CLAIMS

What is claimed is:

1. A secure communication method, comprising:

determining, by a communication apparatus, whether confidentiality protection is activated for communication data between user equipment and an application function device; and

sending, by the communication apparatus, a user plane message to the application function device, wherein the user plane message comprises an identifier of the user equipment, and the identifier is an encrypted identifier in a case in which the confidentiality protection is inactivated.

2. The method according to claim 1, wherein the method further comprises:

determining, by the communication apparatus, to use a procedure with privacy protection, wherein the procedure with privacy protection is used for interaction between the user equipment and the application function device.

3. The method according to claim 2, wherein the procedure with privacy protection comprises an authentication and key management for applications AKMA procedure.

4. The method according to claim 2 or 3, wherein the determining, by the communication apparatus, to use a procedure with privacy protection comprises: determining, by the communication apparatus, to use the procedure with privacy protection when one or more of the following conditions are met:

an application started by the communication apparatus indicates the communication apparatus to select the procedure with privacy protection, wherein a server of the application is comprised in the application function device;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection, and the procedure with privacy protection has a highest priority;

the communication apparatus receives an indication of preferably selecting the procedure with privacy protection;

the communication apparatus determines that the user equipment uses a 5G universal subscriber identity module;

the communication apparatus determines that the user equipment has a valid public key and a valid private key; or

the communication apparatus determines that the user plane message needs to carry a permanent identifier of the user equipment.

5. The method according to any one of claims 1 to 4, wherein the method further comprises:

receiving, by the communication apparatus, encryption algorithm information from the application function device; and

the case in which the confidentiality protection is inactivated comprises:

a case in which the encryption algorithm information indicates that an encryption algorithm is a null algorithm.

6. The method according to any one of claims 1 to 5, wherein the encrypted identifier is a subscription concealed identifier SUCI, a generic public subscription identifier GPSI, or an AKMA-key identifier A-KID.

7. The method according to any one of claims 1 to 6, wherein the user plane message is a discovery request (Discovery request) in a proximity-based service ProSe procedure.

8. A secure communication method, comprising:

determining, by a communication apparatus, to use a procedure with privacy protection, wherein the procedure with privacy protection is used for interaction between the user equipment and an application function device;

determining, by the communication apparatus based on the procedure with privacy protection, a communication key for interaction with the application function device and a non-null encryption algorithm; and

sending, by the communication apparatus, a user plane message to the application function device, wherein the user plane message comprises an identifier of the user equipment, and confidentiality protection is performed on the user plane message by using the communication key and the non-null encryption algorithm.

9. The method according to claim 8, wherein the determining, by a communication apparatus, to use a procedure with privacy protection comprises: determining, by the communication apparatus, to use the procedure with privacy protection when one or more of the following conditions are met:

an application started by the communication apparatus indicates the communication

apparatus to select the procedure with privacy protection, wherein a server of the application is comprised in the application function device;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection, and the procedure with privacy protection has a highest priority;

the communication apparatus receives an indication of preferably selecting the procedure with privacy protection;

the communication apparatus determines that the user equipment uses a 5G universal subscriber identity module;

the communication apparatus determines that the user equipment has a valid public key and a valid private key; or

the communication apparatus determines that the user plane message needs to carry a permanent identifier of the user equipment.

10. The method according to claim 8 or 9, wherein the determining, by the communication apparatus based on the procedure with privacy protection, a communication key for interaction with the application function device and a non-null encryption algorithm comprises:

generating, by the communication apparatus, the communication key based on an anchor key stored in the communication apparatus;

sending, by the communication apparatus, a request message to the application function device, wherein the request message comprises a key identifier and information indicating to use the procedure with privacy protection, and the key identifier is used to assist the application function device in obtaining the communication key; and

receiving, by the communication apparatus, a response message from the application function device, wherein the response message comprises information about the non-null encryption algorithm.

11. The method according to claim 10, wherein the request message further comprises indication information for negotiating the non-null encryption algorithm.

12. The method according to claim 10, wherein the request message further comprises information about an encryption algorithm supported by the communication apparatus, the

information about the encryption algorithm supported by the communication apparatus indicates the application function device to select a non-null encryption algorithm, and the encryption algorithm supported by the communication apparatus is a non-null encryption algorithm.

13. A secure communication method, comprising:

determining, by a communication apparatus, to use a procedure with privacy protection, wherein the procedure with privacy protection is used for interaction between user equipment and an application function device;

determining, by the communication apparatus based on the procedure with privacy protection, a communication key for interaction with the application function device; and

sending, by the communication apparatus, a user plane message to the application function device, wherein the user plane message comprises an encrypted identifier of the user equipment, and confidentiality protection is performed on the user plane message by using the communication key.

14. The method according to claim 13, wherein the procedure with privacy protection comprises an authentication and key management for applications AKMA procedure.

15. The method according to claim 13, wherein the determining, by a communication apparatus, to use a procedure with privacy protection comprises: determining, by the communication apparatus, to use the procedure with privacy protection when one or more of the following conditions are met:

an application started by the communication apparatus indicates the communication apparatus to select the procedure with privacy protection, wherein a server of the application is comprised in the application function device;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection;

the application indicates that one of a plurality of interaction procedures can be selected, wherein the plurality of interaction procedures comprise the procedure with privacy protection, and the procedure with privacy protection has a highest priority;

the communication apparatus receives an indication of preferably selecting the procedure with privacy protection;

the communication apparatus determines that the user equipment uses a 5G universal subscriber identity module;

the communication apparatus determines that the user equipment has a valid public key and a valid private key; or

the communication apparatus determines that the user plane message needs to carry a permanent identifier of the user equipment.

16. A communication apparatus, wherein the communication apparatus comprises a processing module and a transceiver module, wherein the processing module and the transceiver module are used by user equipment to perform the method according to any one of claims 1 to 7, the method according to any one of claims 8 to 12, or the method according to any one of claims 13 to 15.

17. A communication apparatus, wherein the communication apparatus comprises a processor, the processor is coupled to a memory, and the memory is configured to store a computer program, wherein when the computer program is executed by the processor, the apparatus is enabled to perform the method according to any one of claims 1 to 7, the method according to any one of claims 8 to 12, or the method according to any one of claims 13 to 15.

18. A computer-readable storage medium, storing a computer program, wherein when the computer program is executed, a computer is enabled to perform the method according to any one of claims 1 to 7, the method according to any one of claims 8 to 12, or the method according to any one of claims 13 to 15.

19. A computer program product comprising instructions, wherein when the computer program product runs on a computer, the computer is enabled to perform the method according to any one of claims 1 to 7, 8 to 12, or 13 to 15.