

METHOD AND SYSTEM FOR AUTHENTICATION WITH ASYMMETRIC KEY

Technical Field

Embodiments of the invention further relate to authentication of user
5 equipment with asymmetric key in USIM/eUICC as authentication credentials.

Background

To protect mobile devices and networks in the data communications from
being eavesdropped or manipulated, in the 4G networks, mutual authentications are
10 employed to ensure the mobile devices (normally known as User Equipment (UE)),
and networks are genuine. To perform mutual authentication, both UEs and
networks are required to keep some credentials that can prove the identity of each
other.

In the 3G/4G networks, symmetric key technology is used for authentication
15 and key generation. With such a technology, at the network side, the credentials are
kept in servers named Home Subscriber Server (HSS); while at the UE side, the
credentials are kept in an isolated device named Universal Subscriber Identity
Module (USIM) card. For a given International Mobile Subscriber Identity (IMSI), the
credentials kept in the corresponding USIM and HSS are the same.

20 USIM card is a computing device. It is embedded in the USIM slot inside the
UE devices. USIM and UE can exchange information via a special interface.

With the 3G/4G network, when UE wants to access network and transmits
data, it has to attach to a network first. Authentication is performed during the
attachment and authentication procedure, also known as EPS-AKA. EPS-AKA
25 stands for Evolved Packet System-Authentication and Key Agreement.

With the EPS-AKA procedure, UE first sends an Attach Request to the
Mobility Management Entity (MME) via the eNodeB. MME forwards the request to
the HSS and HSS generates an authentication vector based on the credentials
shared with UE. The authentication vectors are sent to MME and MME further sends
30 authentication material to UE. UE authenticates the network and then sends an
authentication code to MME. MME verifies the authentication code and authenticates
the UE. After authentication, UE exchanges key material with MME and eNB to

further generate session keys for control and data plane. Figure 1 shows the authentication signalling exchanging procedure. Figure 2 shows key architecture of the Long-Term Evolution (LTE) network.

All the keys are derived based on the root key kept in USIM and HSS, and also the parameters exchanged between UE and core network. Keys are not transmitted in the air interface. It has been proven that the session keys generated for control and data plane with aforementioned procedure are secure provided that the root keys are not disclosed. However, recent news reported that hacking of certain servers led to theft of root keys for SIM cards. If roots key for SIM card have been stolen, this implies that the credentials in the USIM may have been disclosed. Disclosure of the USIM card credentials to attackers results in serious security risks. With the current authentication and key generation mechanism, once credentials in the SIM card is exposed to attackers, attackers can derive the user's session key by eavesdropping to the attachment and authentication signaling exchanges between UE and network.

Another technical trend is that mobile industry needs a more flexible design to support update or change of the credentials kept in the USIM. These credentials may be exposed to third parties and increases the security risks.

To overcome the security issue caused by USIM card credentials exposing to third party or being accidentally stolen, one way is to enhance the session generation with stronger forward secrecy technology, for example, the Diffie-Hellman (DH) procedure. With the DH procedure, two parties, Alice and Bob, who want to generate a session key, first agree on a finite cyclic group G and a generating element g in G . Alice picks a random natural number A and sends g^A to Bob. Bob picks a random natural number B and sends g^B to Alice. Alice computes $(g^B)^A$ and Bob computes $(g^A)^B$. The value $K = (g^B)^A = (g^A)^B$ can be used as a key for encryption. It can also be used as a base for key derivation. Figure 3 shows an example procedure of the Diffie-Hellman key exchange.

Although the Diffie-Hellman procedure can prevent user data from being eavesdropping, it cannot prevent the attackers from playing the Man-In-the-Middle attack. Another way that can protect user from being eavesdropped and at the same time can also prevent Man-In-the-Middle attack is to use public key technology.

CN 101969638 B provides a method for protecting international mobile subscriber identity (IMSI) in mobile communication. By protecting IMSI with the public key in the Attach Request transmission as proposed in CN 101969638 B, it increases the difficulty for the attackers to break the session key of the relative user even if the credentials in the SIM card are disclosed. The reason is that without knowing the IMSI, the attackers do not know which credentials can be used to break the session key. However, protection is insufficient since the attacker can do an offline dictionary attack and break the session key. Because the number of users of an operator is limited, usually vary between a few hundred thousand to a few hundred millions, it is not difficult for an attacker to break the session key, especially when the number of users belonging to one operator is not high. Therefore, protecting the IMSI with public key cannot prevent breaking of the session key using dictionary attack.

CN 102664725 provides a security certificate method of a femtocell base station and a femtocell wireless communication system. CN 102664725 proposes a use of public key to authenticate the network. The method is valid for authentication. However, method for network to authenticate the UE with the public key is not provided. Therefore, the solution is not complete for cellular networks. Also, method of generating session key after authentication is not provided.

In view of the possible security threats resulting from loss of USIM card credentials, improved methods and systems to address the above and other issues are highly desirable.

Summary

Instead of keeping a symmetric key at both UE and core network entity, embodiments of the invention disclose storage of a pair of asymmetric keys at User Equipment (UE) and core network entity separately, and a mechanism based on the asymmetric keys to authenticate UE and core network entity, and also generate session keys.

According to a first aspect of the invention, a method for authentication and key generation in a cellular network is provided, wherein the method comprising:

receiving, at a core network entity, at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the
5 UE identity;

decrypting, based at least on asymmetric key technique, the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity;

generating an authentication vector based at least on the decrypted first
10 random number; and

transmitting the authentication vector which is destined for the UE for authentication of the core network entity.

With reference to the first aspect, in a first possible implementation manner of the first aspect, further comprising:

15 receiving a first message authentication code (MAC) from the UE;

generating a second MAC based at least on the decrypted first random number;

authenticating the UE successfully when the first MAC and the second MAC meet a preset condition(for example, the first MAC and the second MAC are equal).

20 With reference to the first possible implementation manner of the first aspect, in a second possible implementation manner of the first aspect, wherein generating a second message authentication code (MAC) based at least on the decrypted first random number comprises:

generating the second MAC based at least on the decrypted first random
25 number and a symmetric key which is shared between the core network entity and the UE.

With reference to the first possible implementation manner of the first aspect, in a third possible implementation manner of the first aspect, wherein generating a second message authentication code (MAC) based at least on the decrypted first random number comprises:

- 5 generating the second MAC based at least on the decrypted first random number and a hash function which is shared between the core network entity and the UE.

With reference to any one of the first aspect, the first to the third possible implementation manner of the first aspect, in a fourth possible implementation
10 manner of the first aspect, further comprising:

 generating one of a third MAC and a signature based at least on the decrypted first random number;

 transmitting, from the core network entity to the UE, the one of the generated third MAC or the signature.

15 With reference to the first possible implementation manner of the first aspect, in a fifth possible implementation manner of the first aspect, wherein decrypting, based at least on asymmetric key technique, the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity is performed at a Home Subscriber Server (HSS) of the core network;

20 wherein generating an authentication vector based at least on the decrypted first random number comprises:

 generating, at the HSS, the authentication vector based on the decrypted first random number, and at least one of a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric
25 key is shared between the HSS and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

wherein transmitting the authentication vector comprises:

transmitting, to a management entity of the core network, at least the network AUTN and the XRES; and

wherein the method further comprising:

- 5 receiving from the UE a response value (RES) at the management entity of the core network; and

authenticating the UE successfully when the RES and XRES meet a preset condition(for example, the RES and XRES meet a preset condition).

- 10 With reference to the fifth possible implementation manner of the first aspect, in a sixth possible implementation manner of the first aspect, wherein decrypting the encrypted first random number with a private key which is retrieved from the core network entity is performed at a management entity of the core network;

wherein generating an authentication vector based at least on the decrypted first random number comprises:

- 15 generating, at a Home Subscriber Server (HSS), the authentication vector based on the decrypted first random number, and at least one of a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric key is shared between the HSS and the UE, wherein the authentication vector includes a network AUTN and an XRES;

- 20 wherein transmitting the authentication vector comprises:

transmitting, to a management entity of the core network entity, at least the network AUTN and the XRES; and

wherein the method further comprising:

receiving from the UE a response value (RES) at the management entity;
and authenticating the UE successfully when the response value (RES) and
expected result value (XRES) are equal.

With reference to the first aspect, in a seventh possible implementation
5 manner of the first aspect, further comprising:

receiving a signature from the UE;

verifying the received signature based on a public key which is retrieved from
the core network entity and associated with the UE identity;

10 encrypting at least a second random number generated at the core network
by using a public key which is retrieved from the core network entity based on the
UE identity, upon the received signature is verified successfully;; and

signing at least the second random number by using a private key which is
associated with the core network entity and retrieved therefrom; and

15 transmitting the encrypted second random number and the signed second
random number to the UE.

With reference to the first aspect, in an eighth possible implementation
manner of the first aspect, wherein generating an authentication vector based at
least on the decrypted first random number comprises:

generating a first key ($K_{\text{RND-CN}}$) based on the decrypted first random number;

20 generating a first Diffie-Hellman public key (g^x);

generating a first message authentication code (MAC) based at least on the
first Diffie-Hellman public key (g^x) by using the first key($K_{\text{RND-CN}}$);;

the method further comprising:

receiving a second Diffie-Hellman public key (g^y) and a MAC from the UE;

authenticating the UE based at least on the first MAC and the second MAC.

With reference to the first aspect, in a ninth possible implementation manner of the first aspect, further comprising:

generating a session key based on the first key ($K_{\text{RND-CN}}$) and the second
5 Diffie-Hellman public key (g^y).

According to a second aspect of the invention, a method for authentication and key generation in a cellular network is provided, the method comprising:

generating, at a user equipment (UE), a first random number and encrypting
the first random number with a public key which is retrieved from a UE and
10 associated with a UE identity;

transmitting at least the UE identity and the encrypted first random number to
a core network entity;

receiving a first authentication data from the core network entity; and

authenticating the core network entity by verifying the first authentication data
15 by using at least one of symmetric key and asymmetric key technique.

With reference to the second aspect, in a first possible implementation manner of the second aspect, wherein authenticating the core network by verifying the first authentication data comprises:

verifying one of a message authentication code (MAC) and a signature
20 included in the first authentication data to generate an authentication result; and

transmitting the authentication result to the core network entity.

With reference to the second aspect, in a second possible implementation manner of the second aspect, wherein authenticating the core network entity by verifying the first authentication data comprises:

generating a second authentication data based at least on a second random number included in the first authentication data; and

authenticating the core network entity successfully when a first authentication token (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data meet a preset condition (for example, the first AUTN and the second AUTN are equal).

With reference to the first possible implementation manner of the second aspect, in a third possible implementation manner of the second aspect, wherein generating a second authentication data based at least on a second random number included in the first authentication data comprises:

generating the second authentication data based at least on the second random number and a symmetric key shared between the UE and a Home Subscriber Server (HSS) in the core network entity.

With reference to any one of the second aspect, the first to the third possible implementation manner of the second aspect, in the fourth possible implementation manner of the second aspect, further comprising:

generating a message authentication code (MAC) based at least on a symmetric key shared between the UE and the core network entity;

transmitting the message authentication code (MAC) to the core network entity.

With reference to the second aspect, in a fifth possible implementation manner of the second aspect, the method further comprises:

further comprising:

generating a first signature based at least on a first secret key retrieved from the UE;

transmitting the first signature to the core network entity;

receiving a second signature and an encrypted second random number from the core network entity;

wherein authenticating the core network by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique, comprises:

5 decrypting the encrypted second random number by using a secret key;

 verifying the second signature by using the public key; and

 generating a session key based on the first random number and the decrypted second random number.

10 With reference to the second aspect, in a sixth possible implementation manner of the second aspect, further comprising:

 receiving a first message authentication code (MAC);

wherein authenticating the core network entity by verifying the first authentication data comprises:

15 generating a second message authentication code (MAC) based at least on a first Diffie-Hellman public key included in the first authentication data; and

 authenticating the core network entity successfully when the first MAC and the second MAC are equal.

 According to a third aspect of the invention, a system for authentication and key generation in a cellular network is provided, the system comprising:

20 a random number generation unit configured to: generate, at a user equipment (UE), a first random number;

 an encryption-decryption unit configured to: encrypt the first random number with a public key retrieved from the UE, wherein the public key is based on a UE identity associated with the UE;

a transmitting unit configured to: transmit at least the UE identity and the encrypted first random number to a core network entity;

a receiving unit configured to: receive a first authentication data from the core network entity; and

- 5 an authentication unit configured to: authenticate the core network entity by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique.

With reference to the third aspect, in a first possible implementation manner of the third aspect, wherein the authentication unit is further configured to:

- 10 verify one of a message authentication code (MAC) and a signature included in the first authentication data to generate an authentication result; and

transmit the authentication result to the core network entity.

With reference to the third aspect, in a second possible implementation manner of the third aspect, wherein the authentication unit is further configured to:

- 15 generate a second authentication data based at least on a second random number included in the first authentication data; and

- authenticate the core network entity successfully when a first authentication token (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data meet a preset condition(for
20 example, the first AUTN and the second AUTN are equal).

With reference to the second possible implementation manner of the third aspect, in a third possible implementation manner of the third aspect, wherein the authentication unit is further configured to:

- generate the second authentication data based at least on the second random
25 number and a symmetric key shared between the UE and a Home Subscriber Server (HSS) in the core network entity.

With reference to any one of the third aspect, the first to the third possible implementation manner of the third aspect, in a fourth possible implementation manner of the third aspect, the system further comprising:

5 an authentication data generation unit configured to: generate a message authentication code (MAC) based at least on a symmetric key shared between the UE and the core network entity;

wherein the transmitting unit is further configured to:

transmit the message authentication code to the core network entity.

10 With reference to the first possible implementation manner of the third aspect, in a fifth possible implementation manner of the third aspect, the system further comprising:

an authentication data generation unit configured to: generate a message authentication code (MAC) based at least on a hash function shared between the UE and the core network entity;

15 wherein the transmitting unit is further configured to:

transmit the message authentication code to the core network entity.

With reference to the third aspect, in a sixth possible implementation manner of the third aspect, wherein the encryption-decryption unit is further configured to:

20 generate a first signature based at least on a first secret key retrieved from the UE;

wherein the transmitting unit is configured to:

transmit the first signature to the core network entity;

wherein the receiving unit is further configured to:

receive a second signature and an encrypted second random number from the core network entity;

wherein the encryption-decryption unit is further configured to:

decrypt the encrypted second random number by using the secret key;

5 wherein the authentication unit is further configured to:

verify the second signature by using the public key; and

the system further comprises:

a key generation unit configured to: generate a session key based on the first random number and the decrypted second random number.

10 With reference to the third aspect, in a seventh possible implementation manner of the third aspect, wherein the receiving unit is further configured to:

receive a first message authentication code (MAC);

wherein the authentication unit is further configured to:

15 generate a second message authentication code (MAC) based at least on a first Diffie-Hellman public key included in the first authentication data; and

authenticate the core network entity successfully when the first MAC and the second MAC are equal.

According to a fourth aspect of the invention, a method for authentication and key generation in a cellular network is provided, comprising:

20 at a first core network entity:

receiving at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

transmitting the authentication vector to a second core network entity.

5 With reference to the fourth aspect, in a first possible implementation manner of the third aspect, wherein generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number comprises:

10 generating the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

15 wherein transmitting the authentication vector to a second core network entity comprises:

transmitting at least the network authentication token (AUTN) and the expected result value (XRES).

20 With reference to the fourth aspect, in a second possible implementation manner of the fourth aspect, wherein before generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number, the method further comprising:

decrypting the encrypted first random number with a private key by using at least asymmetric key technique, wherein the private key is retrieved from the first core network entity based on the UE identity.

25 With reference to the second possible implementation manner of the fourth aspect, in a third possible implementation manner of the fourth aspect, wherein the first core network entity includes Home Subscriber Server (HSS).

According to a fifth aspect of the invention, a system for authentication and key generation in a cellular network is provided, the system comprises:

a communication unit provided at a first core network entity and configured to:

5 receive at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

an authentication vector generation unit provided at the first core network entity and configured to:

10 generate an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

a communication unit provided at the first core network and configured to:

transmit the authentication vector to a second core network entity.

With reference to the fifth aspect, in a first possible implementation manner of the fifth aspect, wherein the communication unit is further configured to:

15 receive the decrypted first random number;

wherein the authentication vector generation unit is further configured to:

20 generate the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

wherein the communication unit is further configured to:

25 transmit at least the network authentication token (AUTN) and the expected result value (XRES).

With reference to the fifth aspect, in a second possible implementation manner of the fifth aspect, The system of claim 30, further comprising:

a decryption unit provided at the first core network entity and configured to:

5 before generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number, decrypt the encrypted first random number with a private key by using at least asymmetric key techniques, wherein the private key is retrieved from the first core network entity based on the UE identity.

10 With reference to the second possible implementation manner of the fifth aspect, in a third possible implementation manner of the fifth aspect, wherein the first core network entity includes Home Subscriber Server (HSS).

In another aspect, a method for authentication and key generation in a cellular network, at a first core network entity, the method comprising:

15 receiving at least a user equipment (UE) identity and decrypted first random number from the second core network entity; generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and transmitting the authentication vector to a second core network entity. wherein the first core network entity includes Home Subscriber Server (HSS).

20 wherein generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number comprises: generating the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication
25 vector includes a network authentication token (AUTN) and an expected result value (XRES); wherein transmitting the authentication vector to a second core network entity comprises: transmitting at least the network authentication token (AUTN) and the expected result value (XRES). wherein before generating an authentication vector based at least on a decrypted first random number which is obtained from the

encrypted first random number, the method further comprising: decrypting the encrypted first random number with a private key which is retrieved from the first core network entity based on the UE identity, by using at least asymmetric key technique.

5 Correspondingly, a system for authentication and key generation in a cellular network, comprising: a communication unit provided at a first core network entity and configured to receive at least a user equipment (UE) identity and decrypted first random number from the second core network entity ;an authentication vector generation unit provided at the first core network entity and configured to generate
10 an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and a communication unit provided at the first core network and configured to transmit the authentication vector to a second core network entity. wherein the communication unit is further configured to receive the decrypted first random number; wherein the authentication vector
15 generation unit is further configured to generate the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network
20 authentication token (AUTN) and an expected result value (XRES); wherein the communication unit is further configured to transmit at least the network authentication token (AUTN) and the expected result value (XRES).

According to a sixth aspect of the invention, a method for authentication and key generation in a cellular network is provided, comprising:

25 at a second core network entity:

receiving at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

decrypting the encrypted first random number with a private key by using at least asymmetric key techniques, wherein the private key is retrieved from the second core network entity based on the UE identity;

transmitting an authentication vector request to a first core network entity,
5 wherein the authentication vector request includes the UE identity and the decrypted first random number;

receiving an authentication vector from the first core network entity; and

transmitting the authentication vector to the UE.

With reference to the sixth aspect, in a first possible implementation manner
10 of the sixth aspect, wherein the authentication vector at least includes expected result value (XRES);

receiving from the UE a response value (RES); and

authenticating the UE successfully when the response value (RES) and expected result value (XRES) are equal;

15 wherein the first core network entity includes Home Subscriber Server (HSS) and the second core network entity includes one of Mobility Management Entity (MME) and Authentication, Authorization and Accounting (AAA) server.

According to a seventh aspect of the invention, a system for authentication and key generation in a cellular network is provided, wherein the system comprises:

20 a communication unit provided at a second core network entity and configured to receive at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity; a decryption unit provided at the second core network entity and configured to use at least asymmetric key techniques, decrypt the encrypted first random number with a
25 private key which is retrieved from the second core network entity based on the UE identity; wherein the communication unit is further configured to transmit an authentication vector request to a first core network entity, wherein the authentication

vector request includes the UE identity and the decrypted first random number receive an authentication vector from the first core network entity; and transmit the authentication vector to the UE.

With reference to the seventh aspect, in a first possible implementation manner of the seventh aspect, wherein the authentication vector at least includes expected result value (XRES); the communication unit is configured to: receive from the UE a response value (RES); and authentication unit is configured to : authenticate the UE successfully when the response value (RES) and expected result value (XRES) are equal; wherein the first core network entity includes Home Subscriber Server (HSS), and the second core network entity includes one of Mobility Management Entity (MME) and Authentication, Authorization and Accounting (AAA) server.

In another aspect, a method for authentication and key generation in a cellular network, comprising: receiving, at a core network entity, at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity; decrypting, based at least on asymmetric key technique, the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity; generating an authentication vector based at least on one of the decrypted first random number; and a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric key is shared between the HSS and the UE, transmitting the authentication vector which is destined for the UE for authentication of the core network entity.

wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES); wherein transmitting the authentication vector comprises: transmitting, to a management entity of the core network, at least the network authentication token (AUTN) and the expected result value (XRES); and wherein the method further comprising: receiving from the UE a response value (RES) at the management entity of the core network; and authenticating the UE successfully when the response value (RES) and expected result value (XRES) meet a preset condition(for example, the RES and XRES are equal).

According to an eighth aspect of the invention, a user equipment comprises a processor; and a storage medium communicably coupled thereto and storing instructions which are executable by the processor to cause the processor to:

generate, at a user equipment (UE), a first random number;

5 encrypt the first random number with a public key retrieved from the UE, wherein the public key is based on a UE identity associated with the UE;

transmit at least the UE identity and the encrypted first random number to a core network entity;

receive a first authentication data from the core network entity; and

10 authenticate the core network entity by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique.

With reference to the eighth aspect, in a first possible implementation manner of the eighth aspect, the processor is further configured to:

15 verify one of a message authentication code (MAC) and a signature included in the first authentication data to generate an authentication result; and

transmit the authentication result to the core network entity.

With reference to the eighth aspect, in a second possible implementation manner of the eighth aspect, the processor is further configured to:

20 generate a second authentication data based at least on a second random number included in the first authentication data; and

authenticate the core network entity successfully when a first authentication token (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data meet a preset condition (for example, the first AUTN and the second AUTN are equal).

With reference to the second possible implementation manner of the eighth aspect, in a third possible implementation manner of the eighth aspect, the processor is further configured to:

- 5 generate the second authentication data based at least on the second random number and a symmetric key shared between the UE and a Home Subscriber Server (HSS) in the core network entity.

With reference to any one of the eighth aspect, the first to the third possible implementation manner of the eighth aspect, in a fourth possible implementation manner of the eighth aspect, the processor is further configured to:

- 10 generate a message authentication code (MAC) based at least on a symmetric key shared between the UE and the core network entity;

transmit the message authentication code (MAC) to the core network entity.

With reference to the eighth aspect, in a fifth possible implementation manner of the eighth aspect, the processor is further configured to:

- 15 generate a first signature based at least on a first secret key retrieved from the UE;

transmit the first signature to the core network entity;

receive a second signature and an encrypted second random number from the core network entity;

- 20 decrypt the encrypted second random number by using the secret key;

verify the second signature by using the public key; and

generate a session key based on the first random number and the decrypted second random number.

- 25 With reference to the eighth aspect, in a sixth possible implementation manner of the eighth aspect, the processor is further configured to:

receive a first message authentication code (MAC);

generate a second message authentication code (MAC) based at least on a first Diffie-Hellman public key included in the first authentication data; and

5 authenticate the core network entity successfully when the first MAC and the second MAC are equal.

According to a ninth aspect of the invention, a first core network entity comprises a processor; and a storage medium communicably coupled thereto and storing instructions which are executable by the processor to cause the processor to:

10 receive at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

generate an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

transmit the authentication vector to a second core network entity.

15 With reference to the ninth aspect, in a first possible implementation manner of the ninth aspect, the processor is further configured to:

receive the decrypted first random number from the second core network entity;

20 generate the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

25 transmit at least the network authentication token (AUTN) and the expected result value (XRES).

With reference to the ninth aspect, in a second possible implementation manner of the ninth aspect, the processor is further configured to: before generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number,

- 5 decrypt the encrypted first random number with a private key by using at least asymmetric key technique, wherein the private key is retrieved from the first core network entity based on the UE identity.

With reference to any one of the ninth aspect, in a third possible implementation manner of the ninth aspect, the first core network entity includes
10 Home Subscriber Server (HSS).

In another aspect of the invention, a first core network entity comprises a processor; and a storage medium communicably coupled thereto and storing instructions which are executable by the processor to cause the processor to:

- 15 receive at least a user equipment (UE) identity and decrypted first random number from the second core network entity;

 generate an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

 transmit the authentication vector to a second core network entity.

- 20 the processor is further configured to: wherein generate an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number comprises:

- 25 generate the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value

(XRES); wherein transmit the authentication vector to a second core network entity comprises:

transmit at least the network authentication token (AUTN) and the expected result value (XRES).

5 the processor is further configured to:

decrypt the encrypted first random number with a private key which is retrieved from the first core network entity based on the UE identity, by using at least asymmetric key technique, wherein the first core network entity includes Home Subscriber Server (HSS).

10 According to a tenth aspect of the invention, a second core network entity comprises a processor; and a storage medium communicably coupled thereto and storing instructions which are executable by the processor to cause the processor to:
receive at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

15 decrypt the encrypted first random number with a private key by using at least asymmetric key techniques, wherein the private key is retrieved from the second core network entity based on the UE identity;

transmit an authentication vector request to a first core network entity, wherein the authentication vector request includes the UE identity and the decrypted
20 first random number;

receive an authentication vector from the first core network entity; and

transmit the authentication vector to the UE.

With reference to the tenth aspect, in a first possible implementation manner of the tenth aspect, the first core network entity includes Home Subscriber Server
25 (HSS) and the second core network entity includes one of Mobility Management Entity (MME) and Authentication, Authorization and Accounting (AAA) server.

In another aspect, a method for authentication and key generation in a cellular network, comprising:

receiving, at a Home Subscriber Server (HSS), at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE
5 associated with the UE identity;

decrypting, at the HSS, based at least on asymmetric key technique, the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity;

generating, at the HSS, an authentication vector based at least on the
10 decrypted first random number; and

transmitting, at the HSS, the authentication vector which is destined for the UE for authentication of the core network entity.

In another aspect, a method for authentication and key generation in a cellular network, comprising:

15 receiving, at a Home Subscriber Server (HSS), at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

decrypting, at the HSS, based at least on asymmetric key technique, the encrypted first random number with a private key which is retrieved from the core
20 network entity based on the UE identity;

generating, at the HSS, an authentication vector based at least on the decrypted first random number; and

transmitting, at the HSS, the authentication vector to a Mobility Management Entity (MME);

25 transmitting, at the MME, the authentication vector which is destined for the UE for authentication of the core network entity.

Brief Description of the Drawings

Embodiments of the invention are disclosed hereinafter with reference to the drawings, in which:

Figure 1 shows an existing authentication signaling exchanging procedure;

5 Figure 2 shows key architecture of the Long-Term Evolution (LTE) network;

Figure 3 shows a Diffie-Hellman procedure;

Figure 4 is a flow chart illustrating a method for mutual authentication between UE and CN using a pair of asymmetric keys according to one embodiment of the invention;

10 Figure 5 is a flow chart illustrating a method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of asymmetric keys according to one embodiment of the invention;

Figure 6 is a flow chart illustrating a method for mutual authentication between UE and CN using a pair of asymmetric keys together with a symmetric key;

15 Figure 7 is a flow chart illustrating a method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of asymmetric keys together with a symmetric key according to one embodiment of the invention;

Figure 8 is a flow chart illustrating an alternative method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of asymmetric keys together with a symmetric key according to one embodiment of the invention;

20 Figure 9 is a flow chart illustrating a method for mutual authentication between UE and CN using two pairs of asymmetric keys according to one embodiment;

Figure 10 is a flow chart illustrating a method for mutual authentication between UE and CN using a pair of asymmetric keys and Diffie-Hellman procedure according to one embodiment;

Figure 11 shows a network architecture of 3G/4G network system where embodiments of the invention may be applied; and

30 Figure 12 is a schematic system representation showing functional modules for supporting embodiments of the invention.

Detailed Description

In the following description, numerous specific details are set forth in order to provide a thorough understanding of various illustrative embodiments of the invention. It will be understood, however, to one skilled in the art, that embodiments of the invention may be practiced without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure pertinent aspects of embodiments being described. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

As used in the description and claims, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common element, merely indicate that different instances of like elements are being referred to, and are not intended to imply that the elements so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

In this disclosure, the phrase "authentication vector" is comprised of a plurality of components or parameters that provide temporary authentication data that enables authentication of a core network entity and/or a UE. Examples of authentication vector (AV) components include, but are not limited to, random number (RND), network authentication token (AUTN), expected response value (XRES), master key (K_{ASME}). An authentication vector may include a plurality of components which are selected from the above-mentioned component examples and may include other suitable components. The phrase "authentication data" refers to any of the listed AV components and/or other suitable components.

Embodiments of the invention provide methods to alleviate threats resulting of exposure of credentials in the USIM card. Asymmetric key techniques are used in mutual authentication between UE and CN to prevent Man-in-the-Middle attack.

Figure 4 is a flow chart 400 illustrating a method for mutual authentication between a user equipment (UE) and a core network (CN) using a pair of asymmetric keys according to one embodiment of the invention.

UE and CN jointly own a pair of asymmetric keys, i.e. public key PKx and

private key SK_x . PK_x is stored in the USIM card of a UE and may be referred to as UE-public key. The USIM card may be either a normal USIM card or an eUICC. SK_x is stored at the CN and may be referred to as CN-private key. Each UE may own multiple unique pairs of keys.

5 In block 401, UE attempts to access the network and activates mutual authentication procedure with CN. UE generates a random number RND_{UE} , i.e. a UE-derived random parameter, and a first message authentication code MAC_{UE} , i.e. first UE-derived MAC (optional). The first MAC_{UE} may be generated with the RND_{UE} and a sequence number SQN (optional) as inputs to a predefined hash function. UE
10 further encrypts RND_{UE} , MAC_{UE} , and SQN with the UE-public key PK_x . SQN and MAC_{UE} are optional; one or both of them may be omitted from encryption and subsequent steps. The MAC_{UE} can be generated with a hash function known to both UE and core network entity, for example, SHA256.

 In block 402, UE transmits a first message to CN. The first message includes
15 an identity of the UE, i.e. UE identity, the UE-encrypted RND_{UE} , first MAC_{UE} and SQN which are generated in block 401. UE identity may be IMSI, GUTI or other suitable parameters.

 In block 403, CN receives the first message and commences authentication of UE. Particularly, a core network entity, e.g. HSS/ Authentication, Authorization and
20 Accounting (AAA)/controller, retrieves the private key SK_x based on the UE identity provided in the first message. The private key SK_x may be stored at the network entity. The network entity decodes or decrypts the RND_{UE} , SQN and MAC_{UE} . The network entity generates a first MAC_{CN} , i.e. first CN-derived MAC, with the decrypted RND_{UE} and SQN as inputs. The MAC_{CN} can be generated with a hash function
25 known to both UE and core network entity, for example, SHA256.

 The network entity compares the first MAC_{CN} which is generated by the network entity with the first MAC_{CN} which is contained in the first message. If the first MAC_{CN} and the first MAC_{UE} are equal, i.e. have same values, CN successfully authenticates UE.

30 In block 403, after authenticating the UE, the network entity generates a second message for UE to authenticate the CN. The second message contains parameters for key generation and a second MAC_{CN} , i.e. second CN-derived MAC, or a signature. The second MAC_{CN} or signature is generated based at least on the

decrypted RND_{UE} as input. SK_x is used when signature is generated. The network entity of CN may also generate a random number RND_{CN} i.e. a CN-derived random parameter, and include it in both the parameters list and also in the second MAC_{CN} or signature generation.

5 In block 404, the network entity of CN, e.g. MME/AAA/controller, transmits the second message to UE for authentication of CN.

 In block 405, after receiving the second message from CN, UE extracts parameters from the second message, and verifies the MAC or signature contained in the message. PK_x of the UE is used when a signature is contained in the second
10 message. If the verification succeeds, CN is successfully authenticated. Otherwise, authentication of CN fails.

 In block 406, based on the authentication result of block 405, UE transmits a third message to CN. The third message can contain either notification of success/failure of the authentication or a code for CN to authenticate UE.

15 In block 407, CN authenticates UE based on the code from block 406 if this authentication had not been performed in block 403.

 Figure 5 is a flow chart 500 illustrating a method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of
20 asymmetric keys according to one embodiment of the invention.

 In block 501, before transmitting an Attach Request to a Management Entity such as MME or AAA server or other network entity with similar functionalities, UE generates a random number RND_{UE} and encrypts RND_{UE} with UE-public key PK_x .

 In block 502, UE transmits an Attach Request to a Management Entity such as
25 MME, AAA server or other network entity with similar functionalities. The Attach Request includes UE identity, the encrypted RND_{UE} and possibly other parameters such as SQN and a first MAC_{UE} generated based on RND_{UE} . The first MAC_{UE} can be generated with a hash function known to both UE and core network entity, for example, SHA256.

30 In block 503, after Management Entity receives the Attach Request, it further generates a message, for example, an Authentication Data Request message as specified in the 3GPP specification, with the UE identity and encrypted RND_{UE} extracted from the Attach Request, and transmits the Authentication Data Request,

to HSS.

In block 504, after receiving the message from the Management Entity, HSS retrieves or locates the CN-private key SK_x based on either the UE identity such as IMSI, GUTI, or other identity information. HSS decrypts the Authentication Data Request to obtain a decrypted RND_{UE} . HSS may verify the validity of the RND_{UE} based on the received MAC if a MAC is contained in the message. HSS generates a first MAC_{CN} , i.e. first CN-derived MAC, with the decrypted RND_{UE} and SQN as inputs. The first MAC_{CN} can be generated with a hash function known to both UE and core network entity, for example, SHA256. HSS generates CN-derived random number RND_{CN} , and uses RND_{CN} , RND_{UE} or a value derived from RND_{UE} , together with any SQN (optional), SN_ID (optional) as inputs to a Key Derive Function, for example, EPS-AKA algorithm defined in the LTE specification, to generate authentication vectors. Each Authentication Vector (AV) includes RND_{CN} , HSS-derived network authentication token $AUTN_{HSS}$, expected result value XRES, and key K_{ASME} .

In block 505, HSS transmits an Authentication Data Response message with the generated AV to the Management Entity.

In block 506, after receiving the generated AV, the Management Entity generates and transmits an Authentication Request to be sent to UE, which contains RND_{CN} and $AUTN_{HSS}$.

In block 507, after receiving the Authentication Request, UE extracts RND_{CN} and $AUTN_{HSS}$ from the Authentication Request message received from network. USIM/eUICC in the UE generates UE-derived network authentication token $AUTN_{UE}$ by inputting RND_{CN} , RND_{UE} , SN ID and SQN to the LTE AKA Algorithm. UE compares the $AUTN_{UE}$ with $AUTN_{HSS}$. If $AUTN_{UE}$ and $AUTN_{HSS}$ are equal, UE successfully authenticates CN. Otherwise, authentication of CN fails.

In block 508, UE transmits a response code RES based on the authentication result in block 508 to the Management Entity such as MME, AAA, controller other network entity with similar functionality.

In block 509, the Management Entity compares the RES with XRES. If RES and XRES values are equal, UE is successfully authenticated. Otherwise, authentication of UE fails.

Figure 6 is a flow chart 600 illustrating a method for mutual authentication

between UE and CN using a pair of asymmetric keys together with a symmetric key. A pair of symmetric keys K_{UE} is shared by UE and HSS, e.g. stored in the USIM card of the UE and in HSS. K_{UE} is unique to each UE. At the same time, UE and CN share a pair of asymmetric keys, where PK_x is stored in the USIM/eUICC of UE and also referred to as UE-public key, and SK_x is stored in HSS and also referred to as CN-private key. The pair of PK_x and SK_x may be shared by many UEs.

In block 601, UE generates a random number RND_{UE} , encrypts the RND_{UE} and SQN (optional) with the UE-public key PK_x , and generates a first MAC_{UE} with K_{UE} , UE identity, RND_{UE} , and SQN as input. SQN may be optional for encryption and MAC calculation.

In block 602, UE sends a first message to CN. The first message includes an identity of the UE, i.e. UE identity, the UE-encrypted RND_{UE} and SQN, and first MAC_{UE} .

In block 603, after receiving first message, a network entity at the CN, e.g. MME or HSS, decrypts the message with CN-private key SK_x and extracts RND_{UE} and any SQN. The network entity calculates a first MAC_{CN} based on K_{UE} and the decrypted RND_{UE} , SQN and UE identity and compares the first MAC_{CN} with first MAC_{UE} received at the CN. If the first MAC_{CN} and first MAC_{UE} are equal, UE is successfully authenticated. Otherwise, authentication of UE fails.

In block 603, the network entity generates authentication vectors. Each authentication vector includes RND_{CN} , $AUTN_{CN}$ and other parameters. The generation of authentication vectors is based on RND_{UE} , RND_{CN} , K_{UE} , SQN and other parameters in consideration.

In block 604, CN transmits a second message which includes RND_{CN} , and $AUTN_{CN}$.

In block 605, after receiving the second message, UE extracts the RND_{CN} , and $AUTN_{CN}$. UE generates $AUTN_{UE}$. The generation of $AUTN_{UE}$ takes RND_{UE} , RND_{CN} , K_{UE} , SQN and other parameters in consideration. If the generated $AUTN_{UE}$ and the received $AUTN_{CN}$ are equal, the CN is successfully authenticated. Otherwise, authentication of CN fails.

In block 606, when MAC_{UE} is not included in the first message, UE sends a third message containing RES code to the CN to authenticate UE.

In block 607, CN authenticates UE with RES code received.

Figure 7 is a flow chart 700 illustrating a method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of asymmetric keys together with a symmetric key according to one embodiment of the invention. The symmetric key is shared by HSS and UE.

In block 701, before transmitting an Attach Request to a network entity such as MME or AAA server or other network entity with similar functionalities, UE generates a random number RND_{UE} and encrypts RND_{UE} with the UE-public key.

In block 702, the UE transmits an Attach Request which includes UE identity and RND_{UE} which is encrypted by the PKx. The Attach Request includes the encrypted RND_{UE} and other parameters.

In block 703, after the Management Entity receives the Attach Request, it generates another message, for example, an Authentication Data Request message, with the UE identity and encrypted RND_{UE} extracted from the Attach Request and transmits the Authentication Data Request to HSS.

In block 704, HSS retrieves or locates the CN-private key SKx based on the UE identity in the Authentication Data Request and decrypts the Authentication Data Request to obtain a decrypted RND_{UE} . HSS generates CN-derived RND_{CN} , and further generates a new number based on both RND_{CN} and decrypted RND_{UE} , for example, generating the new random number by performing an Exclusive-or function (XOR) on RND_{CN} and RND_{UE} , together with K_{UE} , SQN, SN ID as inputs to EPS-AKA algorithm defined in the LTE specification to generate authentication vectors. Each authentication vector includes RND_{CN} , HSS-derived $AUTN_{HSS}$, XRES, and K_{ASME} .

In block 705, HSS transmits an Authentication Data Response message with the generated AV to the Management Entity.

In block 706, after receiving the generated AV, the Management Entity generates and transmits an Authentication Request to UE, which contains RND_{CN} and $AUTN_{HSS}$.

In block 707, after receiving the Authentication Request, UE extracts RND_{CN} and $AUTN_{HSS}$ from the Authentication Request message received from network. USIM/eUICC in the UE generates UE-derived network authentication token $AUTN_{UE}$ by inputting K_{UE} , RND_{CN} , RND_{UE} , SN ID and SQN to the LTE AKA Algorithm. RND_{CN}

and RND_{UE} are used to generate a new number as an input for EPS-AKA algorithm. For example, the random number can be $RND_{UE} \text{ XOR } RND_{CN}$.

In block 708, UE compares the $AUTN_{UE}$ with $AUTN_{HSS}$. If $AUTN_{UE}$ and $AUTN_{HSS}$ are equal, CN is successfully authenticated.

5 In block 709, UE transmits a response code RES based on the authentication result in block 708 to the Management Entity.

In block 710, the Management Entity compares the RES with XRES. If RES and XRES values are equal, UE is successfully authenticated. Otherwise, authentication of UE fails.

10

Figure 8 is a flow chart 800 illustrating another method for mutual authentication between UE and CN in LTE network or its evolved version using a pair of asymmetric keys together with a symmetric key according to one embodiment of the invention. The symmetric key is shared by Management Entity and UE.

15 In block 801, before transmitting an Attach Request to a management entity such as MME or AAA server or other network entity with similar functionalities, UE generates a random number RND_{UE} and encrypts RND_{UE} with the UE-public key.

In block 802, the UE transmits to Management Entity an Attach Request which includes UE identity and RND_{UE} encrypted by the PKx. The Attach Request includes
20 the encrypted RND_{UE} and other parameters. In another embodiment, UE may encrypt UE identity and RND_{UE} with the PKx.

In block 803, after the Management Entity receives the Attach Request, it retrieves or locates the CN-private key SKx based on the UE identity in the Attach Request and decrypts the Attach Request to obtain a decrypted RND_{UE} . In another
25 embodiment, Management Entity decrypts both the UE identity and RND_{UE} included in the received Attach Request.

In block 804, the Management Entity generates an Authentication Data Request message with the UE identity and decrypted RND_{UE} and transmits the Authentication Data Request to HSS.

30 In block 805, HSS extracts RND_{UE} from the Authentication Data Request. HSS generates CN-derived RND_{CN} , and further derives a new random number based on both RND_{CN} and RND_{UE} , for example, generating the new random number by performing an Exclusive-or function (XOR) on RND_{CN} and RND_{UE} , together with K_{UE} ,

SQN, SN ID as inputs to EPS-AKA algorithm defined in the LTE specification to generate authentication vectors. Each authentication vector includes RND_{CN} , HSS-derived $AUTN_{HSS}$, XRES, and K_{ASME} .

5 In block 806, HSS transmits an Authentication Data Response message with the generated AV to the Management Entity.

In block 807, after receiving the generated AV, the Management Entity generates and transmits an Authentication Request to UE, which contains RND_{CN} and $AUTN_{HSS}$.

10 In block 808, after receiving the Authentication Request, UE extracts RND_{CN} and $AUTN_{HSS}$ from the Authentication Request message received from network. USIM/eUICC in the UE generates UE-derived network authentication token $AUTN_{UE}$ by inputting K_{UE} , RND_{CN} , RND_{UE} , SN ID and SQN to the LTE AKA Algorithm. RND_{CN} and RND_{UE} are used to generate a new random number as an input for EPS-AKA algorithm. For example, the new random number can be $RND_{UE} \text{ XOR } RND_{CN}$.

15 In block 809, UE compares the $AUTN_{UE}$ with $AUTN_{HSS}$. If $AUTN_{UE}$ and $AUTN_{HSS}$ are equal, UE successfully authenticates CN. Otherwise, authentication of the CN fails.

In block 810, UE transmits a response code RES based on the authentication result in block 809 to the Management Entity.

20 In block 811, the Management Entity compares the RES with XRES. If RES and XRES values are equal, UE is successfully authenticated. Otherwise, authentication of UE fails.

Figure 9 is a flow chart 900 illustrating a method for mutual authentication
25 between UE and CN using two pairs of asymmetric keys according to one embodiment. UE is assigned a pair of asymmetric keys, i.e. UE-public key PK_{UE} and UE-private key SK_{UE} , which are different from other UEs. CN is assigned a pair of asymmetric keys, i.e. CN-public key PK_{CN} and CN-private key SK_{CN} . The CN has two choices: the CN may be assigned a pair of asymmetric keys that apply to all UEs, or
30 the CN may be assigned different pairs of asymmetric keys for different UEs. The UICC card of UE stores CN-public key PK_{CN} and UE-private key SK_{UE} ; while a network entity in CN such as MME or HSS stores the UE-public key PK_{UE} and CN-private key SK_{CN} .

In block 901, before sending a first message from UE to CN, UE generates a random number RND_{UE} . UE encrypts the RND_{UE} and SQN_1 (optional) using CN-public key PK_{CN} , and generates a signature by signing UE identity, RND_{UE} , and SQN_1 using UE-private key SK_{UE} . SQN_1 may be optional in encryption and signature generation.

In block 902, UE transmits a first message to CN. The first message includes UE identity, the UE-encrypted RND_{UE} and SQN_1 , and UE-generated signature.

In block 903, after receiving the first message, CN decrypts the first message using CN-private key SK_{CN} and extracts RND_{UE} and any SQN_1 . CN also verifies the signature in the first message by using PK_{UE} which is stored at CN and retrieved therefrom based on the UE identity. If the signature is correct, UE is successfully authenticated. CN generates a random number RND_{CN} , encrypts RND_{CN} and any SQN_2 using the UE-public key PK_{UE} , and signs the RND_{UE} , RND_{CN} and SQN_2 using CN-private key SK_{CN} . CN may generate session keys based on the RND_{CN} and RND_{UE} .

In block 904, CN transmits a second message to UE. The second message includes CN-generated signature, and the CN-encrypted RND_{CN} and SQN_1 .

In block 905, after receiving the second message, UE decrypts the second message using UE-private key PK_{UE} to extract RND_{CN} and any SQN_2 . UE verifies the received signature. If the signature is correct, CN is successfully authenticated. Otherwise, authentication of CN fails.

In block 906, UE transmits or returns a confirmation information to CN.

Figure 10 is a flow chart illustrating a method for mutual authentication between UE and CN and embedding Diffie-Hellman procedure in the authentication. UE and CN share a pair of asymmetric keys, where PK_x is stored in the USIM/eUICC of UE and also referred to as UE-public key, and SK_x is stored in core network entity or HSS and also referred to as CN-private key. The pair of PK_x and SK_x can be unique to the UE.

In block 1001, UE generates a random number RND_{UE} . Using PK_x , UE encrypts the RND_{UE} and a sequence number SQN (optional). Using PK_x , UE generates a first MAC_{UE} based on RND_{UE} and SQN (optional). UE also generates a

key $K_{\text{RND-UE}}$ based on RND_{UE} . One embodiment is to input RND_{UE} to a KDF function to derive the key K_{RND} .

In block 1002, UE sends a first message to the core network entity. The first message includes UE identity and the encrypted RND_{UE} , SQN and the first MAC_{UE} .

5 In block 1003, after receiving the first message from UE, the CN first retrieves or locates a private key SK_x based on the UE identity received in the first message and then decrypts the RND_{UE} , SQN and first MAC_{UE} with the private key SK_x . CN authenticates the UE based on the decrypted RND_{UE} , SQN and first MAC_{UE} , or validates the received RND_{UE} with MAC and SQN. After authenticating the UE, CN
10 generates a key $K_{\text{RND-CN}}$ based on the decrypted RND_{UE} . CN further generates a Diffie-Hellman public key g^x , where x is a random number.

CN encrypts SQN by $K_{\text{RND-CN}}$, and generates a first MAC_{CN} which is based on SQN and g^x and using $K_{\text{RND-CN}}$.

15 In block 1004, CN sends a second message to the UE, which includes the encrypted SQN, g^x , and the first MAC_{CN} generated in block 1003.

In block 1005, after receiving the second message, UE decrypts the SQN with $K_{\text{RND-UE}}$ which was generated with RND_{UE} at the UE side in block 1001, and calculates a second MAC_{UE} based on both SQN and g^x as inputs. If the second MAC_{UE} generated by UE and the first MAC_{CN} received in the second message are
20 equal, CN is successfully authenticated. Otherwise, authentication of CN fails.

In block 1006, UE generates a Diffie-Hellman public key, g^y , where y is a random number, and sends a third message to CN. The third message includes SQN', encrypted by $K_{\text{RND-UE}}$, a third MAC_{UE} which is generated with SQN and g^y using $K_{\text{RND-UE}}$, and g^y . SQN and g^y are encrypted using $K_{\text{RND-UE}}$.

25 In block 1007, CN may further authenticate UE based on the received third MAC_{UE} and the first MAC_{CN} , and generate a session key based on $K_{\text{RND-CN}}$ and Diffie-Hellman public key, g^y .

The above-described methods for mutual authentication of CN and UE may
30 be implemented in a system specified by the 3G/4G specification or a system evolved from the system specified by the 3G/4G specification which is defined by the 3GPP standard organization. Figure 11 shows network architecture of 3G/4G network system.

Figure 12 is a schematic system representation showing functional modules for supporting the above-described methods. Particularly, UE is provided with asymmetric and/or symmetric key(s), encryption and/or decryption unit, DH procedure unit, key generation unit, random number generation unit, authentication data generation unit, authentication unit, communication unit. E-UTRAN is provided with key generation unit. Management Entity (MME/AAA) is provided with asymmetric and/or symmetric key(s), encryption and/or decryption unit, DH procedure unit, key generation unit, random number generation unit, authentication unit, communication unit. HSS is provided with asymmetric and/or symmetric key(s), encryption and/or decryption unit, DH procedure unit, key generation unit, random number generation unit, authentication vector generation unit, authentication unit, communication unit. Each of the UE, Management Entity and HSS are provided with transmitting unit and receiving unit which comprise the communication unit. It is to be appreciated that the UE/Management Entity/HSS may be provided with some or all of the respectively-listed units depending on requirements. It is to be appreciated that each listed unit may be incorporated with another listed unit.

With reference to the CN of Figure 12 and in accordance with Figures 4 to 10, a system for authentication and key generation is provided, the system comprising: a receiving unit configured to: receive, at a core network entity, at least a user equipment (UE) identity and an encrypted first random number which is generated by the UE; a decryption unit configured to: using at least asymmetric key techniques, decrypt the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity; an authentication vector generating unit configured to: generate an authentication vector based at least on the decrypted first random number; and a transmitting unit configured to: transmit the authentication vector which is destined for the UE for authentication of the core network entity.

With reference to the CN of Figure 12 and in accordance with Figure 4, the receiving unit is further configured to: receive a first message authentication code

(MAC); the authentication vector generation unit is further configured to: generate a second message authentication code (MAC) based at least on the decrypted random number; wherein the system further comprising an authentication unit configured to: successfully authenticate the UE if the first MAC and the second MAC are equal. As
5 an additional option, the transmitting unit is further configured to: generate one of a third message authentication code (MAC) and a signature based at least on the decrypted random number; and transmit the one of the second MAC and the signature.

10 With reference to the CN of Figure 12 and in accordance with Figure 6, the authentication vector generation unit is further configured to: generate the second message authentication code (MAC) further based on a symmetric key which is shared by the core network entity and the UE.

With reference to the CN of Figure 12 and in accordance with Figure 5, the decryption unit is provided at a Home Subscriber Server (HSS); the system further
15 comprises: a random number generation unit configured to: generate, at the HSS, a second random number; the authentication vector generation unit is further configured to: generate, at the HSS, the authentication vector further based on the first random number received from UE and the second random number generated, wherein the authentication vector includes a network authentication token (AUTN)
20 and an expected result value (XRES); the transmitting unit is further configured to: transmit, to a management entity, at least the network authentication token (AUTN) and the expected result value (XRES); and wherein the system further comprises: an authentication unit configured to: at the management entity, receive from the UE a response value (RES), and successfully authenticate the UE if the response value
25 (RES) and expected result value (XRES) are equal.

With reference to the CN of Figure 12 and in accordance with Figure 7, the authentication vector generating unit is further configured to: generate, at a Home Subscriber Server (HSS), the authentication vector further based on a symmetric key which is shared by the HSS and the UE.

30 With reference to the CN of Figure 12 and in accordance with Figure 8, the decryption unit is provided at a management entity; the system further comprises: a

random number generation unit configured to: generate, at the HSS, a second random number; the authentication vector generation unit is further configured to: generate, at a Home Subscriber Server (HSS), the authentication vector further based on the second random number and a symmetric key which is shared by the HSS and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES); the transmitting unit is further configured to: transmit, to a management entity, at least the network authentication token (AUTN) and the expected result value (XRES); and the system further comprises: an authentication unit configured to: at the management entity, receive from the UE a response value (RES), and successfully authenticating the UE if the response value (RES) and expected result value (XRES) are equal.

With reference to the CN of Figure 12 and in accordance with Figure 9, the receiving unit is further configured to: receive a signature; the system further comprises: a random number generation unit configured to: generate a second random number; the authentication vector generation unit is further configured to: using a public key which is retrieved from the core network entity based on the UE identity, encrypt at least the second random number; and using a private key which is associated with the core network entity and retrieved therefrom, sign at least the second random number; and the system further comprises: an authentication unit further configured to: verify the received signature.

With reference to the CN of Figure 12 and in accordance with Figure 10, the receiving unit is further configured to: receive a first message authentication code (MAC); the authentication vector generation unit is further configured to: generate a first key ($K_{\text{RND-CN}}$) based on the decrypted first random number; generate a first Diffie-Hellman public key (g^x); using the first key ($K_{\text{RND-CN}}$), generate a second message authentication code (MAC) based at least on the first Diffie-Hellman public key (g^x); the transmitting unit is further configured to: transmit at least the second message authentication code; the system further comprises: a Diffie-Hellman procedure unit configured to: receive a second Diffie-Hellman public key (g^y); generate a second key based on the Diffie-Hellman public key (g^y). As an additional option, the Diffie-Hellman procedure unit is further configured to: generate a session key based on the first key and the second key.

With reference to the UE of Figure 12 and in accordance with Figures 4 to 10, a system for authentication and key generation in a cellular network is provided, the system comprising: a random number generation unit configured to: generate, at a user equipment (UE), a first random number; an encryption-decryption unit
5 configured to: encrypt the first random number with a public key retrieved from the UE; a transmitting unit configured to: transmit at least a UE identity and the encrypted first random number to a core network entity; a receiving unit configured to: receive a first authentication data from the core network entity; and an authentication unit configured to: using at least one of symmetric key and asymmetric key
10 techniques, authenticate the core network entity by verifying the first authentication data.

With reference to the UE of Figure 12 and in accordance with Figure 4, the authentication unit is further configured to: verify one of a message authentication code (MAC) and a signature included in the first authentication data to generate an
15 authentication result; and transmit the authentication result to the core network entity.

With reference to the UE of Figure 12 and in accordance with Figure 5, the authentication unit is further configured to: generate a second authentication data based at least on a second random number included in the first authentication data; and successfully authenticate the core network entity if a first authentication token
20 (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data are equal.

With reference to the UE of Figure 12 and in accordance with Figure 6, the system further comprises: an authentication data generation unit configured to: generate a message authentication code (MAC) based at least on a symmetric key
25 shared by the UE and the core network entity; the transmitting unit is further configured to: transmit the message authentication code to the core network entity.

With reference to the UE of Figure 12 and in accordance with Figure 6, the system further comprises: an authentication data generation unit configured to: generate a message authentication code (MAC) based at least on a hash function
30 shared by the UE and the core network entity; wherein the transmitting unit is further configured to: transmit the message authentication code to the core network entity.

With reference to the UE of Figure 12 and in accordance with Figures 7 and 8, the authentication unit is further configured to: generate the second authentication data further based on a symmetric key shared by the UE and a Home Subscriber Server (HSS) in the core network entity.

- 5 With reference to the UE of Figure 12 and in accordance with Figure 9, the encryption-decryption unit is further configured to: generate a first signature based at least on a first secret key retrieved from the UE; the transmitting unit is configured to: transmit the first signature; the receiving unit is further configured to: receive a second signature and an encrypted second random number; the
- 10 encryption-decryption unit is further configured to: using the secret key, decrypt the encrypted second random number; the authentication unit is further configured to: using the public key, verify the second signature; and the system further comprises: a key generation unit configured to: generate a session key based on the first random number and the decrypted second random number.
- 15 With reference to the UE of Figure 12 and in accordance with Figure 10, the receiving unit is further configured to: receive a first message authentication code (MAC); the authentication unit is further configured to: generate a second message authentication code (MAC) based at least on a first Diffie-Hellman public key included in the first authentication data; and successfully authenticate the core
- 20 network entity if the first MAC and the second MAC are equal.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity, and not to limit the

25 disclosed embodiments of the invention. The embodiments and features described above should be considered exemplary.

Claims:

1. A method for authentication and key generation in a cellular network, comprising:

receiving, at a core network entity, at least a user equipment (UE) identity and
5 an encrypted first random number which is generated by a UE associated with the
UE identity;

decrypting, by the core network entity, based at least on asymmetric key
technique, the encrypted first random number with a private key which is retrieved
from the core network entity based on the UE identity;

10 generating, by the core network entity, an authentication vector based at least
on the decrypted first random number; and

transmitting, by the core network entity, the authentication vector which is
destined for the UE for authentication of the core network entity.

2. The method of claim 1, further comprising:

15 receiving a first message authentication code (MAC) from the UE;

generating a second MAC based at least on the decrypted first random
number;

authenticating the UE successfully when the first MAC and the second MAC
meet a preset condition.

20 3. The method of claim 2, wherein generating a second message authentication
code (MAC) based at least on the decrypted first random number comprises:

generating the second MAC based at least on the decrypted first random
number and a symmetric key which is shared between the core network entity and
the UE.

25 4. The method of claim 2, wherein generating a second message authentication
code (MAC) based at least on the decrypted first random number comprises:

generating the second MAC based at least on the decrypted first random number and a hash function which is shared between the core network entity and the UE.

5. The method of any one of claims 1-4, further comprising:

5 generating one of a third MAC and a signature based at least on the decrypted first random number;

transmitting, from the core network entity to the UE, the one of the generated third MAC or the signature.

6. A method for authentication and key generation in a cellular network, the method
10 comprising:

generating, at a user equipment (UE), a first random number and encrypting the first random number with a public key which is retrieved from a UE and associated with a UE identity;

15 transmitting at least the UE identity and the encrypted first random number to a core network entity which is configured to decrypt the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity;

receiving a first authentication data from the core network entity; and

20 authenticating the core network entity by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique.

7. The method of claim 6, wherein authenticating the core network by verifying the first authentication data comprises:

verifying one of a message authentication code (MAC) and a signature included in the first authentication data to generate an authentication result; and

25 transmitting the authentication result to the core network entity.

8. The method of claim 6, wherein authenticating the core network entity by verifying the first authentication data comprises:

generating a second authentication data based at least on a second random number included in the first authentication data; and

5 authenticating the core network entity successfully when a first authentication token (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data meet a preset condition.

9. The method of claim 8, wherein generating a second authentication data based at least on a second random number included in the first authentication data comprises:

10 generating the second authentication data based at least on the second random number and a symmetric key shared between the UE and a Home Subscriber Server (HSS) in the core network entity.

10. The method of any one of claims 6 to 9, further comprising:

15 generating a message authentication code (MAC) based at least on a symmetric key shared between the UE and the core network entity;

transmitting the message authentication code (MAC) to the core network entity.

11. The method of claim 6, further comprising:

20 generating a first signature based at least on a first secret key retrieved from the UE;

transmitting the first signature to the core network entity;

receiving a second signature and an encrypted second random number from the core network entity;

25 wherein authenticating the core network by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique, comprises:

decrypting the encrypted second random number by using a secret key;

verifying the second signature by using the public key; and

generating a session key based on the first random number and the decrypted second random number.

5 12. The method of claim 6, further comprising:

receiving a first message authentication code (MAC);

wherein authenticating the core network entity by verifying the first authentication data comprises:

generating a second message authentication code (MAC) based at least on a
10 first Diffie-Hellman public key included in the first authentication data; and

authenticating the core network entity successfully when the first MAC and the second MAC are equal.

13. A system for authentication and key generation in a cellular network, the system comprising:

15 a random number generation unit configured to: generate, at a user equipment (UE), a first random number;

an encryption-decryption unit configured to: encrypt the first random number with a public key retrieved from the UE, wherein the public key is based on a UE identity associated with the UE ;

20 a transmitting unit configured to: transmit at least the UE identity and the encrypted first random number to a core network entity which is configured to decrypt the encrypted first random number with a private key which is retrieved from the core network entity based on the UE identity;

a receiving unit configured to: receive a first authentication data from the core
25 network entity; and

an authentication unit configured to: authenticate the core network entity by verifying the first authentication data by using at least one of symmetric key and asymmetric key technique.

14. The system of claim 13, wherein the authentication unit is further configured to:

5 verify one of a message authentication code (MAC) and a signature included in the first authentication data to generate an authentication result; and

transmit the authentication result to the core network entity.

15. The system of claim 13, wherein the authentication unit is further configured to:

10 generate a second authentication data based at least on a second random number included in the first authentication data; and

authenticate the core network entity successfully when a first authentication token (AUTN) included in the first authentication data and a second authentication token (AUTN) included in the second authentication data meet a preset condition.

16. The system of claim 15, wherein the authentication unit is further configured to:

15 generate the second authentication data based at least on the second random number and a symmetric key shared between the UE and a Home Subscriber Server (HSS) in the core network entity.

17. A method for authentication and key generation in a cellular network, comprising:

20 at a first core network entity:

receiving at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

transmitting the authentication vector to a second core network entity which is to authenticate the UE based on a response which is generated by the UE based on the authentication vector.

18. The method of claim 17, wherein generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number comprises:

generating the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

wherein transmitting the authentication vector to a second core network entity comprises:

transmitting at least the network authentication token (AUTN) and the expected result value (XRES).

19. The method of claim 17, wherein before generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number, the method further comprising:

decrypting the encrypted first random number with a private key by using at least asymmetric key technique, wherein the private key is retrieved from the first core network entity based on the UE identity.

20. The method of any one of claims 17 to 19, wherein the first core network entity includes Home Subscriber Server (HSS).

21. A system for authentication and key generation in a cellular network, the system comprises:

a communication unit provided at a first core network entity and configured to:

receive at least a user equipment (UE) identity and an encrypted first random number which is generated by a UE associated with the UE identity;

an authentication vector generation unit provided at the first core network entity and configured to:

5 generate an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

a communication unit provided at the first core network entity and configured to:

10 transmit the authentication vector to a second core network entity which is to authenticate the UE based on a response which is generated by the UE based on the authentication vector.

22. The system of claim 21, wherein the communication unit is further configured to:

receive the decrypted first random number;

15 wherein the authentication vector generation unit is further configured to:

generate the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the the first core network entity, wherein the symmetric key is shared between the first core network entity and the UE,
20 wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

wherein the communication unit is further configured to:

transmit at least the network authentication token (AUTN) and the expected result value (XRES).

25 23. The system of claim 21, further comprising:

a decryption unit provided at the first core network entity and configured to:

before generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number, decrypt the encrypted first random number with a private key by using at least asymmetric key techniques, wherein the private key is retrieved from the first core network entity based on the UE identity.

24. A method for authentication and key generation in a cellular network, the method comprising:

at a first core network entity:

receiving at least a user equipment (UE) identity and encrypted first random number from a second core network entity;

generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number; and

transmitting the authentication vector to a second core network entity which is to authenticate a UE associated with the UE identity based on a response which is generated by the UE based on the authentication vector.

25. The method of claim 24, wherein generating an authentication vector based at least on a decrypted first random number which is obtained from the encrypted first random number comprises:

generating the authentication vector based on the decrypted first random number and at least one of a second random number and a symmetric key, wherein the second random number is generated at the HSS, wherein the symmetric key is shared between the first core network entity and the UE, wherein the authentication vector includes a network authentication token (AUTN) and an expected result value (XRES);

wherein transmitting the authentication vector to a second core network entity comprises:

transmitting at least the network authentication token (AUTN) and the expected result value (XRES).