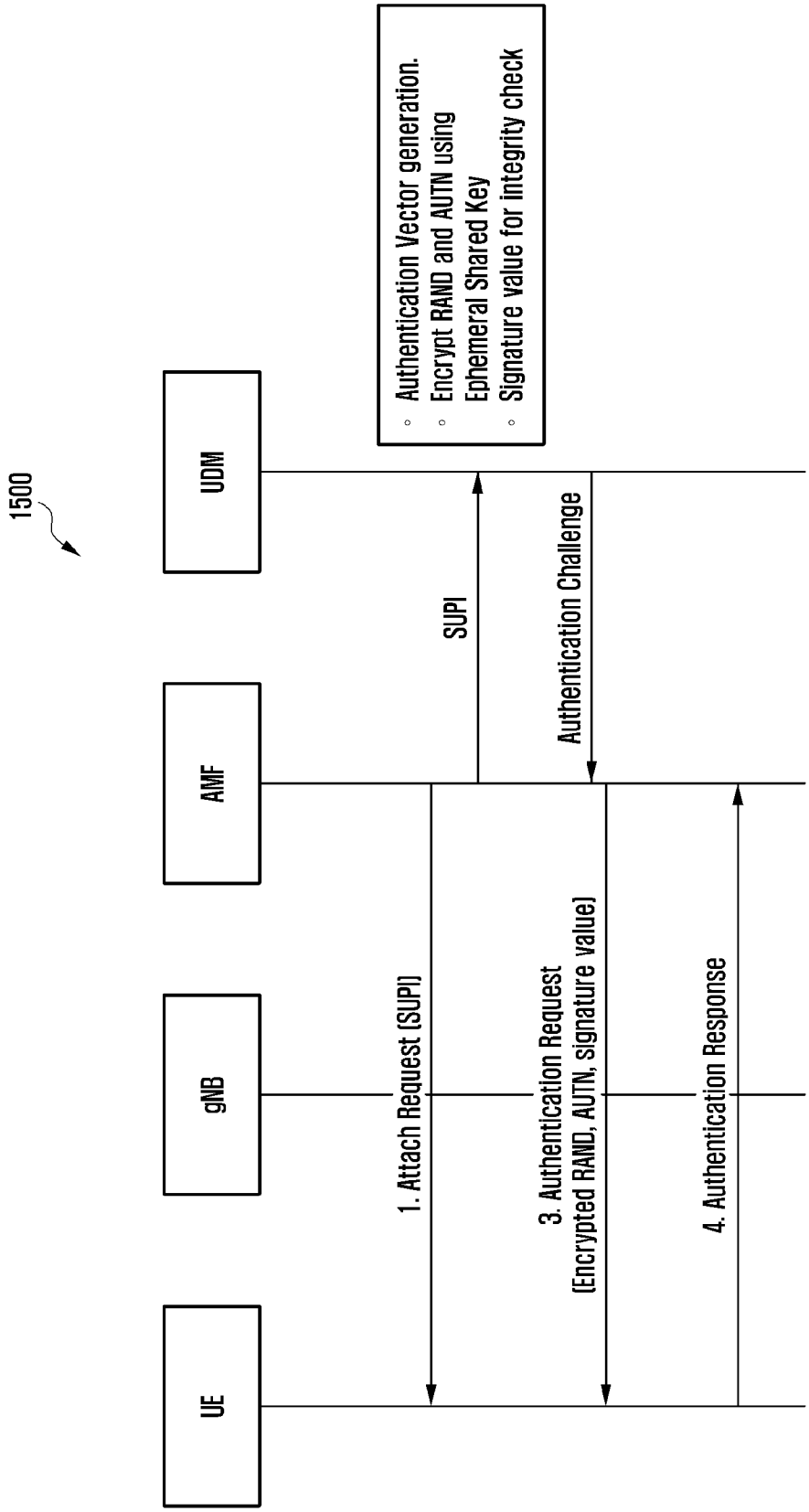
[Fig. 14a]


1400
QRNG based RAND
RAND/ AUTN
HN Private Key
PQC based encryption
Sign using PQC based Digital Signature
Signed and Encrypted RAND

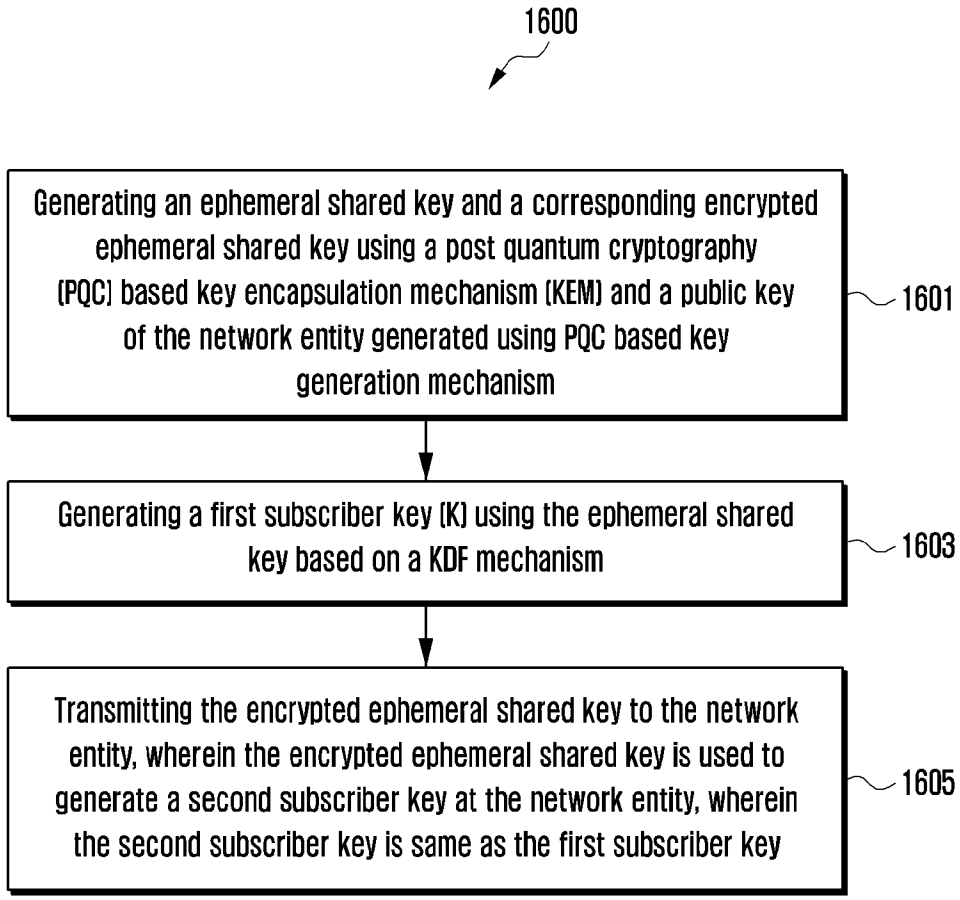
[Fig. 14b]


1400
Encrypted RAND/ AUTN with signature
HN Public Key
Verify using PQC based Digital Signature
PQC based decryption
RAND/ AUTN

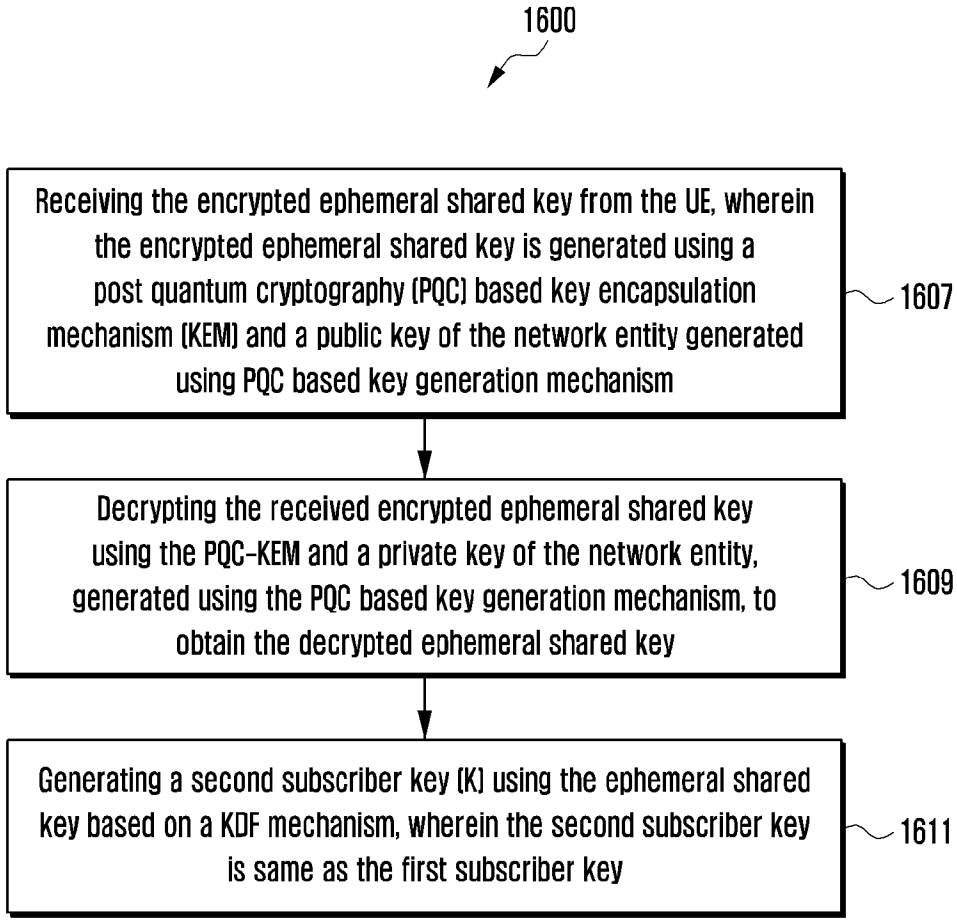
[Fig. 15]


1500
UDM
AMF
gNB
UE
Authentication Vector generation.
Encrypt RAND and AUTN using Ephemeral Shared Key
Signature value for integrity check
SUPI
Authentication Challenge
1. Attach Request (SUPI)
3. Authentication Request (Encrypted RAND, AUTN, signature value)
4. Authentication Response

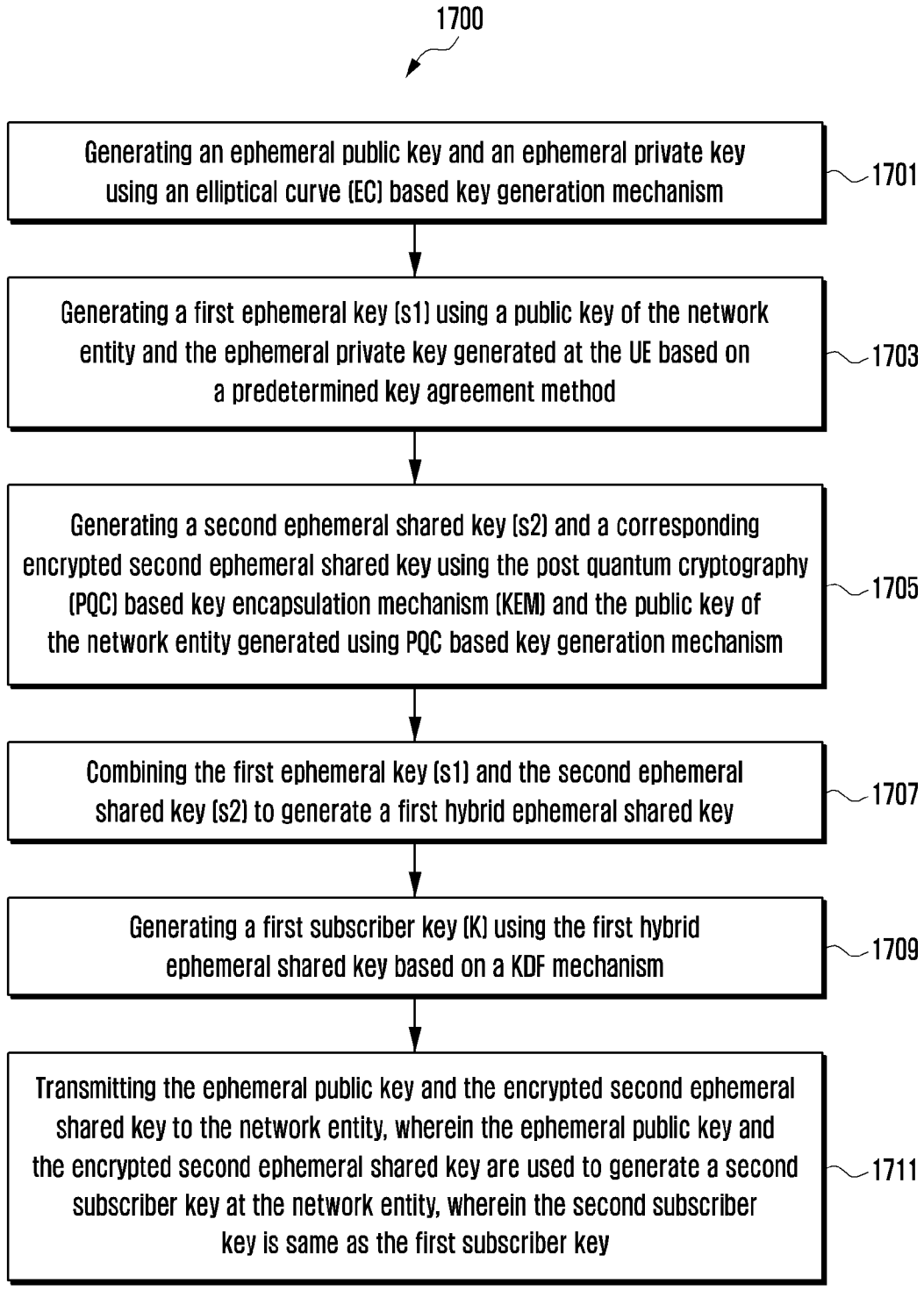
[Fig. 16a]


1600
Generating an ephemeral shared key and a corresponding encrypted ephemeral shared key using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism
1601
Generating a first subscriber key (K) using the ephemeral shared key based on a KDF mechanism
1603
Transmitting the encrypted ephemeral shared key to the network entity, wherein the encrypted ephemeral shared key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key
1605

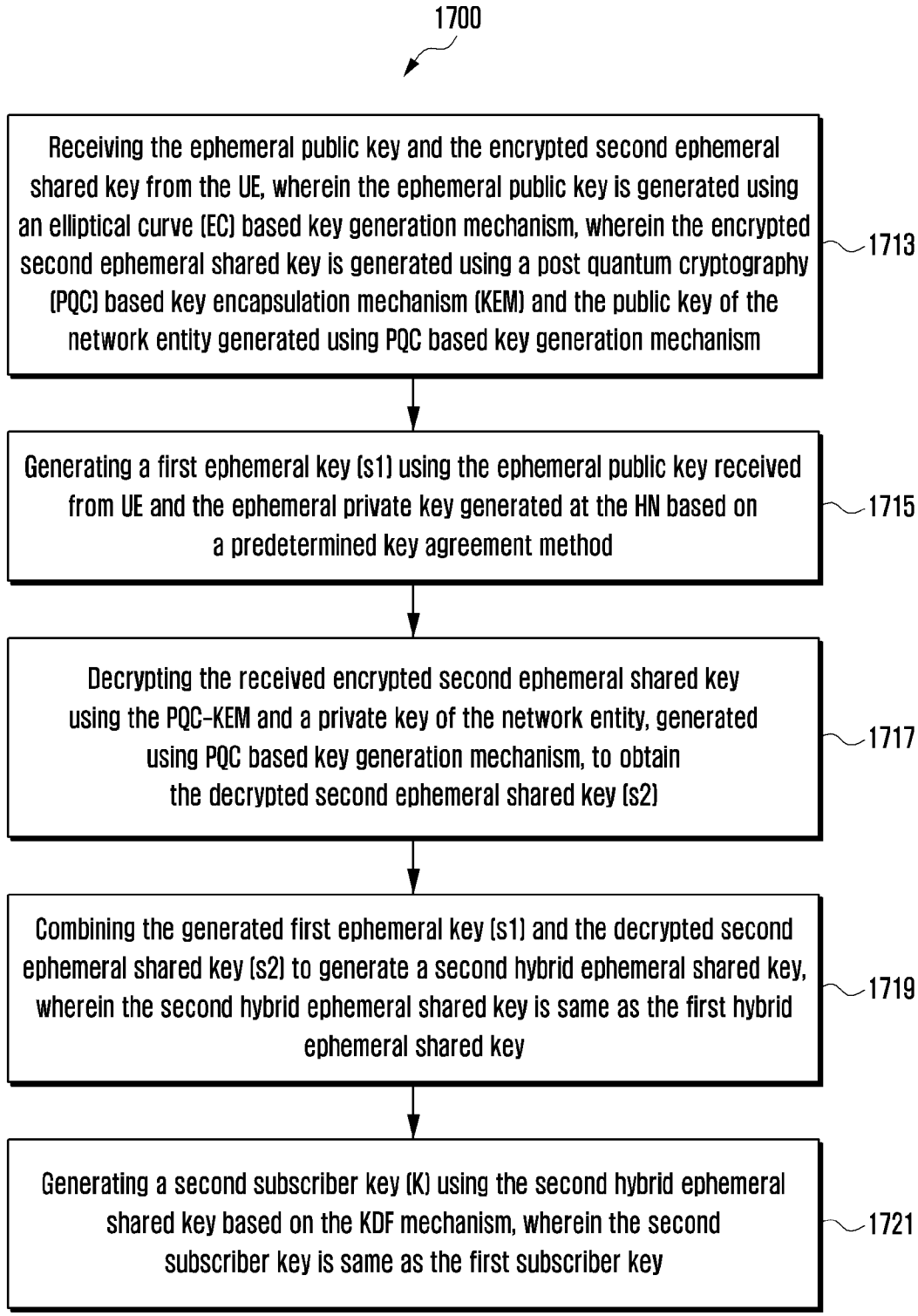
[Fig. 16b]


1600
Receiving the encrypted ephemeral shared key from the UE, wherein the encrypted ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and a public key of the network entity generated using PQC based key generation mechanism
1607
Decrypting the received encrypted ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using the PQC based key generation mechanism, to obtain the decrypted ephemeral shared key
1609
Generating a second subscriber key (K) using the ephemeral shared key based on a KDF mechanism, wherein the second subscriber key is same as the first subscriber key
1611

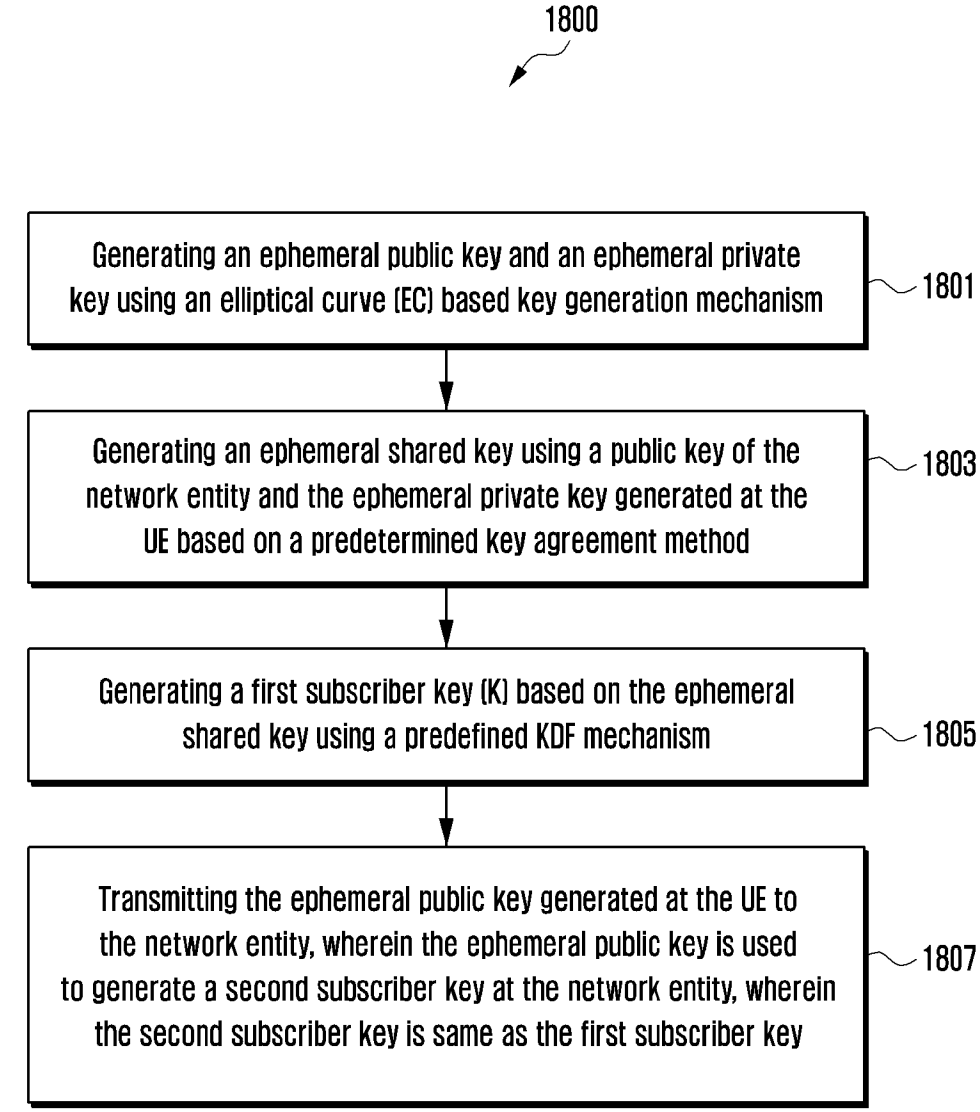
[Fig. 17a]


1700
Generating an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism
1701
Generating a first ephemeral key (s1) using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method
1703
Generating a second ephemeral shared key (s2) and a corresponding encrypted second ephemeral shared key using the post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and the public key of the network entity generated using PQC based key generation mechanism
1705
Combining the first ephemeral key (s1) and the second ephemeral shared key (s2) to generate a first hybrid ephemeral shared key
1707
Generating a first subscriber key (K) using the first hybrid ephemeral shared key based on a KDF mechanism
1709
Transmitting the ephemeral public key and the encrypted second ephemeral shared key to the network entity, wherein the ephemeral public key and the encrypted second ephemeral shared key are used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key
1711

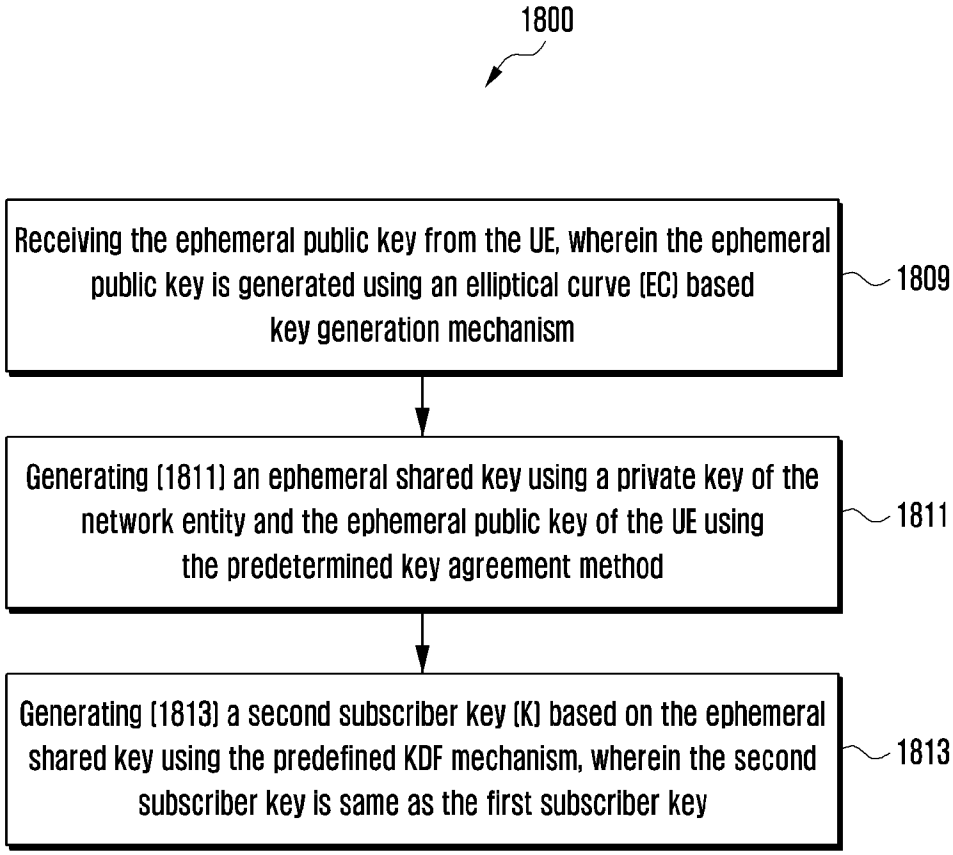
[Fig. 17b]


1700
Receiving the ephemeral public key and the encrypted second ephemeral shared key from the UE, wherein the ephemeral public key is generated using an elliptical curve (EC) based key generation mechanism, wherein the encrypted second ephemeral shared key is generated using a post quantum cryptography (PQC) based key encapsulation mechanism (KEM) and the public key of the network entity generated using PQC based key generation mechanism
1713
Generating a first ephemeral key (s1) using the ephemeral public key received from UE and the ephemeral private key generated at the HN based on a predetermined key agreement method
1715
Decrypting the received encrypted second ephemeral shared key using the PQC-KEM and a private key of the network entity, generated using PQC based key generation mechanism, to obtain the decrypted second ephemeral shared key (s2)
1717
Combining the generated first ephemeral key (s1) and the decrypted second ephemeral shared key (s2) to generate a second hybrid ephemeral shared key, wherein the second hybrid ephemeral shared key is same as the first hybrid ephemeral shared key
1719
Generating a second subscriber key (K) using the second hybrid ephemeral shared key based on the KDF mechanism, wherein the second subscriber key is same as the first subscriber key
1721

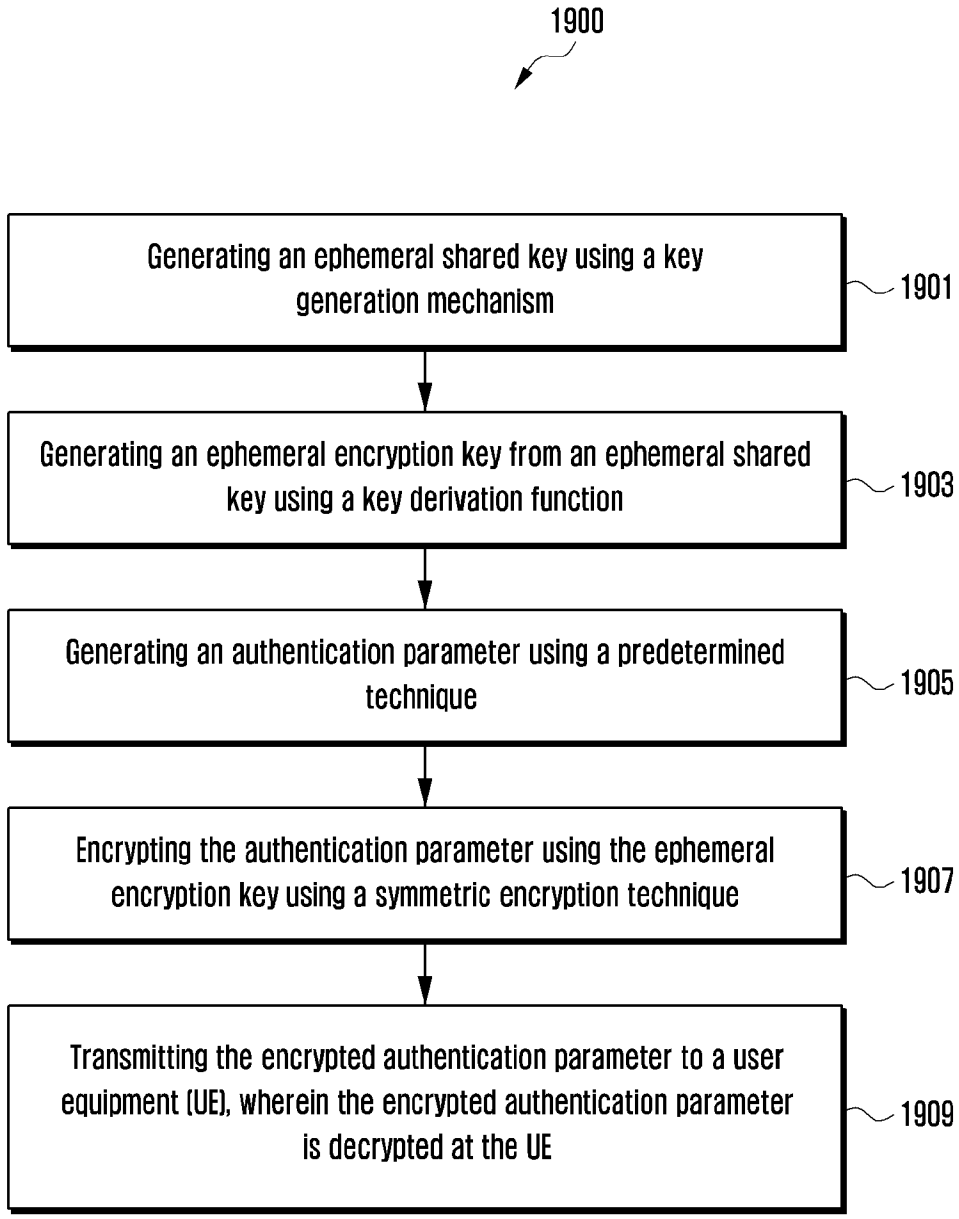
[Fig. 18a]


1800
Generating an ephemeral public key and an ephemeral private key using an elliptical curve (EC) based key generation mechanism
1801
Generating an ephemeral shared key using a public key of the network entity and the ephemeral private key generated at the UE based on a predetermined key agreement method
1803
Generating a first subscriber key (K) based on the ephemeral shared key using a predefined KDF mechanism
1805
Transmitting the ephemeral public key generated at the UE to the network entity, wherein the ephemeral public key is used to generate a second subscriber key at the network entity, wherein the second subscriber key is same as the first subscriber key
1807

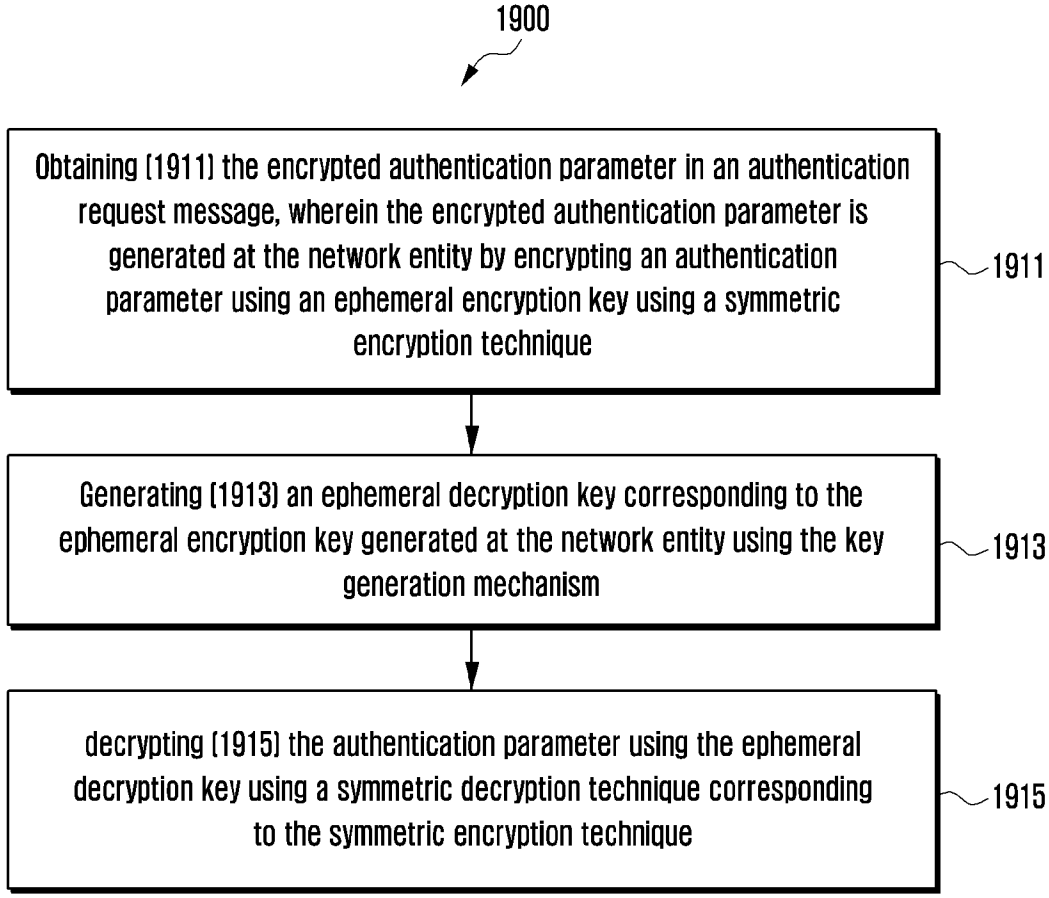
[Fig. 18b]


1800
Receiving the ephemeral public key from the UE, wherein the ephemeral public key is generated using an elliptical curve (EC) based key generation mechanism
1809
Generating (1811) an ephemeral shared key using a private key of the network entity and the ephemeral public key of the UE using the predetermined key agreement method
1811
Generating (1813) a second subscriber key (K) based on the ephemeral shared key using the predefined KDF mechanism, wherein the second subscriber key is same as the first subscriber key
1813

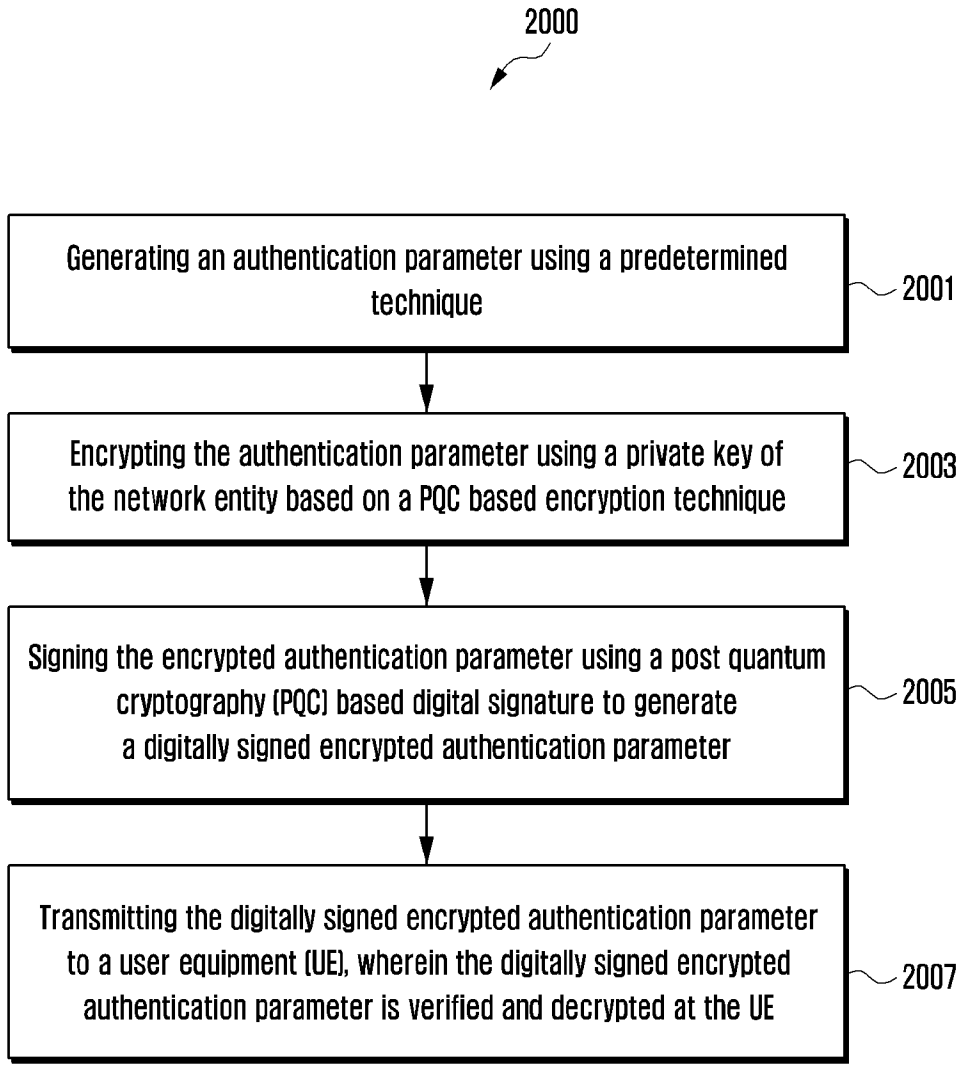
[Fig. 19a]


1900
Generating an ephemeral shared key using a key generation mechanism
1901
Generating an ephemeral encryption key from an ephemeral shared key using a key derivation function
1903
Generating an authentication parameter using a predetermined technique
1905
Encrypting the authentication parameter using the ephemeral encryption key using a symmetric encryption technique
1907
Transmitting the encrypted authentication parameter to a user equipment (UE), wherein the encrypted authentication parameter is decrypted at the UE
1909

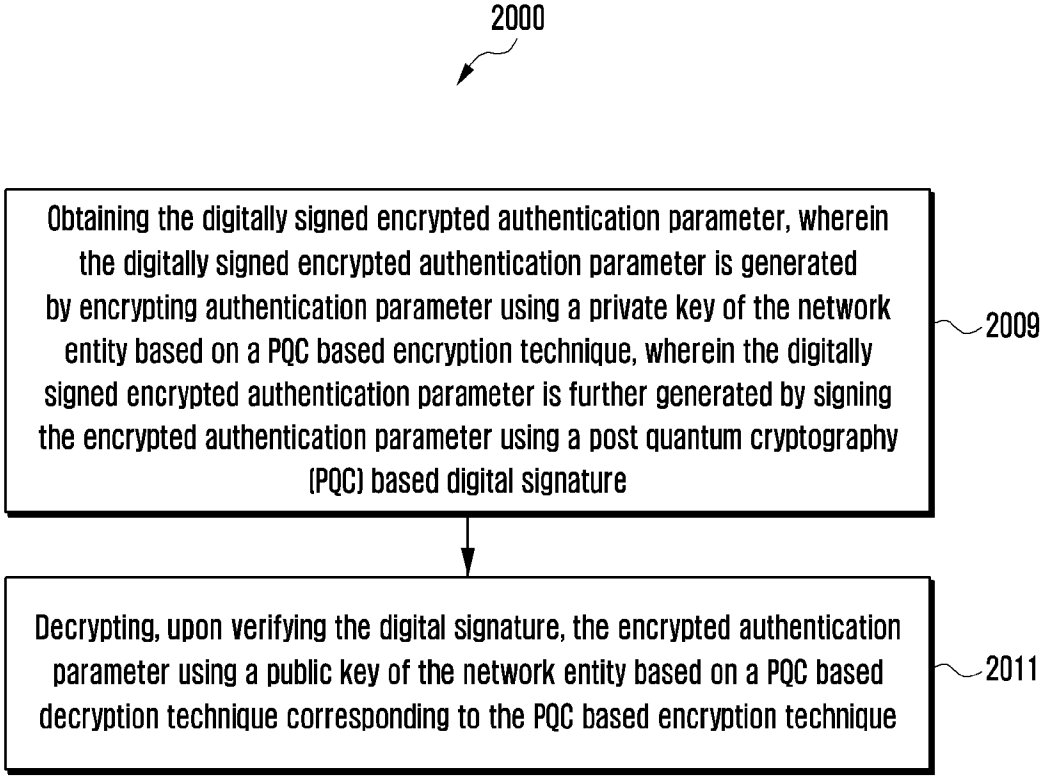
[Fig. 19b]


1900
Obtaining (1911) the encrypted authentication parameter in an authentication request message, wherein the encrypted authentication parameter is generated at the network entity by encrypting an authentication parameter using an ephemeral encryption key using a symmetric encryption technique
1911
Generating (1913) an ephemeral decryption key corresponding to the ephemeral encryption key generated at the network entity using the key generation mechanism
1913
decrypting (1915) the authentication parameter using the ephemeral decryption key using a symmetric decryption technique corresponding to the symmetric encryption technique
1915

[Fig. 20a]


2000
Generating an authentication parameter using a predetermined technique
2001
Encrypting the authentication parameter using a private key of the network entity based on a PQC based encryption technique
2003
Signing the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature to generate a digitally signed encrypted authentication parameter
2005
Transmitting the digitally signed encrypted authentication parameter to a user equipment (UE), wherein the digitally signed encrypted authentication parameter is verified and decrypted at the UE
2007

[Fig. 20b]


2000
Obtaining the digitally signed encrypted authentication parameter, wherein the digitally signed encrypted authentication parameter is generated by encrypting authentication parameter using a private key of the network entity based on a PQC based encryption technique, wherein the digitally signed encrypted authentication parameter is further generated by signing the encrypted authentication parameter using a post quantum cryptography (PQC) based digital signature
2009
Decrypting, upon verifying the digital signature, the encrypted authentication parameter using a public key of the network entity based on a PQC based decryption technique corresponding to the PQC based encryption technique
2011

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2024/095830

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; **H04L 9/32**(2006.01)i

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)

H04L 9/08(2006.01); H04L 29/06(2006.01); H04L 9/30(2006.01)

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: Post Quantum Cryptography (PQC), KEM(Key Encapsulation Mechanism), ephemeral shared key, key derivation function(KDF), subscriber key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2022-0038269 A1 (JOHN A. NIX) 03 February 2022 (2022-02-03) paragraphs [0046]-[0266], [0305]; and figures 1-2, 5, 7	1-2,5-6,9-10,13-14
A		3-4,7-8,11-12,15
Y	US 2022-0006835 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 06 January 2022 (2022-01-06) paragraphs [0038]-[0067], [0135]; and figures 1-3, 12	1-2,5-6,9-10,13-14
A	US 2022-0321333 A1 (DEUTSCHE TELEKOM AG) 06 October 2022 (2022-10-06) paragraphs [0073]-[0078]; and figures 2-3	1-15
A	US 2022-0078186 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 10 March 2022 (2022-03-10) paragraphs [0040]-[0117]; and figures 2-4	1-15

☑ Further documents are listed in the continuation of Box C. ☑ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent 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
27 August 2024	**27 August 2024**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**YANG, Jeong Rok**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5709**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2024/095830

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2022-0209950 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 30 June 2022 (2022-06-30) paragraphs [0019]-[0052]; and figures 1-8	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2024/095830

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2022-0038269 A1	03 February 2022	US 11153080 B1	19 October 2021
		US 11722296 B2	08 August 2023
		US 2024-0097891 A1	21 March 2024
		WO 2022-060471 A2	24 March 2022
		WO 2022-060471 A3	02 June 2022
US 2022-0006835 A1	06 January 2022	EP 4176563 A1	10 May 2023
		JP 2023-531241 A	21 July 2023
		US 11374975 B2	28 June 2022
		WO 2022-003009 A1	06 January 2022
US 2022-0321333 A1	06 October 2022	EP 4068677 A1	05 October 2022
		EP 4068677 B1	07 June 2023
		US 11936781 B2	19 March 2024
US 2022-0078186 A1	10 March 2022	EP 3900286 A1	27 October 2021
		US 11818124 B2	14 November 2023
		WO 2020-125942 A1	25 June 2020
US 2022-0209950 A1	30 June 2022	CN 116601914 A	15 August 2023
		GB 2617509 A	11 October 2023
		JP 2024-501197 A	11 January 2024
		US 11632246 B2	18 April 2023
		WO 2022-142837 A1	07 July 2022