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 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 the decrypted first random number; and

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

2. The method of claim 1, further comprising:

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.

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.

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:

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 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;

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 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

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

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:

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:

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:

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:

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.

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 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:

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

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:

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:

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:

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:

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.

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:

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.

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

receive the decrypted first random number;

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, 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).

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 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.

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).