CLAIMS

What is claimed is:

1. A key management method, comprising:sending, by a terminal device, a protocol data unit, PDU, session modification request to an access and mobility management function, wherein the PDU session modification request comprises IP address of a multicast service;

obtaining, by the terminal device, a target key corresponding to the IP address by using a control plane message, wherein the target key comprises a target multimedia broadcast/multicast service key MSK;

receiving, by the terminal device, a multicast message from a multicast user-plane processing network element, wherein the multicast message comprises a protected part and an unprotected part, and the protected part is obtained by encrypting a target multimedia broadcast/multicast service transport key, MTK, and an identifier of the target MTK by using the target MSK;

receiving, by the terminal device, target data from a multicast user-plane processing network element, wherein the target data is data on which security protection is performed; and

processing, by the terminal device, the target data by using the target MTK.

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

receiving, by the terminal device, a security algorithm from a first network element, wherein the security algorithm comprises at least one of an encryption algorithm and an integrity protection algorithm; and

the processing, by the terminal device, the target data by using the target key comprises:

processing, by the terminal device, the target data by using the security algorithm and the target key.

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

receiving, by the terminal device, security protection status information from the first network element, wherein the security protection status information indicates a security protection status, and the security protection comprises at least one of data encryption and integrity verification; and

the processing, by the terminal device, the target data by using the target key comprises:

if the status indicated by the security protection status information is enabled, processing, by the terminal device, the target data by using the target key.

4. The method according to any one of claims 1 to 3, wherein

the obtaining, by a terminal device, a target key comprises:

receiving, by the terminal device, the target key from the first network element.

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

obtaining, by the terminal device, an identifier of the target key; and

the obtaining, by a terminal device, a target key comprises:

obtaining, by the terminal device, the target key corresponding to the identifier of the target key.

6. The method according to claim 5, wherein the obtaining, by the terminal device, an identifier of the target key comprises:

receiving, by the terminal device, the identifier of the target key from the first network element; or

receiving, by the terminal device, a key number part from the first network element; and determining, by the terminal device, the identifier of the target key based on the key number part and an identifier ID of a multicast service.

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

receiving, by the terminal device, first information from a key generation network element, wherein the first information comprises at least one of the following: an identifier of the multicast user-plane processing network element, a first parameter, or an ID of a multicast service, and the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp; and

generating, by the terminal device, a multimedia broadcast/multicast service user key MUK based on the first information and a shared key, wherein the shared key is a key shared between the terminal device and a core network device; and

the obtaining, by a terminal device, a target key comprises:

receiving, by the terminal device, key information from the multicast user-plane processing network element, wherein the key information is information obtained after the target key is encrypted by using the MUK; and

decrypting, by the terminal device, the key information by using the MUK, to obtain the target key.

8. The method according to claim 7, wherein

the shared key is an authentication server function key Kausf or a security anchor function key Kseaf.

9. The method according to any one of claims 1 to 8, wherein the processing, by the terminal device, the target data by using the target key comprises:

performing, by the terminal device, a derivation operation on the target MSK to obtain a derivation key; and

performing, by the terminal device, decryption or integrity verification on the target data by using the derivation key.

10. The method according to claim 9, wherein the performing, by the terminal device, a derivation operation on the target MSK to obtain a derivation key comprises:

performing, by the terminal device, a derivation operation on the target MSK and second information to obtain the derivation key, wherein the second information comprises at least one of the following: a protocol name, an identifier of a target multimedia broadcast/multicast service transport key MTK, or a second parameter, and the second parameter is a parameter determined based on at least one of a second sequence number and a second timestamp.

11. A key management method, comprising:

obtaining, by a key generation network element, a target key, wherein the target key comprises a target multimedia broadcast/multicast service key MSK, wherein the target MSK is used to protect a target multimedia broadcast/multicast service transport key, MTK, and the target MTK is used to protect transmission of service data;

sending, by the key generation network element, the target key to a terminal device by using a control plane message; and

sending, by the key generation network element, the target key to a multicast user-plane processing network element.

12. The method according to claim 11, wherein the method further comprises:

sending, by the key generation network element, an identifier of the target key to the multicast user-plane processing network element; or

sending, by the key generation network element, a key number part to the multicast user-plane processing network element, wherein there is a mapping relationship between the key number part and the identifier of the target key.

13. The method according to claim 11 or 12, wherein the method further comprises:

sending, by the key generation network element, at least one of the key number part, the target key, and the identifier of the target key to a terminal device, wherein there is the mapping relationship between the key number part and the identifier of the target key.

14. The method according to any one of claims 11 to 13, wherein the method further comprises:

generating, by the multicast user-plane processing network element, the target MTK and sending a multicast message to the terminal device, wherein the multicast message comprises a protected part and an unprotected part, and the protected part is obtained by encrypting the target MTK, and an identifier of the target MIK by using the target MSK;

sending, by the multicast user-plane processing network element, target data to the terminal device, and the target data is protected by using the target MTK.

15. A key management method, comprising:

receiving, by a session management function, a protocol data unit, PDU, session modification request of a terminal device from an access and mobility management function, wherein the PDU session modification request comprises IP address of a multicast service;

obtaining, by the session management function, a target key corresponding to the IP address, wherein the target key comprises a target multimedia broadcast/multicast service key MSK, wherein the target MSK is used to protect a target multimedia broadcast/multicast service transport key, MTK, and the target MIK is used to protect transmission of service data;

sending, by the session management function, the target key to the terminal device via the access and mobility management function.

16. A communication apparatus, comprising units configured to perform the steps according to any one of claims 1 to 10.

17. A communication apparatus, comprising a processor, configured to invoke a program in a memory, so that the communication apparatus performs the key management method according to any one of claims 1 to 10.

18. A communication apparatus, comprising a processor and an interface circuit, wherein the interface circuit is configured to communicate with another apparatus, and the processor is configured to perform the key management method according to any one of claims 1 to 10.

19. A communication apparatus, comprising units configured to perform the steps according to any one of claims 11 to 20.

20. A communication apparatus, comprising a processor, configured to invoke a program in a memory, so that the communication apparatus performs the key management method according to any one of claims 11 to 20.

21. A computer-readable storage medium, wherein the computer-readable storage medium stores a program; and when the program is invoked by a processor, the key management method according to any one of claims 1 to 10 is performed, the key management method according to any one of claims 11 to 14 is performed, or the key management method according to claim 15.

22. A computer program, wherein when the program is invoked by a processor, the key management method according to any one of claims 1 to 10 is performed, the key management method according to any one of claims 11 to 14 is performed, or the key management method according to claim 15 is performed.