

KEY MANAGEMENT METHOD AND COMMUNICATION APPARATUS

TECHNICAL FIELD

[0001] This application relates to the field of communication technologies, and in particular,
5 to a key management method and a communication apparatus.

BACKGROUND

[0002] To meet requirements of the real-time transport protocol (real-time transport protocol, RTP) and the file delivery over unidirectional transport (file delivery over unidirectional transport, FLUTE) protocol in a long term evolution (long term evolution, LTE) network, a multimedia
10 broadcast/multicast service (multimedia broadcast/multicast service, MBMS) uses a three-layer key system to ensure secure data transmission. As shown in FIG. 1, one terminal device corresponds to one multimedia broadcast/multicast service user key (multimedia broadcast/multicast service user key, MUK). The MUK is for encrypting a multimedia broadcast/multicast service service key (multimedia broadcast/multicast service service key, MSK)
15 to protect MSK distribution. The MSK is for encrypting a multimedia broadcast/multicast service transport key (multimedia broadcast/multicast service transport key, MTK) to protect MTK distribution. The MTK is for encrypting service data to ensure secure service data transmission. The service data and the MTK are transmitted from a network device to a terminal device in a multicast session (session).

20 [0003] However, to further optimize a broadcast/multicast service, an architecture and a procedure of a 5th generation mobile communication (5th-generation, 5G) system are different from those of an LTE network. However, security protection on MBMS service data is not defined in the 5G system. Therefore, how to perform security protection on MBMS service data is a problem that urgently needs to be resolved.

SUMMARY

[0004] Embodiments of this application provide a key management method and a communication apparatus, to simplify a procedure of secure transmission of multicast service data, and prevent an unauthorized terminal device from obtaining the multicast service data.

5 **[0005]** To achieve the foregoing objectives, the following technical solutions are used in embodiments of this application.

[0006] According to a first aspect, an embodiment of this application provides a key management method. The method may be performed by a terminal device, or may be performed by a chip used in the terminal device. The following provides descriptions by using an example in
10 which the method is performed by the terminal device. The method includes: The terminal device obtains a target key, where the target key includes at least one of a target multimedia broadcast/multicast service service key MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The terminal
15 device receives target data from a multicast user-plane processing network element, where the target data is data on which security protection is performed. Then, the terminal device processes the target data by using the target key. Herein, the multicast user-plane processing network element is one of the following network elements: a multicast/broadcast service user plane MBSU network element, a user plane function UPF network element, a user plane gateway UPGW, or a multicast
20 service function MSF network element. The security protection includes at least one of data encryption and integrity verification.

[0007] In this way, after the terminal device receives the target data of the multicast user-plane processing network element, the terminal device processes the target data by using the target key. Herein, the target data is data obtained after security protection is performed on multicast service
25 data. This ensures secure data transmission, and simplifies a processing procedure of the secure data transmission. Only the terminal device that obtains the target key can process the target data, and a terminal device that does not obtain the target key cannot process the target data, and therefore cannot obtain the data obtained after the target data is deprotected. This prevents an unauthorized terminal device from obtaining the multicast service data.

30 **[0008]** In a possible design, the key management method in this embodiment of this

application further includes: The terminal device receives a security algorithm from a first network element, where the security algorithm includes at least one of an encryption algorithm and an integrity protection algorithm. That the terminal device processes the target data by using the target key includes: The terminal device processes the target data by using the security algorithm and the target key. Herein, the first network element is the multicast user-plane processing network element or a key generation network element. The key generation network element is an SMF network element, an AMF network element, or an AUSF network element.

[0009] In this way, when the first network element is the multicast user-plane processing network element, the terminal device may obtain the security algorithm from a user plane message.

Alternatively, when the first network element is the key generation network element, the terminal device receives the security algorithm from the key generation network element via an AMF network element. In other words, the terminal device may obtain the security algorithm from a control plane message. Then, the target data is processed by using the security algorithm.

[0010] In a possible design, the key management method in this embodiment of this application further includes: The terminal device receives security protection status information from the first network element, where the security protection status information indicates a security protection status, and the security protection includes at least one of data encryption and integrity verification. For example, the security protection status information indicates that the security protection status is enabled or disabled. For example, the security protection status information indicates that the data encryption protection is in an enabled or disabled state, or the security protection status information indicates that the integrity verification is in an enabled or disabled state. That the terminal device processes the target data by using the target key includes: If the status indicated by the security protection status information is enabled, the terminal device processes the target data by using the target key.

[0011] Herein, the first network element is the multicast user-plane processing network element or a key generation network element. When the first network element is the multicast user-plane processing network element, the security protection status information is provided by the multicast user-plane processing network element. When the first network element is the key generation network element, the security protection status information is a target security policy determined by the key generation network element. The terminal device receives the target security policy from the key generation network element via an AMF network element. In this way, the

terminal device can process the target data based on the obtained security protection status information.

[0012] In a possible design, that a terminal device obtains a target key includes: The terminal device receives the target key from the first network element. Herein, the first network element is the multicast user-plane processing network element or a key generation network element. In other words, the terminal device may obtain the target key from a control plane message or a user plane message.

[0013] In a possible design, the key management method in this embodiment of this application further includes: The terminal device obtains an identifier of the target key. That a terminal device obtains a target key includes: The terminal device obtains the target key corresponding to the identifier of the target key.

[0014] In this way, the terminal device obtains the target key through indexing based on the identifier of the target key, to process the target data by using the "target key corresponding to the identifier of the target key". This simplifies a processing procedure on a terminal device side.

[0015] In a possible design, that the terminal device obtains an identifier of the target key includes: The terminal device receives the identifier of the target key from the first network element; or the terminal device receives a key number part from the first network element; and the terminal device determines the identifier of the target key based on the key number part and an identifier ID of a multicast service.

[0016] In other words, the terminal device can obtain the identifier of the target key in two manners. If an access network device provides the identifier of the target key for the terminal device, a processing procedure of "obtaining the identifier of the target key" on the terminal device side can be simplified. If the access network device provides the key number part for the terminal device, transmission resource overheads can be reduced in comparison with transmission of the "identifier of the target key".

[0017] In a possible design, the key management method in this embodiment of this application further includes: The terminal device receives first information from a key generation network element, where the first information includes 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. Herein, the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp. The terminal device generates a multimedia

broadcast/multicast service user key MUK based on the first information and a shared key, where the shared key is a key shared between the terminal device and a core network device. That a terminal device obtains a target key includes: The terminal device receives key information from the multicast user-plane processing network element, where the key information is information
5 obtained after the target key is encrypted by using the MUK; and the terminal device decrypts the key information by using the MUK, to obtain the target key.

[0018] In this way, when the key generation network element provides the first information for the terminal device, the terminal device can independently generate the MUK. When the multicast user-plane processing network element protects distribution of the target key by using
10 the MUK, the terminal device can decrypt the key information by using the MUK, to obtain the target key.

[0019] In a possible design, the shared key is an authentication server function key Kausf, a security anchor function key Kseaf, or a key derived from Kausf.

[0020] In a possible design, the key management method in this embodiment of this
15 application further includes: The terminal device receives time information corresponding to the target key from the key generation network element. The time information corresponding to the target MSK indicates valid time of the target MSK. For example, the target key is the target MSK. Within valid time of the target MSK, the multicast user-plane processing network element protects distribution of second information (information for generating the target MTK) by using the target
20 MSK. In this way, the terminal device can obtain the second information to generate the target MTK. On the contrary, the second information is not distributed beyond the valid time of the target MSK. In this case, the terminal device cannot obtain the second information, and therefore cannot generate the target MTK. Alternatively, within valid time of the target MSK, the multicast user-plane processing network element protects distribution of the multicast service data by using the
25 target MSK. In this way, the terminal device can obtain the multicast service data. On the contrary, the target MSK does not exist beyond the valid time of the target MSK, and the multicast service data is no longer distributed. In this case, the terminal device cannot obtain the multicast service data.

[0021] In a possible design, that the terminal device processes the target data by using the
30 target key includes: The terminal device decrypts ciphertext by using the target MSK or the first sub-key, to obtain a first plaintext, and the terminal device determines integrity of the first plaintext

based on a MAC and at least one of the target MSK and the second sub-key, where the target data includes the first plaintext and the MAC. Alternatively, the terminal device decrypts ciphertext by using the target MSK or the first sub-key, where the target data includes the ciphertext. Alternatively, the terminal device determines integrity of a second plaintext based on a message authentication code MAC and at least one of the target MSK and the second sub-key, where the target data includes the MAC and the second plaintext. That is, the target MSK can be for both decryption and integrity verification processing. There are two types of processing performed by the terminal device on the target data, that is, decryption and integrity verification processing.

[0022] In a possible design, that the terminal device processes the target data by using the target key includes: The terminal device performs a derivation operation on the target MSK to obtain a derivation key; and then, the terminal device performs decryption or integrity verification on the target data by using the derivation key.

[0023] Herein, the derivation key is one of the following keys: the first sub-key, the second sub-key, a target multimedia broadcast/multicast service transport key MTK, a third sub-key, or a fourth sub-key. When the derivation key includes the first sub-key, the terminal device performs a first derivation operation on the target MSK to obtain the first sub-key. When the derivation key includes the second sub-key, the terminal device performs a second derivation operation on the target MSK to obtain the second sub-key. When the derivation key includes the target MTK, the terminal device performs a third derivation operation on the target MSK to obtain the target MTK, where the MTK is for decryption or integrity verification. When the derivation key includes the third sub-key, the terminal device performs a third derivation operation on the target MSK to obtain a target MTK, and then the terminal device performs a fourth derivation operation on the target MTK to obtain the third sub-key. The third sub-key is for confidentiality protection calculation. When the derivation key includes the fourth sub-key, the terminal device performs a third derivation operation on the target MSK to obtain a target MTK, and then the terminal device performs a fifth derivation operation on the target MTK to obtain the fourth sub-key. The fourth sub-key is for integrity protection calculation.

[0024] In this way, when security protection is performed on the target data by using the derivation key, the terminal device side can also perform derivation by using the target key, to obtain the derivation key, and then process the target data by using the derivation key. In addition, when the derivation key is implemented by the target MTK, the third sub-key, or the fourth sub-

key, the terminal device can also perform derivation based on the target key, to obtain a key at an MTK level, to process the target data. Compared with a conventional technology in which "a terminal device directly receives an MTK from a network side", the terminal device obtains the key at the MTK level through derivation, to avoid a risk of key leakage in transmission.

5 **[0025]** In a possible design, that the terminal device performs a derivation operation on the target MSK to obtain a derivation key includes: The terminal device performs a derivation operation on the target MSK and second information to obtain the derivation key, where the second information includes at least one of the following: a protocol name, an identifier of the target MTK, or a second parameter. The second parameter is a parameter determined based on at least one of a
10 second sequence number and a second timestamp. Herein, the second information may be information provided by the multicast user-plane processing network element for the terminal device.

[0026] In other words, when obtaining the target MSK and the second information, the terminal device may perform the derivation operation to obtain the second key, and the network
15 side does not need to provide the target MTK for the terminal device, to reduce a risk of key leakage in transmission.

[0027] In a possible design, the second information is information encrypted by using the target MSK. The key management method provided in this embodiment of this application further includes: The terminal device decrypts the second information by using the target MSK, to obtain
20 decrypted information. That the terminal device performs a derivation operation on the target MSK and second information to obtain the derivation key includes: The terminal device performs a third derivation operation on the target MSK and the decrypted information to obtain the target MTK.

[0028] Herein, although the second information is distributed by using a multicast message, because the target MSK is transmitted by using a unicast message, the target MSK protects a
25 distribution process of the second information, and the second information is for derivation of the target MTK. In this way, security of the target MTK derived based on the second information is equivalent to security of unicast message transmission.

[0029] In a possible design, the key management method in this embodiment of this application further includes: The terminal device receives the encryption algorithm from the first
30 network element. That the terminal device performs a first derivation operation on the target MSK to obtain the first sub-key includes: The terminal device performs the first derivation operation on

the target MSK by using the encryption algorithm, to obtain the first sub-key. That the terminal device performs a fourth derivation operation on the target MTK to obtain the third sub-key includes: The terminal device performs the fourth derivation operation on the target MTK by using the encryption algorithm to obtain the third sub-key. Herein, the first network element is the multicast user-plane processing network element or a key generation network element.

[0030] In other words, the terminal device can obtain the encryption algorithm from a user plane message or a control plane message, and the encryption algorithm can be for deriving the first sub-key and the third sub-key.

[0031] In a possible design, the key management method in this embodiment of this application further includes: The terminal device receives the integrity protection algorithm from the first network element. That the terminal device performs a second derivation operation on the target MSK to obtain the second sub-key includes: The terminal device performs the second derivation operation on the target MSK by using the integrity protection algorithm, to obtain the second sub-key. That the terminal device performs a fifth derivation operation on the target MTK to obtain the fourth sub-key includes: The terminal device performs the fifth derivation operation on the target MTK by using the integrity protection algorithm, to obtain the fourth sub-key. Herein, the first network element is the multicast user-plane processing network element or a key generation network element.

[0032] In other words, the terminal device can obtain the integrity protection algorithm from a user plane message or a control plane message, and the integrity protection algorithm can be for deriving the second sub-key and the fourth sub-key.

[0033] According to a second aspect, an embodiment of this application provides a key management method. The method may be performed by a multicast user-plane processing network element, or may be performed by a chip used in the multicast user-plane processing network element. The following provides descriptions by using an example in which the method is performed by the multicast user-plane processing network element. The method includes: The multicast user-plane processing network element obtains a target key, where the target key includes at least one of a target multimedia broadcast/multicast service service key MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. Then, the multicast user-plane processing network element performs

security protection on multicast service data by using the target key, to obtain target data. The multicast user-plane processing network element sends the target data to a terminal device.

[0034] In a possible design, that the multicast user-plane processing network element obtains a target key includes: The multicast user-plane processing network element generates the target key; or the multicast user-plane processing network element receives the target key from a key generation network element.

[0035] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element sends the target key to the terminal device.

[0036] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives a multimedia broadcast/multicast service user key MUK from the key generation network element. The multicast user-plane processing network element encrypts the target key by using the MUK, to obtain key information. Then, the multicast user-plane processing network element sends the key information to the terminal device.

[0037] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives time information corresponding to the MUK from the key generation network element. The time information corresponding to the MUK indicates valid time of the MUK.

[0038] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element sends an identifier of the target MSK to the terminal device; or the multicast user-plane processing network element sends a key number part to the terminal device, where there is a mapping relationship between the key number part and an identifier of the target MSK.

[0039] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives time information corresponding to the target MSK from the key generation network element. The time information corresponding to the target MSK indicates valid time of the target MSK.

[0040] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element obtains a security algorithm. The security algorithm includes at least one of an encryption algorithm and an

integrity protection algorithm. That the multicast user-plane processing network element performs security protection on multicast service data by using the target key, to obtain target data includes: The multicast user-plane processing network element performs security protection on the multicast service data by using the security algorithm and the target key, to obtain the target data.

5 **[0041]** In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element determines security protection status information. The security protection status information indicates a security protection status, and the security protection includes at least one of data encryption and integrity verification. That the multicast user-plane processing network element performs security protection on multicast service data by using the target key, to obtain target data includes: If the status indicated by the security protection status information is enabled, the multicast user-plane processing network element performs security protection on the multicast service data by using the target key, to obtain the target data.

15 **[0042]** In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives a target security policy from the key generation network element. The target security policy includes at least one of a confidentiality protection policy and an integrity protection policy. That the multicast user-plane processing network element determines security protection status information includes: The multicast user-plane processing network element determines the security protection status information based on the target security policy.

25 **[0043]** In a possible design, that the multicast user-plane processing network element performs security protection on multicast service data by using the target key, to obtain target data includes: The multicast user-plane processing network element encrypts the multicast service data by using the target MSK or the first sub-key, to obtain the ciphertext, where the target data includes the ciphertext; and/or the multicast user-plane processing network element determines a message authentication code MAC based on the multicast service data and at least one of the target MSK and the second sub-key, where the target data includes the MAC.

30 **[0044]** In a possible design, that the multicast user-plane processing network element performs security protection on multicast service data by using the target key, to obtain target data includes: The multicast user-plane processing network element performs a derivation operation on the target MSK to obtain a derivation key; and the multicast user-plane processing network element performs

security protection on the multicast service data by using the derivation key, to obtain the target data.

[0045] Herein, the derivation key is one of the following keys: the first sub-key, the second sub-key, a target multimedia broadcast/multicast service transport key MTK, a third sub-key, or a fourth sub-key. When the derivation key includes the first sub-key, the multicast user-plane processing network element performs a first derivation operation on the target MSK to obtain the first sub-key. When the derivation key includes the second sub-key, the multicast user-plane processing network element performs a second derivation operation on the target MSK to obtain the second sub-key. When the derivation key includes the target MTK, the multicast user-plane processing network element performs a third derivation operation on the target MSK to obtain the target MTK, where the MTK is for decryption or integrity verification. When the derivation key includes the third sub-key, the multicast user-plane processing network element performs a third derivation operation on the target MSK to obtain a target MTK, and then the multicast user-plane processing network element performs a fourth derivation operation on the target MTK to obtain the third sub-key. The third sub-key is for confidentiality protection calculation. When the derivation key includes the fourth sub-key, the multicast user-plane processing network element performs a third derivation operation on the target MSK to obtain a target MTK, and then the multicast user-plane processing network element performs a fifth derivation operation on the target MTK to obtain the fourth sub-key. The fourth sub-key is for integrity protection calculation.

[0046] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element sends second information to the terminal device, where the second information includes at least one of the following: a protocol name, an identifier of the target MTK, or a second parameter. Herein, the second parameter is a parameter determined based on at least one of a second sequence number and a second timestamp. The second information is used by the terminal device to determine the target MTK.

[0047] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element encrypts the second information by using the target MSK. That the multicast user-plane processing network element sends second information to the terminal device includes: The multicast user-plane processing network element sends encrypted second information to the terminal device.

[0048] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives the encryption algorithm from the key generation network element. That the multicast user-plane processing network element performs a first derivation operation on the target MSK to obtain the first sub-key includes: The multicast user-plane processing network element performs the first derivation operation on the target MSK by using the encryption algorithm, to obtain the first sub-key. That the multicast user-plane processing network element performs a fourth derivation operation on the target MTK to obtain the third sub-key includes: The multicast user-plane processing network element performs the fourth derivation operation on the target MTK by using the encryption algorithm, to obtain the third sub-key.

[0049] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element receives the integrity protection algorithm from the key generation network element. That the multicast user-plane processing network element performs a second derivation operation on the target MSK to obtain the second sub-key includes: The multicast user-plane processing network element performs the second derivation operation on the target MSK by using the integrity protection algorithm, to obtain the second sub-key. That the multicast user-plane processing network element performs a fifth derivation operation on the target MTK to obtain the fourth sub-key includes: The multicast user-plane processing network element performs the fifth derivation operation on the target MTK by using the integrity protection algorithm, to obtain the fourth sub-key.

[0050] In a possible design, that the multicast user-plane processing network element performs a derivation operation on the target MSK to obtain a derivation key includes: The multicast user-plane processing network element performs a derivation operation on the target MSK and second information to obtain a derivation key, where the second information includes at least one of the following: a protocol name, an identifier of the target MTK, or a second parameter. Herein, the second parameter is a parameter determined based on at least one of a second sequence number and a second timestamp.

[0051] In a possible design, the key management method in this embodiment of this application further includes: The multicast user-plane processing network element determines, based on at least one of a transport protocol type, a session type, a quality of service QoS parameter, or a network type, to generate the target MTK. The derivation key includes the target MTK.

[0052] In other words, the multicast user-plane processing network element can determine whether to generate the target MTK. The multicast user-plane processing network element derives the target MTK only when the target MTK is generated, and performs security protection on the multicast service data by using the target MTK. On the contrary, when the target MTK does not
5 need to be generated, the multicast user-plane processing network element performs security protection on the multicast service data by using the target key.

[0053] In a possible design, the multicast user-plane processing network element includes one of the following network elements: a multicast/broadcast service user plane MBSU network element, a user plane function UPF network element, or a user plane gateway UPGW.

[0054] According to a third aspect, an embodiment of this application provides a key management method. The method may be performed by a key generation network element, or may be performed by a chip used in the key generation network element. Herein, the key generation network element may be an SMF network element, an AMF network element, or an AUSF network element. The following provides descriptions by using an example in which the method is
10 performed by the key generation network element. The method includes: The key generation network element obtains a multimedia broadcast/multicast service user key MUK; and then the key generation network element sends the MUK to a multicast user-plane processing network element.

[0055] In this way, in a 5G system, the key generation network element can obtain the MUK,
20 and provide the MUK for the multicast user-plane processing network element, to prevent an operator from deploying a GBA system. This helps simplify a multicast service data processing procedure.

[0056] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element obtains first information. The
25 first information includes at least one of the following: an identifier of the multicast user-plane processing network element, a first parameter, or an identifier ID of a multicast service. Herein, the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp. That a key generation network element obtains an MUK includes: The key generation network element generates the MUK based on the first information and a shared key.
30 The shared key is a key shared between a terminal device and a core network device.

[0057] In other words, when the key generation network element obtains the first information,

the key generation network element can independently generate the MUK. In this way, when an AUSF network element generates an MUK, an SMF can obtain the MUK from the AUSF network element.

[0058] It should be noted that when the key generation network element is implemented as an SMF network element, that an SMF network element obtains an MUK includes: The SMF network element sends the first information and a subscription permanent identifier SUPI of the terminal device to an AUSF network element, and the SMF network element receives an MUK from the AUSF network element. The MUK is generated based on the first information and the SUPI. Herein, both the first information and the SUPI that are sent by the SMF network element to the AUSF network element are carried in a key request message. The MUK received from the AUSF network element is carried in a key response message. In other words, when the SMF network element obtains the first information, the SMF network element can further provide the first information for the AUSF network element, so that the AUSF network element generates the MUK, and the SMF can obtain the MUK from the AUSF network element.

[0059] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends the first information to the terminal device, so that the terminal device generates the MUK.

[0060] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends time information corresponding to the MUK to the multicast user-plane processing network element. The time information corresponding to the MUK indicates valid time of the MUK.

[0061] In a possible design, the shared key is an authentication server function key Kausf, a security anchor function key Kseaf, or a key derived from Kausf.

[0062] According to a fourth aspect, an embodiment of this application provides a key management method. The method may be performed by a key generation network element, or may be performed by a chip used in the key generation network element. Herein, the key generation network element may be an SMF network element, an AMF network element, or an AUSF network element. The following provides descriptions by using an example in which the method is performed by the key generation network element. The method includes: The key generation network element obtains a target key, where the target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target

MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The key generation network element sends the target key to a multicast user-plane processing network element.

[0063] In other words, after the key generation network element obtains the target key, the key generation network element can further provide the target key for the multicast user-plane processing network element, so that the multicast user-plane processing network element performs security protection on multicast service data by using the target key.

[0064] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends an identifier of the target key to the multicast user-plane processing network element. Alternatively, the key generation network element sends a key number part to the multicast user-plane processing network element. There is a mapping relationship between the key number part and the identifier of the target key.

[0065] In other words, the key generation network element can provide the identifier of the target key for the multicast user-plane processing network element in two manners. If the key generation network element provides the identifier of the target key for the multicast user-plane processing network element, a processing procedure of "obtaining the identifier of the target key" on a multicast user-plane processing network element side can be simplified. If the key generation network element provides the key number part for the multicast user-plane processing network element, transmission resource overheads can be reduced in comparison with transmission of the "identifier of the target key".

[0066] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends time information corresponding to the target MSK to the multicast user-plane processing network element. The time information corresponding to the target MSK indicates valid time of the target MSK.

[0067] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends at least one of a key number part, the target key, and an identifier of the target key to the terminal device. There is a mapping relationship between the key number part and the identifier of the target key.

[0068] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends time information corresponding to the target MSK to the terminal device. The time information corresponding to

the target MSK indicates valid time of the target MSK.

[0069] According to a fifth aspect, an embodiment of this application provides a key management method. The method may be performed by a key generation network element, or may be performed by a chip used in the key generation network element. Herein, the key generation network element may be an SMF network element, an AMF network element, or an AUSF network element. The following provides descriptions by using an example in which the method is performed by the key generation network element. The method includes: The key generation network element determines a target security policy. The target security policy includes at least one of a confidentiality protection policy and an integrity protection policy. The key generation network element sends the target security policy to a multicast user-plane processing network element.

[0070] In this way, in a 5G system, the key generation network element can determine the target security policy, so that the multicast user-plane processing network element and a terminal device determine whether a status of security protection between the multicast user-plane processing network element and the terminal device is enabled. The multicast user-plane processing network element performs security protection on multicast service data only when the security protection is in an enabled state.

[0071] In a possible design, the key management method in this embodiment of this application further includes: that the key generation network element determines a target security policy includes: The key generation network element determines the target security policy based on a transmission status of a target multimedia broadcast multicast service transmission key MTK and a basic policy. The basic policy includes a multicast security policy in a multicast context or a user plane security policy in unified data management UDM subscription data. For example, when the target MTK is generated and transmitted, the key generation network element uses the basic policy as the target security policy, or the key generation network element modifies the basic policy, to obtain the target security policy.

[0072] In other words, when the key generation network element obtains the basic policy, the key generation network element can further determine the target security policy based on the transmission status of the target MTK.

[0073] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element determines a security algorithm.

The security algorithm is for security protection calculation, and the security protection is indicated by the target security policy. The key generation network element sends the security algorithm to the multicast user-plane processing network element.

[0074] In a possible design, the key management method in this embodiment of this application further includes: The key generation network element sends at least one of the target security policy and the security algorithm to the terminal device. The security algorithm is for security protection calculation, and the security protection is indicated by the target security policy.

[0075] According to a sixth aspect, an embodiment of this application provides a communication apparatus. The communication apparatus includes units configured to perform the steps according to any one of the foregoing aspects. The communication apparatus may be the terminal device according to any one of the first aspect or the possible designs of the first aspect, or a chip that implements a function of the terminal device. The communication apparatus includes a corresponding module, unit, or means (means) for implementing the foregoing method. The module, unit, or means may be implemented by hardware, software, or hardware executing corresponding software. The hardware or the software includes one or more modules or units corresponding to the foregoing function.

[0076] According to a seventh aspect, an embodiment of this application provides a communication apparatus, including a processor and an interface circuit. The processor is configured to: communicate with another apparatus by using the interface circuit, and perform the key management method according to any one of the foregoing aspects. There are one or more processors. The communication apparatus may be the terminal device according to any one of the first aspect or the possible designs of the first aspect, or a chip that implements a function of the terminal device.

[0077] According to an eighth aspect, an embodiment of this application provides a communication apparatus, and the apparatus includes a processor and a memory. The memory is configured to store computer instructions; and when the processor executes the instructions, the communication apparatus performs the method according to any one of the foregoing aspects. The communication apparatus may be the terminal device according to any one of the first aspect or the possible designs of the first aspect, or a chip that implements a function of the terminal device.

[0078] According to a ninth aspect, an embodiment of this application provides a communication apparatus, and the apparatus includes a processor. The processor is coupled to a

memory, and is configured to read instructions in the memory, and perform the method according to any one of the foregoing aspects according to the instructions. The communication apparatus may be the terminal device according to any one of the first aspect or the possible designs of the first aspect, or a chip that implements a function of the terminal device.

5 **[0079]** According to a tenth aspect, an embodiment of this application provides a communication apparatus. The communication apparatus includes units configured to perform the steps according to any one of the foregoing aspects. The communication apparatus may be the multicast user-plane processing network element according to any one of the second aspect or the possible designs of the second aspect, or a chip that implements a function of the multicast user-
10 plane processing network element. The communication apparatus includes a corresponding module, unit, or means (means) for implementing the foregoing method. The module, unit, or means may be implemented by hardware, software, or hardware executing corresponding software. The hardware or the software includes one or more modules or units corresponding to the foregoing function.

15 **[0080]** According to an eleventh aspect, an embodiment of this application provides a communication apparatus, including a processor and an interface circuit. The processor is configured to: communicate with another apparatus by using the interface circuit, and perform the key management method according to any one of the foregoing aspects. There are one or more processors. The communication apparatus may be the multicast user-plane processing network
20 element according to any one of the second aspect or the possible designs of the second aspect, or a chip that implements a function of the multicast user-plane processing network element.

[0081] According to a twelfth aspect, an embodiment of this application provides a communication apparatus, including a processor and a memory. The memory is configured to store computer instructions; and when the processor executes the instructions, the communication
25 apparatus performs the method according to any one of the foregoing aspects. The communication apparatus may be the multicast user-plane processing network element according to any one of the second aspect or the possible designs of the second aspect, or a chip that implements a function of the multicast user-plane processing network element.

[0082] According to a thirteenth aspect, an embodiment of this application provides a
30 communication apparatus, including a processor. The processor is coupled to a memory, and is configured to read instructions in the memory, and perform the method according to any one of

the foregoing aspects according to the instructions. The communication apparatus may be the multicast user-plane processing network element according to any one of the second aspect or the possible designs of the second aspect, or a chip that implements a function of the multicast user-plane processing network element.

5 **[0083]** According to a fourteenth aspect, an embodiment of this application provides a communication apparatus. The communication apparatus includes units configured to perform the steps according to any one of the foregoing aspects. The communication apparatus may be the key generation network element according to any one of the third aspect or the possible designs of the third aspect, or a chip that implements a function of the key generation network element; the
10 communication apparatus may be the key generation network element according to any one of the fourth aspect or the possible designs of the fourth aspect, or a chip that implements a function of the key generation network element; or the communication apparatus may be the key generation network element according to any one of the fifth aspect or the possible designs of the fifth aspect, or a chip that implements a function of the key generation network element. The communication
15 apparatus includes a corresponding module, unit, or means (means) for implementing the foregoing method. The module, unit, or means may be implemented by hardware, software, or hardware executing corresponding software. The hardware or the software includes one or more modules or units corresponding to the foregoing function.

[0084] According to a fifteenth aspect, an embodiment of this application provides a
20 communication apparatus, including a processor and an interface circuit. The processor is configured to: communicate with another apparatus by using the interface circuit, and perform the key management method according to any one of the foregoing aspects. There are one or more processors. The communication apparatus may be the key generation network element according to any one of the third aspect or the possible designs of the third aspect, or a chip that implements
25 a function of the key generation network element; the communication apparatus may be the key generation network element according to any one of the fourth aspect or the possible designs of the fourth aspect, or a chip that implements a function of the key generation network element; or the communication apparatus may be the key generation network element according to any one of the fifth aspect or the possible designs of the fifth aspect, or a chip that implements a function of
30 the key generation network element.

[0085] According to a sixteenth aspect, an embodiment of this application provides a

communication apparatus, including a processor and a memory. The memory is configured to store computer instructions; and when the processor executes the instructions, the communication apparatus performs the method according to any one of the foregoing aspects. The communication apparatus may be the key generation network element according to any one of the third aspect or the possible designs of the third aspect, or a chip that implements a function of the key generation network element; the communication apparatus may be the key generation network element according to any one of the fourth aspect or the possible designs of the fourth aspect, or a chip that implements a function of the key generation network element; or the communication apparatus may be the key generation network element according to any one of the fifth aspect or the possible designs of the fifth aspect, or a chip that implements a function of the key generation network element.

[0086] According to a seventeenth aspect, an embodiment of this application provides a communication apparatus, including a processor. The processor is coupled to a memory, and is configured to read instructions in the memory, and perform the method according to any one of the foregoing aspects according to the instructions. The communication apparatus may be the key generation network element according to any one of the third aspect or the possible designs of the third aspect, or a chip that implements a function of the key generation network element; the communication apparatus may be the key generation network element according to any one of the fourth aspect or the possible designs of the fourth aspect, or a chip that implements a function of the key generation network element; or the communication apparatus may be the key generation network element according to any one of the fifth aspect or the possible designs of the fifth aspect, or a chip that implements a function of the key generation network element.

[0087] According to an eighteenth aspect, an embodiment of this application provides a computer-readable storage medium. The computer-readable storage medium stores instructions; and when the instructions are run on a computer, the computer is enabled to perform the key management method according to any one of the foregoing aspects.

[0088] According to a nineteenth aspect, an embodiment of this application provides a computer program product including instructions. When the computer program product runs on a computer, the computer is enabled to perform the key management method according to any one of the foregoing aspects.

[0089] According to a twentieth aspect, an embodiment of this application provides a circuit

system, where the circuit system includes a processing circuit, and the processing circuit is configured to perform the key management method according to any one of the foregoing aspects.

[0090] According to a twenty-first aspect, an embodiment of this application provides a chip. The chip includes a processor, the processor is coupled to a memory, and the memory stores program instructions. When the program instructions stored in the memory are executed by the processor, the key management method according to any one of the foregoing aspects is implemented.

[0091] According to a twenty-second aspect, an embodiment of this application provides a communication system. The communication system includes a terminal device and a multicast user-plane processing network element. The terminal device is configured to obtain a target key. The target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK. The first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The terminal device is further configured to receive target data from the multicast user-plane processing network element. The target data is data on which security protection is performed. The terminal device is further configured to process the target data by using the target key. The multicast user-plane processing network element is configured to obtain the target key. The target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The multicast user-plane processing network element is further configured to perform security protection on multicast service data by using the target key, to obtain the target data. The multicast user-plane processing network element is further configured to send the target data to the terminal device.

[0092] In a possible design, the communication system in this embodiment of this application further includes a key generation network element. The key generation network element is configured to obtain an MUK. The key generation network element is further configured to send the MUK to the multicast user-plane processing network element. Herein, the key generation network element may be an SMF network element, an AMF network element, or an AUSF network element.

[0093] In a possible design, the communication system in this embodiment of this application further includes a key generation network element. The key generation network element is

configured to obtain the target key. The key generation network element is further configured to send the target key to the multicast user-plane processing network element.

- 5 [0094] In a possible design, the communication system in this embodiment of this application further includes a key generation network element. The key generation network element determines a target security policy. The target security policy includes at least one of a confidentiality protection policy and an integrity protection policy. The key generation network element sends the target security policy to the multicast user-plane processing network element. The multicast user-plane processing network element is further configured to determine security protection status information based on the target security policy. The security protection status information indicates a security protection status, and the security protection includes at least one of data encryption and integrity verification. The multicast user-plane processing network element is specifically configured to: if the status indicated by the security protection status information is enabled, perform security protection on the multicast service data by using the target key, to obtain the target data.
- 10
- 15 [0095] For technical effects brought by any design of the sixth aspect to the twenty-second aspect, refer to beneficial effects in the corresponding methods provided above. Details are not described herein again.

BRIEF DESCRIPTION OF DRAWINGS

- 20 [0096] FIG. 1 is a schematic diagram of a key system of a three-layer architecture according to a related technology;
- [0097] FIG. 2 is a schematic diagram of another key system of a three-layer architecture according to a related technology;
- [0098] FIG. 3 is a schematic flowchart of a data transmission method according to a related technology;
- 25 [0099] FIG. 4(a) is a schematic diagram of an architecture of a communication system according to an embodiment of this application;
- [00100] FIG. 4(b) is a schematic diagram of an architecture of another communication system according to an embodiment of this application;
- [00101] FIG. 5A and FIG. 5B are a schematic flowchart of a key management method according to an embodiment of this application;
- 30

[00102] FIG. 6(a) is a schematic flowchart of another key management method according to an embodiment of this application;

[00103] FIG. 6(b) is a schematic flowchart of another key management method according to an embodiment of this application;

5 **[00104]** FIG. 7(a) is a schematic flowchart of another key management method according to an embodiment of this application;

[00105] FIG. 7(b) is a schematic flowchart of another key management method according to an embodiment of this application;

[00106] FIG. 8 is a schematic flowchart of another key management method according to an
10 embodiment of this application;

[00107] FIG. 9 is a schematic flowchart of another key management method according to an embodiment of this application;

[00108] FIG. 10 is a schematic flowchart of another key management method according to an embodiment of this application;

15 **[00109]** FIG. 11 is a schematic flowchart of another key management method according to an embodiment of this application;

[00110] FIG. 12 is a schematic flowchart of another key management method according to an embodiment of this application;

[00111] FIG. 13 is a schematic diagram of a structure of a communication apparatus according
20 to an embodiment of this application; and

[00112] FIG. 14 is a schematic diagram of a structure of another communication apparatus according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[00113] In the specification and accompanying drawings of this application, the terms "first",
25 "second", and the like are intended to distinguish between different objects or distinguish between different processing of a same object, but do not indicate a particular order of the objects. In addition, the terms "including", "having", or any other variant thereof in descriptions of this application are intended to cover a non-exclusive inclusion. For example, a process, a method, a system, a product, or a device that includes a series of steps or units is not limited to the listed
30 steps or units, but optionally further includes other unlisted steps or units, or optionally further

includes another inherent step or unit of the process, the method, the product, or the device. It should be noted that, in embodiments of this application, the word "example" or "for example" is used to represent giving an example, an illustration, or a description. Any embodiment or design scheme described as an "example" or "for example" in embodiments of this application should not be explained as being more preferred or having more advantages than another embodiment or design scheme. Exactly, use of the word "example", "for example", or the like is intended to present a related concept in a specific manner.

[00114] Technical terms used in embodiments of this application are first described.

[00115] A multimedia broadcast/multicast service (multimedia broadcast/multicast service, MBMS) is a point-to-multipoint service in which a data source sends data to a plurality of terminal devices through a shared transmission link. This service is also referred to as a multicast broadcast service (multicast broadcast service, MBS).

[00116] In a long term evolution (long term evolution, LTE) network, user plane (user plane) security protection is performed between a terminal device and a broadcast/multicast service center (broadcast-multicast service centre, BM-SC). The BM-SC can provide a broadcast/multicast bearer service and an MBMS user service, and has functions such as session transmission, proxy forwarding, user management, and security. Herein, one MBMS user service includes one or more MBMS streaming sessions (sessions), and/or one MBMS user service includes one or more MBMS download sessions. One streaming session includes one or more RTP sessions. One download session includes one or more FLUTE channels. Each streaming session or each download session is carried in one or more MBMS transmission services. The MBMS user service and the MBMS transmission service are independent of each other, and there is a many-to-many relationship between MBMS user services and MBMS transmission services. The BM-SC uses a multimedia broadcast/multicast service service key (multimedia broadcast/multicast service service key, MSK) to protect different RTP sessions and FLUTE channels. Herein, the RTP session and the FLUTE channel are for transmitting a multimedia broadcast/multicast service transport key (multimedia broadcast/multicast service transport key, MTK) and service data. The service data is encrypted by using the MTK. In this way, the MSK is for protecting distribution of the MTK, and the MTK is for protecting transmission of the service data.

[00117] Refer to FIG. 1. FIG. 1 shows a key system of the foregoing three-layer architecture. An MUK is a key at a terminal device granularity, and one terminal device corresponds to one

MUK. MUKs in both a terminal device and a BM-SC are obtained by using a generic bootstrapping architecture (generic bootstrapping architecture, GBA). Different MSK key groups are for protecting different MTKs. As shown in FIG. 1, MSK key group A, MSK key group B, and MSK key group C are for protecting different MTKs. Different MTKs are for protecting different RTP sessions. As shown in FIG. 1, the MTK protected by MSK key group A is for protecting RTP session 1, the MTK protected by MSK key group B is for protecting RTP session 2, and the MTK protected by MSK key group C is for protecting RTP session 3.

[00118] Refer to FIG. 2. FIG. 2 shows a key system of an RTP session. For a same RTP session, one key group includes one or more MSKs, and different MSKs in one key group correspond to different use moments. As shown in FIG. 2, a key group includes n MSKs, which are denoted as MSK1, MSK2, ..., and MSK n respectively. MSK1 is a key used at a current (current) moment, MSK2 is a key used at a next (next) moment, and use moments of other MSKs in the key group are deduced by analogy.

[00119] After a terminal device completes multicast user service registration, a BM-SC selects a sending occasion, and sends an MSK corresponding to a multicast service to the terminal device. A transport protocol used in an MSK transmission process is a MIKEY protocol. In addition, different MSKs have different identifiers. An MSK identifier includes a mobile country code (mobile country code, MCC) || mobile network code (mobile network code, MNC) part, a key group part (key group part), and a key number part (key number part). That is, the MSK identifier is implemented as "MCC || MNC+ key group part + key number part". The "MCC || MNC part" indicates that the MNC is appended after the MCC to form a common character string. The "MCC || MNC part" identifies a public land mobile network (public land mobile network, PLMN), the key group part identifies the BM-SC, and the key number identifies a key number, such as a current moment or a next moment.

[00120] The BM-SC generates an MTK. Distribution of the MTK is protected by an MSK. As shown in FIG. 2, MSK1 protects distribution of MTK₁₁, MTK₁₂, ..., MTK_{1x}, and the like. MSK2 protects distribution of MTK₂₁, MTK₂₂, ..., MTK_{2y}, and the like. MSK n protects distribution of MTK_{n1}, MTK_{n2}, ..., MTK_{nk}, and the like.

[00121] In a service data transmission process, the BM-SC sends service data and an MTK identifier to the terminal device. Correspondingly, the terminal device receives the service data and the MTK identifier from the BM-SC. The service data is data encrypted by using an MTK

corresponding to the MTK identifier. The terminal device searches for the corresponding MTK based on the MTK identifier, and performs security deprotection on the service data by using the found MTK. Herein, the MTK identifier includes the following parts: a key block part (key group part), a key number part (key number part), and an MTK identifier (identity, ID).

5 **[00122]** In a 5th generation mobile communication (5th-generation, 5G) system, a data transmission process of a multicast service is shown in FIG. 3, and specific steps are as follows:

[00123] Step 1. A terminal device completes registration with a network, and the terminal device establishes a protocol data unit (protocol data unit, PDU) session with an application function (application function, AF) network element.

10 **[00124]** Step 2. The AF network element sends a multicast announcement (multicast announcement) message to the terminal device at an application layer. Correspondingly, the terminal device receives the multicast announcement message from the AF network element.

[00125] The multicast announcement message is for notifying the terminal device to start to provide a multicast service. The multicast announcement message further includes an internet
15 protocol (internet protocol, IP) address of the multicast service.

[00126] Step 3. The terminal device joins the multicast service through a user plane.

[00127] A user plane function (user plane function, UPF) network element serves as a multicast router. Herein, the UPF network element sends a message to a session management function (session management function, SMF) network element, to notify the SMF network element of the
20 IP address of the multicast service.

[00128] Step 4. The terminal device joins the multicast service through a signaling plane.

[00129] Herein, the terminal device sends a PDU session modification request to an access and mobility management function (access and mobility management function, AMF) network element. Correspondingly, the AMF network element receives the PDU session modification
25 request from the terminal device.

[00130] The AMF network element sends a PDU session update context message (PDU session update SMcontext) to the SMF network element. Correspondingly, the SMF network element receives the PDU session update context message from the AMF network element.

[00131] Both the PDU session modification request and the PDU session update context
30 message are written into the IP address of the multicast service. In this way, the SMF network element can obtain the IP address of the multicast service.

[00132] It should be noted that, in an actual application process, the terminal device may select a manner corresponding to step 3 or step 4 to join the multicast service.

[00133] Step 5. The SMF network element obtains a multicast context corresponding to the IP address of the multicast service.

5 **[00134]** For example, the SMF network element sends a first request message to a unified data management (unified data management, UDM) network element. Correspondingly, the UDM network element receives the first request message from the SMF network element. The first request message includes the IP address of the multicast service, to request the multicast context corresponding to the IP address of the multicast service. If the UDM network element can provide
10 the multicast context corresponding to the IP address of the multicast service, the UDM network element sends the multicast context corresponding to the IP address of the multicast service to the SMF network element. Correspondingly, the SMF network element receives, from the UDM network element, the multicast context corresponding to the IP address of the multicast service. The multicast context includes a multicast security policy. On the contrary, if the UDM network
15 element cannot provide the multicast context corresponding to the IP address of the multicast service, the UDM network element sends a failure message to the SMF network element. The SMF network element sends a second request message to the UDM network element, to request subscription data. The SMF network element receives the subscription data from the UDM network element. The subscription data includes an allowed PDU session type, an allowed service and session continuity (service and session continuity, SSC) mode (mode), an SMF-associated
20 external parameter, a user plane security policy, and the like. The SMF network element creates, based on the subscription data, the multicast context corresponding to the IP address of the multicast service.

[00135] Step 6. The SMF network element sends service configuration information to the AMF
25 network element. Correspondingly, the AMF network element receives the service configuration information from the SMF network element.

[00136] The service configuration information includes the multicast context, a dedicated quality of service (quality of service, QoS) rule, and the like.

[00137] Step 7. The AMF network element sends an N2 session modification request to an
30 access network device. Correspondingly, the access network device receives the N2 session modification request from the AMF network element.

[00138] The N2 session modification request includes the service configuration information.

[00139] Step 8. The access network device sends a radio resource control (radio resource control, RRC) reconfiguration message to the terminal device. Correspondingly, the terminal device receives the RRC reconfiguration message from the access network device.

5 **[00140]** For example, when the access network device determines, based on common information, that the service is for transmitting multicast data (for example, the service is a service jointly received by a plurality of terminal devices), the access network device associates the service with a common data channel between the UPF network element and the access network device. The common data channel may be an established channel, or may be a channel that is triggered to
10 be established in the foregoing case. In this case, the access network device sends the RRC reconfiguration message to the terminal device, to notify the terminal device that a channel for receiving the multicast data is the common data channel. The service configuration information includes the common information.

[00141] After the terminal device obtains the RRC reconfiguration message, the terminal device
15 sends an RRC reconfiguration acknowledgment to the access network device. Correspondingly, the access network device receives the RRC reconfiguration acknowledgment from the terminal device.

[00142] Step 9. The access network device sends a session response message to the AMF network element. Correspondingly, the AMF network element receives the session response
20 message from the access network device.

[00143] The session response message includes an IP address and a general packet radio service tunneling protocol-user plane (general packet radio service tunneling protocol-user plane, GTP-U) tunnel endpoint identifier (tunnel endpoint identifier, TEID) of the access network device.

[00144] Step 10. The AMF network element sends a session update message to the SMF
25 network element. Correspondingly, the SMF network element receives the session update message from the AMF network element.

[00145] The session update message includes the IP address and the GTP-U TEID of the access network device.

[00146] Step 11. The SMF network element sends a session modification message to the UPF
30 network element. Correspondingly, the UPF network element receives the session modification message from the SMF network element.

[00147] The session modification message includes the IP address and the GTP-U TEID of the access network device.

[00148] The UPF network element establishes a bearer between the UPF and the access network device based on the IP address and the GTP-U TEID of the access network device, to transmit the

5 multicast data.

[00149] Step 12. The AF network element sends the multicast data to a multicast/broadcast service user plane (multicast/broadcast service user plane, MBSU) network element. Correspondingly, the MBSU network element receives the multicast data from the AF network element.

10 **[00150]** The MBSU network element may also be replaced with a user packet data network gateway (user packet data network gateway, UPGW). Both the MBSU network element and the UPGW may be independent network elements, or may be parts of the UPF network element (in other words, both the MBSU network element and the UPGW may be integrated with the UPF network element).

15 **[00151]** Step 13. The MBSU network element sends the multicast data to the UPF network element. Correspondingly, the UPF network element receives the multicast data from the MBSU network element.

[00152] Step 14. The UPF network element sends the multicast data to the access network device. Correspondingly, the access network device receives the multicast data from the UPF

20 network element.

[00153] Step 15. The access network device sends the multicast data to the terminal device. Correspondingly, the terminal device receives the multicast data from the access network device.

[00154] In conclusion, to meet security requirements in the RTP/FULTE protocol, a three-layer key architecture is used in an LTE network. An architecture of the 5G network is different from an

25 architecture of the LTE network, and the 5G system has not defined a security protection processing procedure for MBS service data. If the 5G system does not use the RTP protocol or the FLUTE protocol, but still uses the foregoing key system of the three-layer architecture, there is extra redundancy in a signaling procedure and transmission load of the 5G system. In addition, in the LTE network, an MUK is generated by a terminal device and a network device through

30 negotiation by using a GBA system. In this case, an operator needs to deploy a GBA system in addition to a multimedia broadcast/multicast service system. Therefore, in a 5G

broadcast/multicast service, how to simplify a secure transmission procedure of the multicast service data and prevent an unauthorized user from obtaining the multicast service data is a problem that needs to be resolved.

[00155] In view of this, embodiments of this application provide a key management method. A communication system to which the key management method in embodiments of this application is applicable is first described. The communication system may be a communication system supporting a 5G mobile communication technology, for example, a new radio (new radio, NR) access technology. Alternatively, the communication system may be a communication system supporting a plurality of wireless technologies, for example, a communication system supporting an LTE technology and an NR access technology. In addition, the communication system may alternatively be applicable to a future-oriented communication technology.

[00156] Refer to FIG. 4(a). A network architecture of the communication system is described by using the communication system supporting the 5G mobile communication technology as an example. Network elements in the 5G network architecture include a terminal device, an access network device, a UPF network element, a multicast/broadcast service user plane (multicast/broadcast service user plane, MBSU) network element, a multicast service function (multicast service function, MSF) network element, an application function (application function, AF) network element, an AMF network element, an SMF network element, a network exposure function (network exposure function, NEF) network element, a multicast/broadcast service function (multicast/broadcast service function, MBSF) network element, a policy control function (policy control function, PCF) network element, and the like.

[00157] The terminal device is also referred to as user equipment (user equipment, UE), a mobile station (mobile station, MS), a mobile terminal (mobile terminal, MT), or the like, is a device that provides a voice/data connectivity for a user, for example, a handheld device or a vehicle-mounted device having a wireless connection function. The terminal device may be specifically a mobile phone (mobile phone), a tablet computer, a notebook computer, a palmtop computer, a mobile internet device (mobile internet device, MID), a wearable device, a virtual reality (virtual reality, VR) device, an augmented reality (augmented reality, AR) device, a wireless terminal in industrial control (industrial control), a wireless terminal in self driving (self-driving), a wireless terminal in remote medical surgery (remote medical surgery), a wireless terminal in a smart grid (smart grid), a wireless terminal in transportation safety (transportation safety), a

wireless terminal in a smart city (smart city), a wireless terminal in a smart home (smart home), a terminal device in a future 5G communication network or a communication network after 5G, or the like. This is not limited in embodiments of this application.

[00158] The access network device may be a radio access network (radio access network, RAN) device, and is an apparatus that is deployed in a radio access network to provide a wireless communication function. Optionally, the RAN device in embodiments of this application includes, for example, but is not limited to, a macro base station, a micro base station (also referred to as a small cell), a relay station, a transmission reception point (transmission reception point, TRP), a next generation network node (gNodeB, gNB), an evolved NodeB (ng evolved Node B, ng-eNB) connected to a next-generation core network, and the like, and may further include a RAN device of a non-3rd generation partnership project (3rd generation partnership project, 3GPP) system such as a wireless local area network (wireless local area network, WLAN) access device.

[00159] The UPF network element is a function network element of a user plane, and is mainly responsible for forwarding and receiving user data in a terminal device. The UPF network element may receive the user data from a data network (data network, DN), and transmit the user data to the terminal device through the access network device. Alternatively, the UPF network element may receive the user data from the terminal device through the access network device, and forward the user data to the data network. The UPF network element has resource transmission and scheduling functions that serve the terminal device, which are managed and controlled by the SMF network element. A UPF network element that supports a multicast/broadcast session may also be referred to as an MB-UPF network element.

[00160] The MBSU network element mainly processes user plane data to meet service layer function and management requirements. Herein, the MBSU network element may be a network element of a logical function, and is co-deployed with another network element.

[00161] The MSF network element mainly provides a service layer function. For example, the MSF network element provides a signaling plane function and a user plane function, specifically including multicast service configuration, multicast service management, data encoding, data transmission, and the like. An MSF network element that provides a user plane function may also be denoted as an "MSF-U" network element, and an MSF network element that provides a control plane function may also be denoted as an "MSF-C" network element. Herein, the MSF network element may be a network element of a logical function, and is co-deployed with another network

element.

[00162] The AF network element may interact with a 3GPP core network. The AF network element may be specifically an application server, and may be configured to interact with the PCF network element to customize a policy for an application.

5 **[00163]** The AMF network element has functions such as mobility management, registration management, connection management, lawful interception, access authentication, and access authorization of the terminal device, and supports transmission of session management (session management, SM) information between the terminal device and the SMF network element.

[00164] The SMF network element has functions such as session management and roaming.

10 The session management function includes, for example, session establishment, modification, and release. The roaming function may include charging data collection and supporting of signaling transmission for authentication/authorization with an external (external) data network. An SMF network element that supports a multicast/broadcast session may also be referred to as an MB-SMF network element.

15 **[00165]** The NEF network element may provide network functions such as externally providing a service or a capability of a network element, an application function, and edge computing. Optionally, the NEF network element further provides an application function of providing information to the 3GPP core network, for example, in a mobility mode and a communication mode. In this case, the NEF network element may further provide a network function of
20 authenticating, authorizing, and limiting the foregoing application function.

[00166] The MBSF network element may be a part of the NEF network element, or may be an independent network element. The MBSF network element is configured to process multicast/broadcast service management, provide an interface from a core network to an application server, and authorize a terminal device to join a multicast/broadcast session.

25 **[00167]** The PCF network element provides a user subscription information management function, a policy control function, a charging policy control function, quality of service (quality of service, QoS) control, and the like.

[00168] The terminal device communicates with the access network device through a Uu interface, the access network device communicates with the AMF network element through an N2
30 interface, the access network device communicates with the UPF network element through an N3 interface, the UPF network element communicates with the SMF network element through an N4

interface, the UPF network element accesses the AF network element and the MBSU network element through N6 interfaces, the MBSU network element communicates with the AF network element through an NxMB-U interface, and the MBSU network element communicates with the NEF network element through an Ny interface. The AMF network element communicates with the SMF network element through an N11 interface. The SMF network element communicates with the PCF network element through an N7 interface. The PCF network element communicates with the NEF network element through an N30 interface. The NEF network element communicates with the AF network element through an N33 interface.

[00169] Refer to FIG. 4(b). An embodiment of this application provides another network architecture still by using the communication system supporting the 5G mobile communication technology as an example. Network elements in the 5G network architecture include a terminal device, an access network device, a UPF network element, an MSF-U network element, an AF network element, an AMF network element, an SMF network element, an MSF-C network element, an NEF network element, and the like. Herein, for descriptions of each network element, refer to related descriptions in FIG. 4(a). Details are not described herein again. The MSF-U network element and the MSF-C network element each may be a network element of a logical function, and each are co-deployed with another network element.

[00170] The communication system and a service scenario described in embodiments of this application are intended to describe the technical solutions in embodiments of this application more clearly, but constitute no limitation on the technical solutions provided in embodiments of this application. A person of ordinary skill in the art may learn that the technical solutions provided in embodiments of this application are also applicable to a similar technical problem as a network architecture evolves and a new service scenario emerges.

[00171] The following describes in detail the key management method provided in embodiments of this application.

[00172] It should be noted that, in the following embodiments of this application, names of messages between network elements, names of parameters in messages, or the like are merely examples, and there may be other names during specific implementation. In embodiments of this application, a target key includes at least one of a target MSK, a first sub-key, or a second sub-key. Both the first sub-key and the second sub-key correspond to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection

calculation. The first sub-key may be denoted as MSK_enc, and the second sub-key may be denoted as MSK_int. Both a third sub-key and a fourth sub-key correspond to a target MTK, the third sub-key is for confidentiality protection calculation, and the fourth sub-key is for integrity protection calculation. The third sub-key may be denoted as MTK_enc, and the fourth sub-key may be denoted as MTK_int. This is uniformly described herein, and details are not described below again.

[00173] An embodiment of this application provides a first key management method, and the key management method is applied to an MBS communication process. A terminal device completes a registration process and a PDU session establishment process, and joins a multicast service. For details, refer to related descriptions of step 1 to step 5 in FIG. 3. Details are not described herein again. After joining the multicast service, the terminal device performs a key management method shown in FIG. 5A and FIG. 5B. Specific steps are as follows:

[00174] Phase 1: MUK negotiation. In this phase, both the terminal device and a multicast user-plane processing network element obtain an MUK. A process of obtaining the MUK may be implemented by using the 5G GBA protocol or the authentication and key management for applications (authentication and key management for applications, AKMA) protocol. Details are not described herein. Alternatively, an MUK negotiation manner described in embodiments of this application may be used in a process of obtaining the MUK. For a specific implementation process, refer to related descriptions of S501 to S509.

[00175] S501. A key generation network element obtains the MUK.

[00176] The key generation network element is an SMF network element, an AMF network element, or an AUSF network element.

[00177] For example, the key generation network element initiates a processing process of "obtaining the MUK" only when a specific trigger condition is met. Herein, the key generation network element determines, based on a multicast service authentication or authorization result, whether to initiate the processing process of "obtaining the MUK". It may be understood that, when multicast service authentication of the key generation network element succeeds or the terminal device is authorized, the key generation network element initiates the processing procedure of "obtaining the MUK". On the contrary, when the multicast service authentication of the key generation network element fails or the terminal device is not authorized, the key generation network element does not initiate the processing process of "obtaining the MUK". The

multicast service authentication may be secondary authentication, or may be a specific authentication procedure. This is not limited in this embodiment of this application. Herein, the "secondary authentication" is an authentication process performed between a terminal device and an AF network element after primary authentication between the terminal device and a core network device succeeds. An extensible authentication protocol (extensible authentication protocol, EAP) authentication framework is used in the authentication process. The key generation network element (for example, an SMF network element) may be used as an EAP authenticator (authenticator), the terminal device is used as an EAP client, and the AF network element is used as an EAP server. The "specific authentication procedure" is an authentication procedure dedicated to a multicast service, for example, an authentication procedure performed between the terminal device and the AF network element. An EAP authentication framework or another authentication protocol is used in this authentication process.

[00178] The key generation network element receives an authentication result from the AF network element or a multicast user-plane processing network element, and then the key generation network element determines, based on the authentication result, whether the multicast service authentication succeeds. Herein, "authorization" refers to granting a right of multicast access to the terminal device. The key generation network element obtains subscription data of the terminal device from a UDM network element. The subscription data of the terminal device includes indication information, and the indication information indicates whether the terminal device is allowed to obtain the multicast service. The key generation network element determines, based on the subscription data of the terminal device, whether to perform authorization.

[00179] For example, the MUK is for protecting distribution of an MSK. There are a plurality of manners of obtaining the MUK, and the manners may be, for example, but are not limited to, the following two cases:

[00180] Case 1: When the key generation network element is an SMF network element, an AMF network element, or an AUSF network element, the key generation network element generates the MUK. A specific implementation process is shown in FIG. 6(a).

[00181] S5010. The key generation network element obtains first information.

[00182] The first information includes at least one of the following information:

[00183] 1. Identifier of the multicast user-plane processing network element: Herein, the identifier of the multicast user-plane processing network element may be information

preconfigured on the key generation network element, or may be information obtained after the key generation network element requests the multicast user-plane processing network element. The multicast user-plane processing network element may be one of the following network elements: an MBSU network element, a UPF network element, an MSF network element, or a UPGW. When the multicast user-plane processing network element is implemented as an MBSU network element, the identifier of the multicast user-plane processing network element is an identifier of the MBSU network element. Security protection for the multicast service is implemented between the terminal device and the MBSU network element. When the multicast user-plane processing network element is implemented as a UPF network element, the identifier of the multicast user-plane processing network element is an identifier of the UPF network element. Security protection for the multicast service is implemented between the terminal device and the UPF network element. When the multicast user-plane processing network element is implemented as a UPGW, the identifier of the multicast user-plane processing network element is an identifier of the UPGW. Security protection for the multicast service is implemented between the terminal device and the UPGW. The UPGW may be an independent network element, or may be integrated with one of the UPF network element, the MBSU network element, or the MSF network element. When the multicast user-plane processing network element is implemented as the MSF network element, the identifier of the multicast user-plane processing network element is an identifier of the MSF network element. Security protection for the multicast service is implemented between the terminal device and the MSF network element.

[00184] 2. First parameter: Herein, the first parameter may be a parameter determined based on at least one of a first random number, a first count value, or a first timestamp. For example, the first parameter is the first random number, the first count value, or the first timestamp. The first parameter is generated and maintained by the key generation network element.

[00185] 3. ID of the multicast service: Herein, the ID of the multicast service may be implemented as an IP address of the multicast service, or may be a group identifier of the multicast service. When the key generation network element is implemented as an SMF network element, for a specific implementation process of "obtaining, by the SMF network element, the IP address of the multicast service", refer to related descriptions of step 1 to step 4 in FIG. 3. Details are not described herein again.

[00186] S5011. The key generation network element generates the MUK based on the first

information and a shared key.

[00187] For example, in a process in which the key generation network element derives the MUK, an input key for calculating the MUK is the shared key, an input parameter for calculating the MUK is the first information, and a derivation algorithm for calculating the MUK may be a hash message authentication code (hash message authentication code, HMAC) algorithm.

[00188] The shared key is a key shared between the terminal device and the core network device. Herein, the shared key is an authentication server function key K_{ausf} , a security anchor function key K_{seaf} , or a key derived from K_{ausf} .

[00189] Specific functions of each piece of information in the first information in an MUK generation process are as follows:

[00190] The identifier of the multicast user-plane processing network element is used to isolate security protection between different network elements (such as the MBSU network element, the UPF network element, and the UPGW). For example, when there are a plurality of multicast user-plane processing network elements in a PLMN, identifiers of the multicast user-plane processing network elements correspond to a unique multicast user-plane processing network element. When there is a unique multicast user-plane processing network element (for example, an MBSU network element, a UPF network element, a UPGW, or an MSF network element) in a PLMN, an identifier of the multicast user-plane processing network element may be set to a fixed value, or may not be used as an "input parameter for calculating an MUK".

[00191] The first parameter is used to isolate MUKs of different time sequences. To be specific, the terminal device is allowed to access the multicast service at a moment 1, and both the terminal device and the core network device can perform derivation based on a first parameter corresponding to the moment 1, to obtain an MUK corresponding to the moment 1. The MUK corresponding to moment 1 protects distribution of a target MSK. In this way, when the terminal device has the MUK corresponding to the moment 1, the terminal device can obtain the target MSK. The terminal device is not allowed to access the multicast service at a moment 2, and the terminal device cannot perform derivation based on a first parameter corresponding to the moment 2, and therefore cannot obtain an MUK corresponding to the moment 2. Distribution of an updated target MSK is protected by the MUK corresponding to the moment 2. In this case, when the terminal device does not have the MUK corresponding to the moment 2, the terminal device cannot obtain the updated target MSK.

[00192] The identifier of the multicast service is used to isolate MUKs in different multicast services.

[00193] In this way, the key generation network element can generate the MUK based on the shared key and at least one of the identifier of the multicast user-plane processing network element, the first parameter, and the ID of the multicast service, and further distribute the MUK to the multicast user-plane processing network element.

[00194] Case 2: When the key generation network element is an SMF network element, the SMF network element obtains the MUK from an AUSF network element. A specific implementation process is shown in FIG. 6(b).

[00195] S5012. The SMF network element obtains first information.

[00196] For descriptions of the first information, refer to specific descriptions of S5010. Details are not described herein again.

[00197] S5013. The SMF network element sends the first information and a subscription permanent identifier (subscription permanent identifier, SUPI) to the AUSF network element.

Correspondingly, the AUSF network element receives the first information and the SUPI from the SMF network element.

[00198] The SUPI can identify a real identity of the terminal device in a 5G system. Herein, for a specific implementation process of "obtaining the SUPI by the SMF network element", refer to a conventional technology. Details are not described herein.

[00199] For example, both the first information and the SUPI may be carried in a key request message.

[00200] S5014. The AUSF network element generates the MUK based on the first information and the SUPI.

[00201] For example, the AUSF network element obtains, through indexing by using the SUPI, a shared key corresponding to the terminal device. Herein, for descriptions of the shared key, refer to related descriptions of S5012. Details are not described herein again. For a specific implementation process in which the AUSF network element generates the MUK based on the first information and the shared key, refer to related descriptions of S5012. Details are not described herein again.

[00202] S5015. The AUSF network element sends the MUK to the SMF network element. Correspondingly, the SMF network element receives the MUK from the AUSF network element.

[00203] For example, the MUK is carried in the key response message.

[00204] In other words, when the key generation network element is implemented as the SMF network element, the SMF network element can provide at least one of an identifier of the multicast user-plane processing network element, a first parameter, and an ID of the multicast service for the AUSF network element, so that the AUSF network element generates the MUK. In this way, the SMF network element can obtain the MUK from the AUSF network element, and then distribute the MUK to the multicast user-plane processing network element.

[00205] It should be noted that if the AUSF network element cannot generate the MUK, the AUSF network element sends a failure message to the SMF network element. Correspondingly, the SMF network element receives the failure message from the AUSF network element. The failure message includes a failure cause value. The failure cause value indicates a reason why the AUSF cannot generate the MUK, for example, a derivation parameter stored in the AUSF network element is unavailable.

[00206] S502. The key generation network element sends the MUK to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the MUK from the key generation network element.

[00207] For example, the MUK is carried in a key notification (notification) message. After the multicast user-plane processing network element receives the key notification message from the key generation network element, the multicast user-plane processing network element sends a response message to the key generation network element. Correspondingly, the key generation network element receives the response message from the multicast user-plane processing network element. The response message indicates that the multicast user-plane processing network element has received the MUK.

[00208] In some embodiments, the key generation network element sends time information corresponding to the MUK to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the time information corresponding to the MUK from the key generation network element. The time information corresponding to the MUK indicates valid time of the MUK. To be specific, within the valid time of the MUK, the multicast user-plane processing network element uses the MUK to protect distribution of the target MSK. In this way, the terminal device can obtain the target MSK. On the contrary, the MUK is invalid beyond the valid time of the MUK, and the multicast user-

plane processing network element no longer distributes the target MSK. In this case, the terminal device cannot obtain the target MSK.

[00209] Therefore, when the key generation network element provides the MUK for the multicast user-plane processing network element, the key generation network element can further indicate the valid time of the MUK, to meet use requirements of the multicast user-plane processing network element in different time periods.

[00210] In some embodiments, the key generation network element can further determine a target security policy, and provide the target security policy for the multicast user-plane processing network element. A specific implementation process is shown in S503 and S504 in FIG. 5A and FIG. 5B.

[00211] S503. The key generation network element determines the target security policy.

[00212] The target security policy includes at least one of a confidentiality protection policy and an integrity protection policy. Herein, the confidentiality protection policy indicates whether encryption protection is to be performed on data between the terminal device and the multicast user-plane processing network element. The integrity protection policy indicates whether integrity protection is to be performed on the data between the terminal device and the multicast user-plane processing network element.

[00213] For example, there are two types of target security policies. A first type of target security policy includes two possible cases: "required" and "not required". Herein, "required" means that security protection between the terminal device and the multicast user-plane processing network element needs to be performed. "Not required" means that security protection between the terminal device and the multicast user-plane processing network element does not need to be performed. A second type of target security policy includes three possible cases: "required", "not required", and "preferred (preferred)". Herein, meanings of "required" and "not required" are the same as those in the "first type of target security policy". Details are not described herein again. "Preferred" means that security protection between the terminal device and the multicast user-plane processing network element may or may not be performed.

[00214] For example, a specific implementation process of S503 may be, for example, but is not limited to, the following example 1 and example 2:

[00215] Example 1: The key generation network element determines the target security policy based on a transmission status of a target MTK and a basic policy.

[00216] There are two transmission statuses of the target MTK: The multicast user-plane processing network element sends the target MTK (or second information for generating the target MTK, where for details, refer to descriptions in S1002) to the terminal device, and the multicast user-plane processing network element does not need to send the target MTK (or the second information for generating the target MTK) to the terminal device.

[00217] The basic policy includes a multicast security policy in a multicast context or a user plane security policy in UDM subscription data. Herein, for a specific implementation process in which the key generation network element (for example, an SMF network element) obtains the "multicast security policy in the multicast context", refer to related descriptions of step 5 in FIG.

3. Details are not described herein again. For a specific implementation process in which the key generation network element (for example, an SMF network element) obtains the "user plane security policy in the UDM subscription data", refer to related descriptions of step 5 in FIG. 3. Details are not described herein again.

[00218] Herein, in Example 1, S503 may be specifically implemented as the following step 1 and step 2.

[00219] Step 1. The key generation network element determines a type of the target security policy based on the transmission status of the target MTK.

[00220] When the target MTK does not need to be generated or transmitted, the key generation network element determines that the type of the target security policy is the first type. In other words, the target security policy includes two possible cases: "required" and "not required". On the contrary, when the target MTK is generated and transmitted, the key generation network element determines that the type of the target security policy is the second type. In other words, the target security policy includes three possible cases: "required", "not required", and "preferred".

[00221] Step 2. The key generation network element determines the target security policy based on the type of the target security policy and the basic policy.

[00222] When the key generation network element determines that the type of the target security policy is the first type, if the basic policy indicates that security protection between the terminal device and the multicast user-plane processing network element needs to be performed, the target security policy is consistent with the basic policy, and security protection between the terminal device and the multicast user-plane processing network element is enabled. If the basic policy indicates that security protection between the terminal device and the multicast user-plane

processing network element does not need to be performed, the target security policy is consistent with the basic policy, and security protection between the terminal device and the multicast user-plane processing network element is disabled. If the basic policy indicates "preferred", to be specific, security protection between the terminal device and the multicast user-plane processing network element may or may not be performed, the key generation network element determines the target security policy based on a local configuration, to be specific, determines "whether security protection between the terminal device and the multicast user-plane processing network element is required". For example, when a QoS rule requires that a delay be less than a specific threshold, the key generation network element determines that the target security policy is "not required". In other words, security protection between the terminal device and the multicast user-plane processing network element is not required. As described above, when "security protection between the terminal device and the multicast user-plane processing network element needs to be performed", security protection between the terminal device and the multicast user-plane processing network element is enabled. When "security protection between the terminal device and the multicast user-plane processing network element does not need to be performed", security protection between the terminal device and the multicast user-plane processing network element is disabled. In this way, signaling indicating a "security protection status" does not need to be transmitted between the terminal device and the multicast user-plane processing network element, in other words, the terminal device and the multicast user-plane processing network element do not need to negotiate about a multicast security activation status, to reduce signaling overheads.

[00223] For example, when the key generation network element determines that the type of the target security policy is the second type, the key generation network element may determine that the target security policy is consistent with the basic policy. To be specific, if the basic policy indicates that security protection between the terminal device and the multicast user-plane processing network element needs to be performed, security protection between the terminal device and the multicast user-plane processing network element is enabled. If the basic policy indicates that security protection between the terminal device and the multicast user-plane processing network element does not need to be performed, security protection between the terminal device and the multicast user-plane processing network element is disabled. If the basic policy indicates "preferred", to be specific, security protection between the terminal device and the multicast user-plane processing network element may or may not be performed, the target security

policy still indicates "preferred". In this case, the multicast user-plane processing network element determines "whether to perform security protection", and then the multicast user-plane processing network element notifies the terminal device of "whether to perform security protection". For details, refer to related descriptions of S5121. Details are not described herein again.

5 **[00224]** In this way, the key generation network element can determine the target security policy based on the basic policy and the transmission status of the target MTK, to provide the target security policy for the multicast user-plane processing network element.

10 **[00225]** Example 2: When the key generation network element is used as a network element for determining a security protection status, the multicast user-plane processing network element does not need to determine "whether to perform security protection", and the multicast user-plane processing network element no longer notifies the terminal device of "whether to perform security protection". Herein, there are two types of security protection: data encryption protection and integrity protection. The "security protection status" means that security protection between the terminal device and the multicast user-plane processing network element is enabled or disabled,
15 for example, data encryption protection is enabled or disabled, or integrity protection is enabled or disabled. In this case, the key generation network element determines that the type of the target security policy is the first type. In other words, the target security policy includes two possible cases: "required" and "not required". Then, the key generation network element determines the target security policy based on the type of the target security policy and a basic policy. For details,
20 refer to related descriptions of step 2 in Example 1. Details are not described herein again.

25 **[00226]** It should be noted that a network element that determines the target security policy and the key generation network element may be the same, similar to the specific implementation process described in S503. Certainly, the network element that determines the target security policy and the key generation network element may alternatively be different network elements. A specific process is consistent with that described in S503 and S504, and only network elements that perform the processing process are different.

30 **[00227]** S504. The key generation network element sends the target security policy to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the target security policy from the key generation network element.

30 **[00228]** For example, when the target security policy is implemented as the confidentiality

protection policy, the key generation network element indicates, to the multicast user-plane processing network element, whether to perform data encryption protection, or the key generation network element indicates the multicast user-plane processing network element to determine whether to perform data encryption protection. When the target security policy is implemented as the integrity protection policy, the key generation network element indicates, to the multicast user-plane processing network element, whether to perform data integrity protection, or the key generation network element indicates the multicast user-plane processing network element to determine whether to perform data integrity protection.

[00229] In this way, the key generation network element can provide the target security policy for the multicast user-plane processing network element, so that the multicast user-plane processing network element performs security protection on multicast service data based on the target security policy.

[00230] In some embodiments, the key generation network element can further send a security algorithm to the multicast user-plane processing network element. A specific implementation process is shown in S505 and S506 in FIG. 5A and FIG. 5B.

[00231] S505. The key generation network element determines the security algorithm.

[00232] The security algorithm is for data security protection calculation.

[00233] For example, the security algorithm includes an encryption algorithm and an integrity protection algorithm. The security algorithm may be coupled with the target security policy. For example, when the target security policy is implemented as the confidentiality protection policy, the security algorithm is the encryption algorithm. When the target security policy is implemented as the integrity protection policy, the security algorithm is the integrity protection algorithm. Certainly, the security algorithm may alternatively be decoupled from the target security policy. For example, when the key generation network element provides the security algorithm for the multicast user-plane processing network element in advance, the security algorithm is at least one of the encryption algorithm and the integrity protection algorithm.

[00234] S506. The key generation network element sends the security algorithm to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the security algorithm from the key generation network element.

[00235] For example, when the target security policy is implemented as the confidentiality protection policy, the key generation network element sends the encryption algorithm to the

multicast user-plane processing network element. When the target security policy is implemented as the integrity protection policy, the key generation network element sends the integrity protection algorithm to the multicast user-plane processing network element.

[00236] In this way, the key generation network element can provide the security algorithm for the multicast user-plane processing network element, so that the multicast user-plane processing network element performs security protection on the multicast service data by using the security algorithm.

[00237] It should be noted that the MUK, the time information corresponding to the MUK, the target security policy, and the security algorithm may be carried in a same message, for example, a key notification message, or may be carried in different messages. This is not limited in embodiments of this application.

[00238] In some embodiments, the key generation network element can further send the first information to the terminal device, so that the terminal device determines the MUK. A specific implementation process is shown in S507 to S509 in FIG. 5A and FIG. 5B.

[00239] S507. The key generation network element sends the first information to an access network device. Correspondingly, the access network device receives the first information from the key generation network element.

[00240] For descriptions of the "first information", refer to related descriptions of S5011. Details are not described herein again. Optionally, the first information further includes service configuration information. Herein, for descriptions of the "service configuration information", refer to related descriptions of step 6 in FIG. 3. Details are not described herein again.

[00241] For example, when the key generation network element is implemented as the SMF network element, the SMF network element sends the first information to an AMF network element. Correspondingly, the AMF network element receives the first information from the SMF network element. The AMF network element sends the first information to the access network device. Correspondingly, the access network device receives the first information from the AMF network element.

[00242] For another example, when the key generation network element is implemented as the AMF network element, the AMF network element sends the first information to the access network device. Correspondingly, the access network device receives the first information from the AMF network element. For example, the first information is carried in a session modification request.

[00243] For another example, when the key generation network element is implemented as the AUSF network element, the AUSF network element sends the first information to an SMF network element. Correspondingly, the SMF network element receives the first information from the AUSF network element. The SMF network element sends the first information to the AMF network element. Correspondingly, the AMF network element receives the first information from the SMF network element. The AMF network element sends the first information to the access network device. Correspondingly, the access network device receives the first information from the AMF network element.

[00244] S508. The access network device sends the first information to the terminal device.

Correspondingly, the terminal device receives the first information from the access network device.

[00245] For example, the first information is carried in an RRC reconfiguration message. Herein, for an implementation process of "sending, by the access network device, the RRC reconfiguration message to the terminal device", refer to related descriptions of step 8 in FIG. 3. Details are not described herein again.

[00246] S509. The terminal device generates the MUK based on the first information and a shared key.

[00247] For descriptions of the shared key, refer to related descriptions of S5012. Details are not described herein again. For a specific implementation process of S509, refer to related descriptions of S5012. Details are not described herein again.

[00248] It should be noted that when the key generation network element determines that the type of the target security policy is the first type, the key generation network element sends the target security policy to the terminal device. Correspondingly, the terminal device receives the target security policy from the key generation network element. When the key generation network element determines that the type of the target security policy is the second type, the key generation network element may no longer send the target security policy to the terminal device. Alternatively, the terminal device receives security protection status information from the multicast user-plane processing network element. Similarly, when the key generation network element determines the security algorithm, the key generation network element sends the security algorithm to the terminal device. Correspondingly, the terminal device receives the security algorithm from the key generation network element. When the key generation network element determines that the type of the target security policy is the second type, the key generation network element may no longer

send the security algorithm to the terminal device. Alternatively, the terminal device receives the security algorithm from the multicast user-plane processing network element. Herein, the target security policy, the security algorithm, and the first information may be carried in a same message, or may be carried in different messages. This is not limited in embodiments of this application.

5 When the target security policy is transmitted to the terminal device in a control plane message, the multicast user-plane processing network element does not need to provide the target security policy for the terminal device. Similarly, when the security algorithm is transmitted to the terminal device in a control plane message, the multicast user-plane processing network element does not need to provide the security algorithm for the terminal device.

10 **[00249]** Certainly, it is easy to understand that, regardless of whether the target security policy is of the first type or the second type, the SMF may send neither the target security policy nor the security algorithm to the terminal device, and the multicast user-plane processing network element provides the target security policy and the security algorithm for the terminal device. For details, refer to specific descriptions of S512 to S515. Details are not described herein again.

15 **[00250]** The foregoing is mainly related descriptions of "MUK negotiation". In this phase, both the terminal device and the multicast user-plane processing network element obtain the MUK.

[00251] Phase 2: MSK-level key negotiation. In this phase, both the multicast user-plane processing network element and the terminal device obtain a target key, such as the target MSK, a first sub-key, and a second sub-key. For a specific implementation process, refer to related
20 descriptions of S510 to S515.

[00252] S510. The multicast user-plane processing network element obtains the target key.

[00253] For example, the multicast user-plane processing network element generates the target key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

25 **[00254]** For another example, after the key generation network element obtains the target key, the key generation network element sends the target key to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the target key from the key generation network element. For details, refer to related descriptions of S1201 and S1202 in FIG. 12. Details are not described herein.

30 **[00255]** S511. The multicast user-plane processing network element sends the target key to the terminal device. Correspondingly, the terminal device receives the target key from the multicast

user-plane processing network element.

[00256] For example, the target key is carried in a key distribution message. Herein, the key distribution message is a multimedia internet key (multimedia internet key, MIKEY) message. When the multicast user-plane processing network element provides the target key for the terminal device, the target key is carried in a user plane message, and the terminal device obtains the target key from the user plane message.

[00257] In some embodiments, the MUK protects distribution of the target key. A specific implementation process of S511 may be replaced with S5111 to S5113 shown in FIG. 7(a).

[00258] S5111. The multicast user-plane processing network element encrypts the target key by using the MUK, to obtain key information.

[00259] For example, at a moment 1, the terminal device is allowed to access the multicast service. The multicast user-plane processing network element encrypts the target key by using an MUK corresponding to the moment 1, to obtain the key information. Herein, the moment 1 is within a valid time range of the MUK.

[00260] S5112. The multicast user-plane processing network element sends the key information to the terminal device. Correspondingly, the terminal device receives the key information from the multicast user-plane processing network element.

[00261] For example, the key information is carried in the key distribution message.

[00262] S5113. The terminal device decrypts the key information by using the MUK, to obtain the target key.

[00263] For example, at a moment 1, the terminal device is allowed to access the multicast service. The terminal device has an MUK corresponding to the moment 1. In this way, the terminal device can decrypt the key information by using the MUK corresponding to the moment 1, to obtain the target key.

[00264] In other words, key information sent by the multicast user-plane processing network element to different terminal devices is encrypted by using different MUKs. In this way, a terminal device can obtain a target key based on an MUK owned by the terminal device, to improve transmission reliability of the target key.

[00265] In some embodiments, to enable the terminal device to obtain an identifier of the target MSK, this embodiment of this application provides two possible implementations, which are specifically described in the following case 1 and case 2:

[00266] Case 1: The multicast user-plane processing network element sends the identifier of the target MSK to the terminal device. Correspondingly, the terminal device receives the identifier of the target MSK from the multicast user-plane processing network element.

[00267] For example, the identifier of the target MSK includes two parts: the "ID of the multicast service" and a "key number part (key number part)". That is, when the identifier of the target MSK is implemented as "ID of the multicast service + key number part", "ID of the multicast service + key number part" is transmitted from the multicast user-plane processing network element to the terminal device. Herein, for descriptions of the "ID of the multicast service", refer to related descriptions of S5011. Details are not described herein again.

[00268] In this way, the terminal device can obtain the identifier of the target MSK from the multicast user-plane processing network element.

[00269] Case 2: First, the multicast user-plane processing network element sends a key number part to the terminal device. Correspondingly, the terminal device receives the key number part from the multicast user-plane processing network element. Then, the terminal device determines the identifier of the target MSK based on the key number part and the ID of the multicast service.

[00270] That the identifier of the target MSK is implemented as "ID of the multicast service + key number part" is still used as an example. The key number part is transmitted from the multicast user-plane processing network element to the terminal device. The terminal device may restore the identifier of the target MSK based on the obtained "ID of the multicast service" and the obtained key number part.

[00271] In this way, when the multicast user-plane processing network element provides the key number part for the terminal device, the terminal device can also determine the identifier of the target MSK. Compared with transmitting the "identifier of the target MSK", this reduces transmission resource overheads.

[00272] In some embodiments, the multicast user-plane processing network element can further determine the security protection status information, and provide the security protection status information for the terminal device. A specific implementation process is shown in S512 and S513 in FIG. 5A and FIG. 5B.

[00273] S512. The multicast user-plane processing network element determines the security protection status information.

[00274] The security protection status information indicates a security protection status. The

security protection includes at least one of data encryption and integrity verification. For example, the security protection status information indicates that data encryption protection is enabled or disabled, and/or the security protection status information indicates that integrity verification is enabled or disabled.

5 **[00275]** For example, when the multicast user-plane processing network element performs S504, a specific implementation process of S512 may be, for example, but is not limited to, S504 and S5121 shown in FIG. 7(b). S5121 is specifically described as follows:

[00276] S5121. The multicast user-plane processing network element determines the security protection status information based on the target security policy.

10 **[00277]** For example, when the type of the target security policy is the first type, the multicast user-plane processing network element may determine that the security protection status information is consistent with the target security policy. To be specific, if the target security policy indicates that security protection between the terminal device and the multicast user-plane processing network element needs to be performed, security protection between the terminal
15 device and the multicast user-plane processing network element is enabled. If the target security policy indicates that security protection between the terminal device and the multicast user-plane processing network element does not need to be performed, security protection between the terminal device and the multicast user-plane processing network element is disabled.

[00278] For example, when the type of the target security policy is the second type, if the target
20 security policy indicates that security protection between the terminal device and the multicast user-plane processing network element needs to be performed or does not need to be performed, the multicast user-plane processing network element may determine that the security protection status information is consistent with the target security policy. For details, refer to related descriptions of "the type of the target security policy is the first type". Details are not described
25 herein again. If the target security policy indicates "preferred", to be specific, security protection between the terminal device and the multicast user-plane processing network element may or may not be performed, the multicast user-plane processing network element determines the security protection status information based on a local configuration. In other words, the multicast user-plane processing network element determines, based on the local configuration, to "enable or
30 disable security protection between the terminal device and the multicast user-plane processing network element".

[00279] Optionally, when the key generation network element does not provide the target security policy for the terminal device, the multicast user-plane processing network element performs S513.

[00280] S513. The multicast user-plane processing network element sends the security protection status information to the terminal device. Correspondingly, the terminal device receives the security protection status information from the multicast user-plane processing network element.

[00281] For example, when the security protection status information corresponds to data encryption protection, the multicast user-plane processing network element indicates, to the terminal device, whether to perform data encryption protection. When the security protection status information corresponds to integrity verification, the multicast user-plane processing network element indicates, to the terminal device, whether to perform integrity verification.

[00282] In this way, the multicast user-plane processing network element can provide the security protection status information for the terminal device, so that the terminal device processes target data based on the security protection status information.

[00283] In some embodiments, when the key generation network element does not provide the security algorithm for the terminal device, the multicast user-plane processing network element can further determine a security algorithm, and provide the security algorithm for the terminal device. A specific implementation process is shown in S514 and S515 in FIG. 5A and FIG. 5B.

[00284] S514. The multicast user-plane processing network element determines the security algorithm.

[00285] The security algorithm is for data security protection calculation.

[00286] For example, the security algorithm includes an encryption algorithm and an integrity protection algorithm. The security algorithm may be coupled with the security protection status information. For example, when the security protection status information corresponds to confidentiality protection, the security algorithm is the encryption algorithm. When the security protection status information corresponds to integrity protection, the security algorithm is the integrity protection algorithm. Certainly, the security algorithm may alternatively be decoupled from the security protection status information. For example, when the multicast user-plane processing network element provides the security algorithm for the terminal device in advance, the security algorithm is at least one of the encryption algorithm and the integrity protection

algorithm.

[00287] S515. The multicast user-plane processing network element sends the security algorithm to the terminal device. Correspondingly, the terminal device receives the security algorithm from the multicast user-plane processing network element.

5 **[00288]** For example, when the security protection status information corresponds to confidentiality protection, the multicast user-plane processing network element sends the encryption algorithm to the terminal device. When the security protection status information corresponds to integrity protection, the multicast user-plane processing network element sends the integrity protection algorithm to the terminal device.

10 **[00289]** In this way, the multicast user-plane processing network element can provide the security algorithm for the terminal device, so that the terminal device processes the target data by using the security algorithm.

[00290] It should be noted that the target key, the key information, the identifier of the target MSK, the key number part, the security protection status information, and the security algorithm
15 may be carried in a same message, for example, an MIKEY message, or may be carried in different messages. This is not limited in embodiments of this application.

[00291] The foregoing is mainly related descriptions of "MSK-level key negotiation". In this phase, after obtaining the target key, the multicast user-plane processing network element can further provide the target key for the terminal device. In this way, both the multicast user-plane
20 processing network element and the terminal device obtain the target key. Certainly, it is easy to understand that "phase 2: MSK-level key negotiation" shown in FIG. 5A and FIG. 5B may also be replaced with "phase 1: MSK-level key negotiation" shown in FIG. 12. For a specific implementation process, refer to related descriptions of S1201 to S1204 in FIG. 12. Details are not described herein.

25 **[00292]** Phase 3: Data transmission. In this phase, the multicast user-plane processing network element provides the target data for the terminal device. For a specific implementation process, refer to related descriptions of S516 to S518.

[00293] S516. The multicast user-plane processing network element performs security protection on the multicast service data by using the target key, to obtain the target data.

30 **[00294]** For descriptions of the target key, refer to related descriptions of S510. Details are not described herein again. If the multicast user-plane processing network element performs "data

encryption" protection but does not perform "integrity verification", the target data includes ciphertext and does not include a message authentication code (message authentication code, MAC). If the multicast user-plane processing network element does not perform "data encryption" protection but performs "integrity verification", the target data includes the multicast service data (which may also be referred to as plaintext) and a MAC. If the multicast user-plane processing network element performs "data encryption" protection and "integrity verification", the target data includes ciphertext and a MAC.

[00295] There are a plurality of specific implementations of S516, and the implementations may be, for example, but are not limited to, descriptions in the following four aspects:

[00296] First: In terms of a security protection trigger condition, the multicast user-plane processing network element performs security protection only when "the status indicated by the security protection status information is enabled". That is, a specific implementation of S516 is: If the status indicated by the security protection status information is enabled, the multicast user-plane processing network element performs security protection on the multicast service data by using the target key, to obtain the target data. In other words, the multicast user-plane processing network element performs security protection on the multicast service data only when security protection between the terminal device and the multicast user-plane processing network element is enabled, to ensure secure transmission of the multicast service data.

[00297] Second: In terms of the security algorithm corresponding to security protection, the multicast user-plane processing network element performs security protection only when obtaining the "security algorithm". For example, when "the multicast user-plane processing network element performs S506" or "the multicast user-plane processing network element receives the security algorithm from the AMF network element", S516 is specifically implemented as follows: The multicast user-plane processing network element performs security protection on the multicast service data by using the security algorithm and the target key, to obtain the target data. Herein, when the security algorithm is implemented as the "encryption algorithm", the multicast user-plane processing network element encrypts the multicast service data by using the encryption algorithm and the target key, to obtain the ciphertext. When the security algorithm is implemented as the "integrity protection algorithm", the multicast user-plane processing network element determines the MAC based on the integrity protection algorithm and the multicast service data. In other words, the multicast user-plane processing network element performs security protection on the multicast

service data only when the multicast user-plane processing network element has the security algorithm, to ensure secure transmission of the multicast service data.

[00298] Third: In terms of a security protection type, security protection includes two types: data encryption and integrity verification.

5 **[00299]** When the multicast user-plane processing network element performs "data encryption" protection, the multicast user-plane processing network element encrypts the multicast service data by using the target MSK or the first sub-key, to obtain the ciphertext. The target data includes the ciphertext. Herein, a specific implementation process of encryption may be: inputting the target MSK (or the first sub-key) and the multicast service data into the encryption algorithm for
10 performing an operation, to obtain the ciphertext. In an actual application process, the multicast user-plane processing network element further inputs another information element into the encryption algorithm. For a specific implementation process, refer to a conventional technology. Details are not described herein again.

[00300] When the multicast user-plane processing network element performs "integrity
15 verification", the multicast user-plane processing network element determines the MAC based on the multicast service data and at least one of the target MSK and the second sub-key. The target data includes the MAC. Herein, a specific implementation process of "determining the MAC" may be: inputting the target MSK (or the second sub-key) and the multicast service data into the integrity protection algorithm, to obtain the MAC. In an actual application process, the multicast
20 user-plane processing network element further inputs another information element into the integrity protection algorithm. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00301] In this way, if the multicast user-plane processing network element performs "data encryption" protection on the multicast service data, an effect of hiding the data can be achieved.
25 If the multicast user-plane processing network element performs "integrity verification" on the multicast service data, data tampering can be avoided.

[00302] Fourth: In terms of a key for performing security protection, the key for performing security protection may be the target MSK, or may be a first derivation key determined based on the target MSK, for example, the first sub-key corresponding to the target MSK or the second sub-
30 key corresponding to the target MSK. "Performing security protection on the multicast service data by using the first derivation key" is used as an example. Refer to FIG. 8. S516 may be

specifically implemented as S5161 and S5162.

[00303] S5161. The multicast user-plane processing network element performs a derivation operation on the target MSK to obtain the first derivation key.

[00304] An algorithm of the derivation operation may be an HMAC algorithm. Herein, the first derivation key includes the first sub-key and the second sub-key. For example, S5161 may be specifically implemented as the following Example 1 and Example 2:

[00305] Example 1: The multicast user-plane processing network element performs a first derivation operation on the target MSK to obtain the first sub-key.

[00306] The first derivation key includes the first sub-key, and the first sub-key is for confidentiality protection calculation and is denoted as MSK_enc. For example, the multicast user-plane processing network element uses the target MSK as an input key, uses the encryption algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the first sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00307] In this way, the multicast user-plane processing network element can obtain the first sub-key in a derivation manner by using the target MSK, to perform security protection on the multicast service data.

[00308] Example 2: The multicast user-plane processing network element performs a second derivation operation on the target MSK to obtain the second sub-key.

[00309] The first derivation key includes the second sub-key, and the second sub-key is for integrity protection calculation and is denoted as MSK_int. For example, the multicast user-plane processing network element uses the target MSK as an input key, uses the integrity protection algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the second sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00310] In this way, the multicast user-plane processing network element can obtain the second sub-key in a derivation manner by using the target MSK, to perform security protection on the multicast service data.

[00311] S5162. The multicast user-plane processing network element performs security protection on the multicast service data by using the first derivation key, to obtain the target data.

[00312] For example, the multicast user-plane processing network element performs encryption

protection on the multicast service data by using the first sub-key, to obtain the ciphertext. In this case, the target data includes the ciphertext.

[00313] For another example, the multicast user-plane processing network element performs integrity protection on the multicast service data by using the second sub-key, to obtain the MAC.

5 In this case, the target data includes the MAC.

[00314] In this way, the multicast user-plane processing network element can further derive the target MSK, and perform security protection by using the first derivation key.

[00315] S517. The multicast user-plane processing network element sends the target data to the terminal device. Correspondingly, the terminal device receives the target data from the multicast user-plane processing network element.

10 **[00316]** In an actual application process, the multicast user-plane processing network element sends the target data to the access network device. Correspondingly, the access network device receives the target data from the multicast user-plane processing network element. The access network device sends the target data to the terminal device. Correspondingly, the terminal device

15 receives the target data from the access network device.

[00317] S518. The terminal device processes the target data by using the target key, to obtain a processing result of the target data.

[00318] For descriptions of the target key, refer to related descriptions of S510. Details are not described herein again.

20 **[00319]** For example, the target data includes an identifier of the target key (for example, the target MSK), and the terminal device obtains the target key through indexing based on the identifier of the target key in the target data. The terminal device processes the target data by using the target key (that is, the target key corresponding to the identifier of the target key) obtained through indexing. In other words, when the target data carries the identifier of the target key, the

25 identifier of the target key in the target data can indicate a specific key used by the terminal device to process the target data, so that the terminal device can obtain, through indexing, the target key corresponding to the identifier of the target key in the target data.

[00320] If the target data includes the ciphertext but does not include the MAC, the terminal device performs "data decryption", to obtain the multicast service data (which may also be referred to as a plaintext). If the target data includes the multicast service data (which may also be referred to as a plaintext) and the MAC, the terminal device performs "integrity verification", to verify

30

integrity of the multicast service data. If the target data includes the ciphertext and the MAC, the terminal device performs "data decryption" and "integrity verification", to verify integrity of the multicast service data corresponding to the ciphertext.

[00321] There are a plurality of specific implementations of S518, and the implementations may be, for example, but are not limited to, descriptions in the following four aspects:

[00322] First: In terms of a trigger condition for performing processing by the terminal device, the terminal device performs processing only when "the status indicated by the security protection status information is enabled". That is, a specific implementation of S518 is: If the status indicated by the security protection status information is enabled, the terminal device processes the target data by using the target key, to obtain the processing result of the target data. Alternatively, the terminal device performs processing, that is, S518, only when "the security protection status indicated by the target security policy is enabled". In other words, the terminal device processes the target data only when security protection between the terminal device and the multicast user-plane processing network element is enabled, to improve data processing efficiency.

[00323] Second: In terms of a security algorithm used by the terminal device to perform processing, the terminal device performs processing only when obtaining the "security algorithm". For example, when the terminal device obtains the security algorithm from the key generation network element or performs S515, S518 is specifically implemented as follows: The terminal device processes the target data by using the security algorithm and the target key, to obtain the processing result of the target data. Herein, when the security algorithm is implemented as the "encryption algorithm", the terminal device decrypts the target data by using the encryption algorithm and the target key, to obtain the plaintext. When the security algorithm is implemented as the "integrity protection algorithm", the terminal device verifies integrity of the multicast service data based on the integrity protection algorithm and the MAC. In other words, the terminal device processes the target data only when the terminal device has the security algorithm, to obtain the processing result of the target data.

[00324] Third: In terms of a processing type of processing performed by the terminal device, the processing type of processing performed by the terminal device includes two types: data decryption and integrity verification.

[00325] When the target data includes the ciphertext but does not include the MAC, the terminal device performs "data decryption", that is, the terminal device decrypts the ciphertext by using the

target MSK or the first sub-key, to obtain first plaintext. The processing result of the target data includes the first plaintext. Herein, a specific implementation process of the decryption may be: inputting the target MSK (or the first sub-key) and the ciphertext into the encryption algorithm for processing, to obtain the first plaintext. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00326] When the target data includes second plaintext and the MAC, the terminal device performs "integrity verification", that is, the terminal device determines integrity of the second plaintext based on the MAC and at least one of the target MSK and the second sub-key. The processing result of the target data includes integrity of the second plaintext. Herein, a specific implementation process of the integrity verification may be: inputting the target MSK (or the second sub-key) and the second plaintext into the integrity protection algorithm, to obtain a MAC. The terminal device compares whether the received MAC is the same as the MAC calculated by the terminal device. If the MACs are the same, the verification succeeds. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00327] When the target data includes the ciphertext and the MAC, the terminal device performs "data decryption" and "integrity verification", that is, the terminal device decrypts the ciphertext by using the target MSK or the first sub-key, to obtain first plaintext. The terminal device determines integrity of the first plaintext based on the MAC and at least one of the target MSK and the second sub-key.

[00328] In this way, when the data is hidden, that is, the target data includes the ciphertext, the terminal device can decrypt the target data to obtain the plaintext. When the target data includes the MAC, the terminal device can perform "integrity verification" on the target data, to verify data integrity and avoid data tampering.

[00329] Fourth: In terms of a key for performing processing, the key for performing processing may be the first derivation key determined based on the target MSK, for example, the first sub-key corresponding to the target MSK or the second sub-key corresponding to the target MSK. "Processing the target data by using the first derivation key" is used as an example. Refer to FIG. 9. S518 may be specifically implemented as S5181 and S5182.

[00330] S5181. The terminal device performs a derivation operation on the target MSK to obtain a first derivation key

[00331] An algorithm of the derivation operation may be an HMAC algorithm. Herein, the first

derivation key includes the first sub-key and the second sub-key. Herein, a specific implementation process of S5181 is consistent with that of S5161. To be specific, an execution body is the terminal device. Specifically, the following descriptions are provided by using Example 1 and Example 2:

[00332] Example 1: The terminal device performs a first derivation operation on the target MSK to obtain the first sub-key.

[00333] The first derivation key includes the first sub-key, and the first sub-key is for confidentiality protection calculation and is denoted as MSK_enc. For example, the terminal device uses the target MSK as an input key, uses the encryption algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the first sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00334] In this way, the terminal device can obtain the first sub-key by using the target MSK in a derivation manner, to decrypt the target data.

[00335] Example 2: The terminal device performs a second derivation operation on the target MSK to obtain the second sub-key.

[00336] The first derivation key includes the second sub-key, and the second sub-key is for integrity protection calculation and is denoted as MSK_int. For example, the terminal device uses the target MSK as an input key, uses the integrity protection algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the second sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00337] In this way, the terminal device can obtain the second sub-key by using the target MSK in a derivation manner, to perform integrity verification on the target data.

[00338] S5182. The terminal device processes the target data by using the first derivation key, to obtain the processing result of the target data.

[00339] For example, when the target data includes the ciphertext, the terminal device processes the target data by using the first sub-key, to obtain the ciphertext.

[00340] For another example, when the target data includes the MAC, the terminal device verifies integrity of the multicast service data based on the second sub-key and the MAC.

[00341] In this way, the terminal device can further derive the target MSK, and perform processing by using the first derivation key.

[00342] The foregoing is mainly related descriptions of "data transmission". In this phase, the multicast user-plane processing network element provides the target data on which security protection is performed for the terminal device, to achieve an effect of hiding data or reduce a possibility of data tampering.

5 **[00343]** In some embodiments, the multicast user-plane processing network element can further determine a generation status of the target MTK, as shown in S519 in FIG. 5A and FIG. 5B.

[00344] S519. The multicast user-plane processing network element determines the generation status of the target MTK.

[00345] For example, the multicast user-plane processing network element receives a message
10 from the terminal device. The message from the terminal device includes a session type or a transport protocol type. The multicast user-plane processing network element uses the session type or the transport protocol type as a determining basis. If the session type is a download type or a streaming type, the multicast user-plane processing network element determines to generate the target MTK. On the contrary, if the transport protocol type is not the download type or the
15 streaming type, the multicast user-plane processing network element determines that the target MTK is not required. If the transport protocol type is the RTP, the FLUTE, or another protocol, the multicast user-plane processing network element determines to generate the target MTK. On the contrary, if the transport protocol type is not the RTP or the FLUTE, the multicast user-plane processing network element determines that the target MTK is not required.

20 **[00346]** For another example, the multicast user-plane processing network element receives a message from the SMF network element. The message from the SMF network element includes a transport protocol indication or a quality of service (quality of service, QoS) parameter. Alternatively, the multicast user-plane processing network element receives a message from the AF network element. The message from the AF network element includes a transport protocol
25 indication. If a transport protocol type in the transport protocol indication is the RTP, the FLUTE, or another protocol, the multicast user-plane processing network element determines to generate the target MTK. On the contrary, if the transport protocol type in the transport protocol indication is not the RTP or the FLUTE, the multicast user-plane processing network element determines that the target MTK is not required. If a traffic type parameter in the QoS parameter is a download type
30 or a streaming type, the multicast user-plane processing network element determines to generate the target MTK. On the contrary, if the traffic type parameter in the QoS parameter is not the

download type or the streaming type, the multicast user-plane processing network element determines that the target MTK does not need to be generated.

[00347] For another example, the multicast user-plane processing network element determines the generation status of the target MTK based on a network type. If the network type is an LTE network or a network before the LTE network, the multicast user-plane processing network element determines to generate the target MTK. If the network type is a 5G network or a network after the 5G network, the multicast user-plane processing network element determines that the target MTK does not need to be generated.

[00348] Herein, before performing the phase 3, the multicast user-plane processing network element may perform S519 to determine the generation status of the target MTK.

[00349] In other words, the multicast user-plane processing network element can independently determine whether to generate the target MTK. If the target MTK is not generated, the multicast user-plane processing network element performs "phase 3: data transmission", to perform security protection on the multicast service data by using the target key, to obtain the target data.

[00350] The following describes a second key management method provided in embodiments of this application by using an example in which a target MTK is generated. The key management method is applied to an MBS communication process. A terminal device completes a registration process and a PDU session establishment process, and joins a multicast service. For details, refer to related descriptions of step 1 to step 5 in FIG. 3. Details are not described herein again. After joining the multicast service, the terminal device performs a key management method shown in FIG. 10. Specific steps are as follows:

[00351] For descriptions of the phase 1 and the phase 2, refer to related descriptions of the "first key management method". Details are not described herein again.

[00352] Phase 3: MTK-level key negotiation. In this phase, both a multicast user-plane processing network element and the terminal device obtain a target MTK or a sub-key corresponding to the target MTK. A specific process is shown in S1001 to S1006 in FIG. 10.

[00353] S1001. The multicast user-plane processing network element performs a derivation operation on the target MSK and second information to obtain a second derivation key.

[00354] The second information includes at least one of the following: a protocol name, an identifier of the target MTK, or a second parameter. Herein, the protocol name may be RTP or FULTE. The identifier of the target MTK may be generated and maintained by the multicast user-

plane processing network element. The identifier of the target MTK may be counted from 1. The second parameter may be a parameter determined based on at least one of a second random number, a second count value, or a second timestamp. For example, the second parameter is the second random number, the second count value, or the second timestamp. The second parameter is generated and maintained by the multicast user-plane processing network element.

[00355] The second derivation key includes the target MTK, a third sub-key, or a fourth sub-key. For example, S1001 may be specifically implemented as the following Example 1 to Example 3:

[00356] Example 1: The multicast user-plane processing network element performs a third derivation operation on the target MSK and the second information to obtain the target MTK.

[00357] For example, the multicast user-plane processing network element uses the target MSK as an input key, uses the second information as an input parameter, and performs a second derivation operation by using an HMAC algorithm, to obtain the target MTK. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00358] In this way, the multicast user-plane processing network element may obtain the target MTK in a derivation manner by using the target MSK, to perform encryption protection or integrity protection on multicast service data.

[00359] Example 2: First, the multicast user-plane processing network element performs a third derivation operation on the target MSK and the second information, to obtain the target MTK, or the multicast user-plane processing network element locally generates the target MTK. Then, the multicast user-plane processing network element performs a fourth derivation operation on the target MTK to obtain the third sub-key. For example, the multicast user-plane processing network element uses the target MTK as an input key, uses an encryption algorithm as an input parameter, and performs a derivation operation by using an HMAC algorithm, to obtain the third sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein. The third sub-key is for confidentiality protection calculation.

[00360] In this way, the multicast user-plane processing network element can obtain the third sub-key in a derivation manner by using the target MSK, to perform encryption protection on multicast service data.

[00361] Example 3: First, the multicast user-plane processing network element performs a third derivation operation on the target MSK and the second information, to obtain the target MTK, or

the multicast user-plane processing network element locally generates the target MTK. Then, the multicast user-plane processing network element performs a fifth derivation operation on the target MTK to obtain the fourth sub-key. For example, the multicast user-plane processing network element uses the target MTK as an input key, uses the integrity protection algorithm as an input parameter, and performs a derivation operation by using an HMAC algorithm, to obtain the fourth sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein. The fourth sub-key is for integrity protection calculation.

[00362] In this way, the multicast user-plane processing network element can obtain the fourth sub-key in a derivation manner by using the target MSK, to perform integrity protection on multicast service data.

[00363] S1002. The multicast user-plane processing network element sends the second information to the terminal device. Correspondingly, the terminal device receives the second information from the multicast user-plane processing network element.

[00364] For example, the multicast user-plane processing network element sends the second information to an access network device. Correspondingly, the access network device receives the second information from the multicast user-plane processing network element. The access network device sends the second information to the terminal device. Correspondingly, the terminal device receives the second information from the access network device. Herein, the second information may be carried in a multicast message.

[00365] Optionally, as shown in FIG. 11, S1002 may alternatively be replaced with S1003 to S1005.

[00366] S1003. The multicast user-plane processing network element encrypts the second information by using the target MSK, to obtain encrypted information.

[00367] For example, the encrypted information is carried in a multicast message. The multicast message includes two parts: a protected part and an unprotected part. The protected part is the encrypted information, the unprotected part includes an identifier of the target MSK, and the target MSK corresponding to the identifier is a key for encrypting the second information.

[00368] S1004. The multicast user-plane processing network element sends the encrypted information to the terminal device. Correspondingly, the terminal device receives the encrypted information from the multicast user-plane processing network element.

[00369] For example, the encrypted information is carried in a multicast message. The multicast

message further includes the identifier of the target MSK. The target MSK corresponding to the identifier in the multicast message is a key for decrypting the second information.

[00370] For example, the multicast user-plane processing network element sends the encrypted information to the terminal device through the access network device. Correspondingly, the terminal device receives the encrypted information from the multicast user-plane processing network element through the access network device.

[00371] S1005. The terminal device decrypts the encrypted information by using the target MSK, to obtain the second information.

[00372] For example, when the multicast message further includes the identifier of the target MSK, the terminal device obtains the target MSK through indexing based on the identifier of the target key in the multicast message, and decrypts the encrypted information by using the target MSK (that is, the target MSK corresponding to the identifier of the target MSK) obtained through indexing, to obtain the second information.

[00373] Herein, although the second information is distributed by using a multicast message, because the target MSK is transmitted by using a unicast message, the target MSK protects a distribution process of the second information, and the second information is for derivation of the target MTK. In this way, security of the target MTK derived based on the second information is equivalent to security of unicast message transmission.

[00374] It should be noted that the target MTK may alternatively be a random number locally generated by the multicast user-plane processing network element or in another form. When the target MTK is a random number, the multicast user-plane processing network element sends a multicast message to the terminal device. Correspondingly, the terminal device receives the multicast message from the multicast user-plane processing network element. The multicast message also includes a protected part and an unprotected part. The protected part is a part obtained by encrypting the target MTK and the identifier of the target MTK by using the target MSK, and the unprotected part includes the identifier of the target MSK. In addition, when the "MTK-level key negotiation" phase is performed, at least one of "security protection status information" and a "security algorithm" may be transmitted in the "MSK-level key negotiation" phase, or may be transmitted in the "MTK-level key negotiation" phase. For example, at least one of the "security protection status information" and the "security algorithm" is carried in a multicast message. This is not limited in embodiments of this application.

[00375] S1006. The terminal device performs a derivation operation on the target MSK and the second information to obtain the second derivation key.

[00376] For related descriptions of the second information, refer to related descriptions of S1001. Details are not described herein again.

5 **[00377]** The second derivation key includes the target MTK, the third sub-key, or the fourth sub-key. A specific implementation process of S1006 is consistent with a process of S1001. To be specific, an execution body is the terminal device. Specifically, the following descriptions are provided by using Example 1 to Example 3:

[00378] Example 1: The terminal device performs a third derivation operation on the target
10 MSK and the second information to obtain the target MTK.

[00379] For example, the terminal device uses the target MSK as an input key, uses the second information as an input parameter, and performs a second derivation operation by using an HMAC algorithm, to obtain the target MTK. For a specific implementation process, refer to a conventional technology. Details are not described herein.

15 **[00380]** In this way, the terminal device can obtain the target MTK by using the target MSK in a derivation manner, to perform decryption or integrity verification on target data.

[00381] Example 2: First, the terminal device performs a third derivation operation on the target MSK and the second information, to obtain the target MTK, or the terminal device locally generates the target MTK. Then, the terminal device performs a fourth derivation operation on the
20 target MTK to obtain the third sub-key. For example, the terminal device uses the target MTK as an input key, uses the encryption algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the third sub-key. For a specific implementation process, refer to a conventional technology. Details are not described herein.

[00382] In this way, the terminal device can obtain the third sub-key by using the target MSK
25 in a derivation manner, to decrypt target data.

[00383] Example 3: First, the terminal device performs a third derivation operation on the target MSK and the second information, to obtain the target MTK, or the terminal device locally generates the target MTK. Then, the terminal device performs a fifth derivation operation on the target MTK to obtain the fourth sub-key. For example, the terminal device uses the target MTK as
30 an input key, uses the integrity protection algorithm as an input parameter, and performs a derivation operation by using the HMAC algorithm, to obtain the fourth sub-key. For a specific

implementation process, refer to a conventional technology. Details are not described herein. The fourth sub-key is for integrity protection calculation.

[00384] In this way, the terminal device can obtain the fourth sub-key by using the target MSK in a derivation manner, to perform integrity protection on the target data.

5 **[00385]** The foregoing is mainly related descriptions of "MTK-level key negotiation". In this phase, the multicast user-plane processing network element can obtain an MTK-level key, for example, the target MTK, the third sub-key, or the fourth sub-key. Then, the multicast user-plane processing network element can further provide the second information for the terminal device, so that the terminal device determines the MTK-level key. In this way, both the multicast user-plane
10 processing network element and the terminal device obtain the MTK-level key.

[00386] Phase 4: Data transmission. In this phase, the multicast user-plane processing network element provides the target data for the terminal device. For a specific implementation process, refer to related descriptions of S1007 to S1009.

[00387] S1007. The multicast user-plane processing network element performs security
15 protection on multicast service data by using a target key, to obtain the target data.

[00388] Herein, a "security protection trigger condition", a "security algorithm corresponding to security protection", and a "security protection type" are consistent with those in S516. From a perspective of the key for performing security protection, the target key for performing security protection is implemented as the second derivation key, for example, the target MTK, the third
20 sub-key, or the fourth sub-key. For descriptions of the "target MTK, the third sub-key, or the fourth sub-key", refer to related descriptions of S1001. Details are not described herein again.

[00389] S1008. The multicast user-plane processing network element sends the target data to the terminal device. Correspondingly, the terminal device receives the target data from the multicast user-plane processing network element.

25 **[00390]** For a specific implementation process of S1008, refer to descriptions of S517. Details are not described herein again.

[00391] S1009. The terminal device processes the target data by using the target key, to obtain a processing result of the target data.

[00392] Herein, a "trigger condition for performing processing by the terminal device", a
30 "security algorithm used by the terminal device to perform processing", and a "processing type of processing performed by the terminal device" are consistent with those in S518. From a

perspective of the key for performing processing, the target key for performing security protection is implemented as the second derivation key, for example, the target MTK, the third sub-key, or the fourth sub-key. For descriptions of the "target MTK, the third sub-key, or the fourth sub-key", refer to related descriptions of S1006. Details are not described herein again.

5 **[00393]** For example, the target data further includes the identifier of the target MTK. The terminal device obtains the target MTK through indexing based on the identifier in the target data, and the terminal device processes the target data by using the target MTK (the target MTK corresponding to the identifier of the target MTK) obtained through indexing.

[00394] The foregoing is mainly related descriptions of "data transmission". In this phase, the
10 multicast user-plane processing network element provides the target data on which security protection is performed for the terminal device, to achieve an effect of hiding data or reduce a possibility of data tampering.

[00395] An embodiment of this application provides a third key management method, and the key management method is applied to an MBS communication process. A terminal device
15 completes a registration process and a PDU session establishment process, and joins a multicast service. For details, refer to related descriptions of step 1 to step 5 in FIG. 3. Details are not described herein again. After joining the multicast service, the terminal device performs a key management method shown in FIG. 12. Specific steps are as follows:

[00396] Phase 1: MSK-level key negotiation. In this phase, both the terminal device and a
20 multicast user-plane processing network element obtain a target key, for example, a target MSK, a first sub-key, or a second sub-key. For a specific implementation process, refer to related descriptions of S1201 to S1204.

[00397] S1201. A key generation network element obtains the target key.

[00398] For example, the key generation network element initiates a processing process of
25 "obtaining the target key" only when a specific trigger condition is met. Herein, the key generation network element determines, based on a multicast service authentication or authorization result, whether to initiate the processing process of "obtaining the target key". It may be understood that, when multicast service authentication of the key generation network element succeeds or the terminal device is authorized, the key generation network element initiates the processing
30 procedure of "obtaining the target key". On the contrary, when the multicast service authentication of the key generation network element fails or the terminal device is not authorized, the key

generation network element does not initiate the processing process of "obtaining the target key". For descriptions of "multicast service authentication" and "authorization", refer to related descriptions of S501. Details are not described herein again.

[00399] For example, a specific implementation process of "obtaining the target key by the key generation network element" may be, for example, but is not limited to the following:

[00400] The key generation network element performs multicast transmission session check for a UDM network element based on an identifier of the multicast service, that is, checks whether a multicast context (such as QoS information or the target key) corresponding to the identifier of the multicast service exists. For example, the key generation network element is implemented as an SMF network element. The SMF network element sends the identifier of the multicast service (for example, an IP address of the multicast service) to the UDM network element. Correspondingly, the UDM network element receives the identifier of the multicast service from the SMF network element. Then, the UDM network element checks whether the multicast context corresponding to the identifier of the multicast service exists.

[00401] If the UDM network element determines that the multicast context corresponding to the identifier of the multicast service exists, the UDM network element sends the multicast context corresponding to the identifier of the multicast service to the SMF network element. Correspondingly, the SMF network element receives, from the UDM network element, the multicast context corresponding to the identifier of the multicast service. The multicast context corresponding to the identifier of the multicast service includes the target key.

[00402] If the UDM network element determines that the multicast context corresponding to the identifier of the multicast service does not exist, the SMF network element may obtain the target key in the following two manners. Details are as follows:

[00403] Manner 1: The SMF network element generates the target key. For example, the SMF network element generates the target MSK by using a random number. For a specific implementation process, refer to a conventional technology. Details are not described herein. Optionally, after the SMF network element generates the target MSK, the SMF network element performs a first derivation operation on the target MSK, to obtain the first sub-key. For example, the SMF network element uses the target MSK as an input key, uses an encryption algorithm as an input parameter, and performs a derivation operation by using an HMAC algorithm, to obtain the first sub-key. Alternatively, the SMF network element performs a second derivation operation on

the target MSK to obtain the second sub-key. For example, the SMF network element uses the target MSK as an input key, uses an integrity protection algorithm as an input parameter, and performs a derivation operation by using an HMAC algorithm, to obtain the second sub-key.

[00404] Manner 2: An AUSF network element generates the target key. The SMF network element sends a key request message to the AUSF network element. Correspondingly, the AUSF network element receives the key request message from the SMF network element. The key request message is for requesting the target key. After receiving the key request message, the AUSF network element sends the target key to the SMF network element. In this way, the SMF network element can obtain the target key. Herein, if the AUSF network element cannot generate the target key, the AUSF network element sends a failure message to the SMF network element. Correspondingly, the SMF network element receives the failure message from the AUSF network element. The failure message includes a failure cause value. The failure cause value includes at least one of the following: Kausf stored in the AUSF network element is unavailable, or a derivation parameter stored in the AUSF network element is unavailable.

[00405] It should be noted that when the UDM network element determines that the multicast context corresponding to the identifier of the multicast service does not exist, after the SMF network element obtains the target key, the SMF network element sends the target key and the identifier of the multicast service to the UDM network element. Correspondingly, the UDM network element receives and stores the target key and the identifier of the multicast service from the SMF network element.

[00406] S1202. The key generation network element sends the target key to the multicast user-plane processing network element.

[00407] For example, the target key is carried in a key notification message. After the multicast user-plane processing network element receives the key notification message from the key generation network element, the multicast user-plane processing network element sends a response message to the key generation network element. Correspondingly, the key generation network element receives the response message from the multicast user-plane processing network element. The response message indicates that the multicast user-plane processing network element has received the target key.

[00408] In some embodiments, the key generation network element sends time information corresponding to the target MSK to the multicast user-plane processing network element.

Correspondingly, the multicast user-plane processing network element receives the time information corresponding to the target MSK from the key generation network element. The time information corresponding to the target MSK indicates valid time of the target MSK. In other words, within the valid time of the target MSK, the multicast user-plane processing network element protects distribution of second information (information for generating a target MTK) by using the target MSK. In this way, the terminal device can obtain the second information to generate the target MTK. On the contrary, the second information is not distributed beyond the valid time of the target MSK. In this case, the terminal device cannot obtain the second information, and therefore cannot generate the target MTK. Alternatively, within valid time of the target MSK, the multicast user-plane processing network element protects distribution of the multicast service data by using the target MSK. In this way, the terminal device can obtain the multicast service data. On the contrary, the target MSK does not exist beyond the valid time of the target MSK, and the multicast service data is no longer distributed. In this case, the terminal device cannot obtain the multicast service data.

[00409] Therefore, when the key generation network element provides the target MSK for the multicast user-plane processing network element, the key generation network element can further indicate the valid time of the target MSK, to meet use requirements of the multicast user-plane processing network element in different time periods.

[00410] In some embodiments, the key generation network element can further determine a target security policy, and provide the target security policy for the multicast user-plane processing network element. For details, refer to descriptions of S503 and S504. Details are not described herein again. Alternatively, the key generation network element can further provide a security algorithm for the multicast user-plane processing network element. For details, refer to descriptions of S505 and S506. Details are not described herein again.

[00411] In some embodiments, the key generation network element can further provide the identifier of the target MSK for the multicast user-plane processing network element. This embodiment of this application provides two possible implementations. The following related descriptions of implementation 1 and implementation 2 are specifically provided.

[00412] Implementation 1: The key generation network element sends the identifier of the target MSK to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the identifier of the target MSK from the key

generation network element.

[00413] For example, the identifier of the target MSK includes two parts: an "ID of the multicast service" and a "key number part". To be specific, when the identifier of the target MSK is implemented as "ID of the multicast service + key number part", "ID of the multicast service + key number part" is transmitted from the key generation network element to the multicast user-plane processing network element. Herein, for descriptions of the "ID of the multicast service", refer to related descriptions of S5011. Details are not described herein again.

[00414] Implementation 2: First, the key generation network element sends a key number part to the multicast user-plane processing network element. Correspondingly, the multicast user-plane processing network element receives the key number part from the key generation network element. Then, the multicast user-plane processing network element determines the identifier of the target MSK based on the key number part and an ID of the multicast service.

[00415] That the identifier of the target MSK is implemented as "ID of the multicast service + key number part" is still used as an example. The key number part is transmitted from the key generation network element to the multicast user-plane processing network element. The multicast user-plane processing network element may restore the identifier of the target MSK based on the obtained "ID of the multicast service" and the obtained key number part.

[00416] In this way, when the key generation network element provides the key number part for the multicast user-plane processing network element, the multicast user-plane processing network element can also determine the identifier of the target MSK. Compared with transmitting the "identifier of the target MSK", this reduces transmission resource overheads.

[00417] In some embodiments, the key generation network element can further provide the target key for the terminal device. In other words, the terminal device obtains the target key by using a control plane message. For details, refer to related descriptions of S1203 to S1204.

[00418] S1203. The key generation network element sends the target key to an access network device. Correspondingly, the access network device receives the target key from the key generation network element.

[00419] For example, when the key generation network element is implemented as an SMF network element, the SMF network element sends the target key to an AMF network element. Correspondingly, the AMF network element receives the target key from the SMF network element. The AMF network element sends the target key to the access network device. Correspondingly,

the access network device receives the target key from the AMF network element.

[00420] For another example, when the key generation network element is implemented as an AMF network element, the AMF network element sends the target key to the access network device. Correspondingly, the access network device receives the target key from the AMF network element.

[00421] For another example, when the key generation network element is implemented as an AUSF network element, the AUSF network element sends the target key to an SMF network element. Correspondingly, the SMF network element receives the target key from the AUSF network element. The SMF network element sends the target key to the AMF network element.

Correspondingly, the AMF network element receives the target key from the SMF network element. The AMF network element sends the target key to the access network device. Correspondingly, the access network device receives the target key from the AMF network element.

[00422] S1204. The access network device sends the target key to the terminal device. Correspondingly, the terminal device receives the target key from the access network device.

[00423] In some embodiments, the key generation network element can further provide at least one of the target security policy and the security algorithm for the terminal device. For details, refer to related descriptions of S512 to S515. Details are not described herein again.

[00424] In some embodiments, the key generation network element can further provide the identifier of the target MSK for the terminal device. This embodiment of this application still provides two possible implementations, which are specifically described in the following Example 1 and Example 2:

[00425] Example 1: The key generation network element sends the identifier of the target MSK to the terminal device. Correspondingly, the terminal device receives the identifier of the target MSK from the key generation network element.

[00426] Example 2: First, the key generation network element sends a key number part to the terminal device. Correspondingly, the terminal device receives the key number part from the key generation network element. Then, the terminal device determines the identifier of the target MSK based on the key number part and the ID of the multicast service.

[00427] In this way, when the key generation network element provides the key number part for the terminal device, the terminal device can also determine the identifier of the target MSK. Compared with transmitting the "identifier of the target MSK", this reduces transmission resource

overheads.

[00428] It should be noted that, the terminal device may alternatively receive at least one of the target key, security protection status information, a security algorithm, and an identifier of the target key from the multicast user-plane processing network element. For details, refer to descriptions of "phase 1" and "phase 2" in the "first key management method".

[00429] The foregoing is mainly related descriptions of "MSK-level key negotiation". In this phase, both the terminal device and the multicast user-plane processing network element obtain the target key. Certainly, it is easy to understand that "phase 1: MSK-level key negotiation" shown in FIG. 12 may also be replaced with "phase 2: MSK-level key negotiation" shown in FIG. 5A and FIG. 5B. For a specific implementation process, refer to related descriptions of S510 to S515 in FIG. 5A and FIG. 5B. Details are not described herein.

[00430] After obtaining the target key, the multicast user-plane processing network element performs "phase 3: data transmission" in the "first key management method" when the target MTK does not need to be generated, as shown in FIG. 12. When the target MTK is generated, "phase 3: MTK-level key negotiation" and "phase 4: data transmission" in the "first key management method" are performed, which are not shown in FIG. 12.

[00431] It should be noted that, in the key management method provided in embodiments of this application, names such as "MUK, MSK, and MTK" are only used as examples to describe a key management processing procedure, and do not constitute a limitation on the technical solutions provided in embodiments of this application. A person of ordinary skill in the art may learn that, with evolution of a network architecture and emergence of a new service scenario, at least one of an MUK, an MSK, and an MTK is defined as another name. The technical solutions provided in embodiments of this application are also applicable to similar technical problems.

[00432] In addition, an "execution occasion of S503 to S506" is further described. S503 to S506 may be performed in the "MUK negotiation" phase, specifically, as shown in FIG. 5A and FIG. 5B. Alternatively, S503 to S506 may be performed in the "MSK-level key negotiation" phase (both the phase 2 shown in FIG. 5A and FIG. 5B and the phase 1 shown in FIG. 12), or S503 to S506 may be performed in the "MTK-level key negotiation" phase (the phase 3 shown in FIG. 10). That is, S503 to S506 are performed before the "data transmission" phase. If S503 to S506 are performed in the "MUK negotiation" or "MSK-level key negotiation" phase, S512 to S515 may be performed in the "MSK-level key negotiation" phase (as shown in FIG. 5A and FIG. 5B), or S512 to S515

may be performed in the "MTK-level key negotiation" phase (not shown in FIG. 10). If S503 to S506 are performed in the "MTK-level key negotiation" phase, S512 to S515 are performed in the "MTK-level key negotiation" phase (not shown in FIG. 10).

[00433] The foregoing mainly describes the solutions provided in embodiments of this application from a perspective of interaction between network elements. Correspondingly, embodiments of this application further provide a communication apparatus. The communication apparatus may be the network element in the foregoing method embodiments, or an apparatus including the foregoing network element, or a component that can be used in the network element. It may be understood that, to implement the foregoing functions, the communication apparatus includes a hardware structure and/or a software module for performing a corresponding function. A person skilled in the art should easily be aware that, in combination with units and algorithm steps of the examples described in embodiments disclosed in this specification, this application may be implemented by hardware or a combination of hardware and computer software. Whether a function is performed by hardware or hardware driven by computer software depends on particular applications and design constraints of the technical solutions. A person skilled in the art may use different methods to implement the described functions for each particular application, but it should not be considered that the implementation goes beyond the scope of this application.

[00434] FIG. 13 is a schematic diagram of a structure of a communication apparatus 1300. The communication apparatus 1300 includes a communication unit 1303 and a processing unit 1302.

[00435] For example, the communication apparatus 1300 is the terminal device in FIG. 5A and FIG. 5B, FIG. 10, or FIG. 12 in the foregoing method embodiments. In this case, the processing unit 1302 is configured to obtain a target key. The target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK. The first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The communication unit 1303 is configured to receive target data from a multicast user-plane processing network element. The target data is data on which security protection is performed. The processing unit 1302 is further configured to process the target data by using the target key. Herein, the multicast user-plane processing network element is one of the following network elements: an MBSU network element, a UPF network element, a UPGW, or an MSF network element.

[00436] In a possible design, the communication unit 1303 is further configured to receive a

security algorithm from a first network element. The security algorithm includes at least one of an encryption algorithm and an integrity protection algorithm. The processing unit 1302 is specifically configured to process the target data by using the security algorithm and the target key. Herein, the first network element is the multicast user-plane processing network element or a key generation network element. The key generation network element is an AMF network element, an SMF network element, or an AUSF network element.

[00437] In a possible design, the communication unit 1303 is further configured to receive security protection status information from the first network element. The security protection status information indicates a security protection status, and the security protection includes at least one of data encryption and integrity verification. The processing unit 1302 is specifically configured to process the target data by using the target key if the status indicated by the security protection status information is enabled. Herein, the first network element is the multicast user-plane processing network element or a key generation network element.

[00438] In a possible design, the communication unit 1303 is further configured to receive the target key from the first network element. The processing unit 1302 is specifically configured to obtain the target key through the communication unit 1303.

[00439] In a possible design, the processing unit 1302 is further configured to obtain an identifier of the target key. The processing unit 1302 is specifically configured to obtain the target key corresponding to the identifier of the target key.

[00440] In a possible design, the communication unit 1303 is further configured to receive the identifier of the target data from the first network element. The processing unit 1302 is specifically configured to obtain the identifier of the target key through the communication unit 1303. Alternatively, the communication unit 1303 is further configured to receive a key number part from the first network element. The processing unit 1302 is specifically configured to determine the identifier of the target key based on the key number part and an identifier ID of a multicast service.

[00441] In a possible design, the communication unit 1303 is further configured to receive first information from the key generation network element. The first information includes at least one of the following: an identifier of the multicast user-plane processing network element, a first parameter, or the ID of the multicast service. Herein, the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp. The processing unit 1302

is further configured to generate an MUK based on the first information and a shared key. The shared key is a key shared between the communication apparatus 1300 and a core network device. The communication unit 1303 is further configured to receive key information from the multicast user-plane processing network element. The key information is information obtained after the target key is encrypted by using the MUK. The processing unit 1302 is specifically configured to decrypt the key information by using the MUK, to obtain the target key.

[00442] In a possible design, the processing unit 1302 is specifically configured to perform a derivation operation on the target MSK to obtain a derivation key, and perform decryption or integrity verification on the target data by using the derivation key.

[00443] In a possible design, the processing unit 1302 is specifically configured to perform a derivation operation on the target MSK and second information to obtain a derivation key, where the second information includes at least one of the following: a protocol name, an identifier of a target MTK, or a second parameter. Herein, the second parameter is a parameter determined based on at least one of a second sequence number and a second timestamp.

[00444] For example, the communication apparatus 1300 is the multicast user-plane processing network element in FIG. 5A and FIG. 5B, FIG. 10, or FIG. 12 in the foregoing method embodiments. The processing unit 1302 is configured to obtain a target key. The target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK. The first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation. The processing unit 1302 is further configured to perform security protection on multicast service data by using the target key, to obtain the target data. The communication unit 1303 is configured to send target data to a terminal device.

[00445] In a possible design, the processing unit 1302 is specifically configured to generate the target key. Alternatively, the communication unit 1303 is further configured to receive the target key from a key generation network element. The processing unit 1302 is specifically configured to obtain the target key through the communication unit 1303.

[00446] In a possible design, the communication unit 1303 is further configured to send the target key to the terminal device.

[00447] In a possible design, the communication unit 1303 is further configured to receive an MUK from the key generation network element. The processing unit 1302 is further configured to

encrypt the target key by using the MUK, to obtain key information. The communication unit 1303 is further configured to send the key information to the terminal device.

[00448] In a possible design, the communication unit 1303 is further configured to send an identifier of the target MSK to the terminal device. Alternatively, the communication unit 1303 is further configured to send a key number part to the terminal device. There is a mapping relationship between the key number part and the identifier of the target MSK.

[00449] In a possible design, the processing unit 1302 is further configured to obtain a security algorithm. The security algorithm includes at least one of an encryption algorithm and an integrity protection algorithm. The processing unit 1302 is specifically configured to perform security protection on multicast service data by using the security algorithm and the target key, to obtain the target data.

[00450] In a possible design, the processing unit 1302 is further configured to determine security protection status information. The security protection status information indicates a security protection status, and the security protection includes at least one of data encryption and integrity verification. The processing unit 1302 is specifically configured to: if the status indicated by the security protection status information is enabled, perform security protection on the multicast service data by using the target key, to obtain the target data.

[00451] In a possible design, the processing unit 1302 is specifically configured to perform a derivation operation on the target MSK to obtain a derivation key, and perform security protection on the multicast service data by using the derivation key, to obtain the target data.

[00452] In a possible design, the processing unit 1302 is specifically configured to perform a derivation operation on the target MSK and second information to obtain a derivation key. The second information includes at least one of the following: a protocol name, an identifier of a target MTK, or a second parameter. Herein, the second parameter is a parameter determined based on at least one of a second sequence number and a second timestamp.

[00453] In a possible design, the processing unit 1302 is further configured to determine, based on at least one of a transport protocol type, a session type, a quality of service QoS parameter, or a network type, to generate the target MTK. The derivation key includes the target MTK.

[00454] For example, the communication apparatus 1300 is the key generation network element in FIG. 5A and FIG. 5B in the foregoing method embodiment. The processing unit 1302 is configured to obtain an MUK. The communication unit 1303 is configured to send the MUK to a

multicast user-plane processing network element.

[00455] In a possible design, the processing unit 1302 is further configured to obtain first information. The first information includes at least one of the following: an identifier of the multicast user-plane processing network element, a first parameter, or an identifier ID of a multicast service. Herein, the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp. The processing unit 1302 is specifically configured to generate the MUK based on the first information and a shared key. The shared key is a key shared between a terminal device and a core network device.

[00456] In a possible design, the communication unit 1303 is further configured to send the first information to the terminal device.

[00457] In a possible design, the processing unit 1302 is further configured to determine a target security policy. The target security policy includes at least one of a confidentiality protection policy and an integrity protection policy. The communication unit 1303 is further configured to send the target security policy to the multicast user-plane processing network element.

[00458] In a possible design, the processing unit 1302 is specifically configured to determine the target security policy based on a transmission status of a target MTK and a basic policy. The basic policy includes a multicast security policy in a multicast context or a user plane security policy in UDM subscription data.

[00459] In a possible design, the processing unit 1302 is further configured to determine a security algorithm. The security algorithm is for security protection calculation, and the security protection is indicated by the target security policy. The communication unit 1303 is further configured to send the security algorithm to the multicast user-plane processing network element.

[00460] In a possible design, the communication unit 1303 is further configured to send at least one of the target security policy and the security algorithm to the terminal device. The security algorithm is for security protection calculation, and the security protection is indicated by the target security policy.

[00461] For example, the communication apparatus 1300 is the key generation network element in FIG. 12 in the foregoing method embodiment. The processing unit 1302 is configured to obtain a target key. The target key includes at least one of a target MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation.

The communication unit 1303 is further configured to send the target key to a multicast user-plane processing network element.

[00462] In a possible design, the communication unit 1303 is further configured to send an identifier of the target key to the multicast user-plane processing network element. Alternatively, the communication unit 1303 is further configured to send a key number part to the multicast user-plane processing network element. There is a mapping relationship between the key number part and the identifier of the target key.

[00463] In a possible design, the communication unit 1303 is further configured to send at least one of the key number part, the target key, and the identifier of the target key to a terminal device.

There is a mapping relationship between the key number part and the identifier of the target key.

[00464] For example, the communication apparatus 1300 is the AUSF network element in FIG. 5A and FIG. 5B in the foregoing method embodiment. The communication unit 1303 is configured to receive first information and a SUPI of a terminal device from a key generation network element. The first information includes at least one of the following: an identifier of a multicast user-plane processing network element, a first parameter, or an identifier ID of a multicast service. Herein, the first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp. The processing unit 1302 is configured to generate an MUK based on the first information and the SUPI. The communication unit 1303 is further configured to send the MUK to the key generation network element.

[00465] In a possible design, the processing unit 1302 is specifically configured to: determine a shared key based on the SUPI, where the shared key is a key shared between the terminal device and a core network device; and generate the MUK based on the shared key and the first information.

[00466] All related content of the steps in the foregoing method embodiments may be cited in function descriptions of the corresponding functional modules. Details are not described herein again.

[00467] Optionally, the communication apparatus 1300 further includes a storage unit 1301, configured to store program code and data of the communication apparatus 1300, where the data may include but is not limited to original data, intermediate data, or the like.

[00468] The processing unit 1302 may be a processor or a controller, for example, may be a central processing unit (central processing unit, CPU), a general purpose processor, a digital signal processor (digital signal processor, DSP), an application-specific integrated circuit (application-

specific integrated circuit, ASIC), a field programmable gate array (field programmable gate array, FPGA) or another programmable logic device, a transistor logic device, a hardware component, or any combination thereof. The processor may implement or execute various example logical blocks, modules, and circuits described with reference to content disclosed in this application.

5 Alternatively, the processor may be a combination of processors implementing a computing function, for example, a combination of one or more microprocessors, or a combination of the DSP and a microprocessor.

[00469] The communication unit 1303 may be a communication interface, a transceiver, a transceiver circuit, or the like. The communication interface is a collective name. During specific
10 implementation, the communication interface may include a plurality of interfaces, for example, an interface between a first access network device and a second access network device, and/or another interface.

[00470] The storage unit 1301 may be a memory.

[00471] When the processing unit 1302 is the processor, the communication unit 1303 is the
15 communication interface, and the storage unit 1301 is the memory, a communication apparatus 1400 in this embodiment of this application may be shown in FIG. 14.

[00472] Refer to FIG. 14. The communication apparatus 1400 includes a processor 1402, a transceiver 1403, and a memory 1401.

[00473] The transceiver 1403 may be an independently disposed transmitter, and the transmitter
20 may be configured to send information to another device. Alternatively, the transceiver may be an independently disposed receiver, and is configured to receive information from another device. Alternatively, the transceiver may be a component integrating functions of sending and receiving information. A specific implementation of the transceiver is not limited in the embodiments of this application.

25 **[00474]** Optionally, the communication apparatus 1400 may further include a bus 1404. The transceiver 1403, the processor 1402, and the memory 1401 may be connected to each other through the bus 1404. The bus 1404 may be a peripheral component interconnect (peripheral component interconnect, PCI) bus, an extended industry standard architecture (extended industry standard architecture, EISA) bus, or the like. The bus 1404 may be classified into an address bus,
30 a data bus, a control bus, and the like. For ease of representation, only one thick line is used to represent the bus in FIG. 14, but this does not mean that there is only one bus or only one type of

bus.

[00475] A person of ordinary skill in the art may understand that all or some of the foregoing embodiments may be implemented by software, hardware, firmware, or any combination thereof. When software is used to implement embodiments, all or some of embodiments may be implemented in a form of a computer program product. The computer program product includes one or more computer instructions. When the computer program instructions are loaded and executed on the computer, the procedure or functions according to embodiments of this application are all or partially generated. The computer may be a general-purpose computer, a dedicated computer, a computer network, or other programmable apparatuses. The computer instructions may be stored in a computer-readable storage medium or may be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions may be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (digital subscriber line, DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium accessible by a computer, or a data storage device, such as a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a digital video disc (digital video disc, DVD)), a semiconductor medium (for example, a solid state drive (solid state drive, SSD)), or the like.

[00476] In the several embodiments provided in this application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiment is merely an example. For example, division into the units is merely logical function division and may be other division in actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented through some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in electronic or other forms.

[00477] The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be

distributed on a plurality of network device. Some or all of the units may be selected based on actual requirements to achieve the objectives of the solutions of embodiments.

[00478] In addition, function units in embodiments of this application may be integrated into one processing unit, or each of the function units may exist alone physically, or two or more units are integrated into one unit. The integrated unit may be implemented as hardware, or may be implemented as a combination of hardware and a software functional unit.

[00479] Based on the foregoing descriptions of the implementations, a person skilled in the art may clearly understand that this application may be implemented by software in addition to necessary universal hardware or by hardware only. In most circumstances, the former is a preferred implementation. Based on such an understanding, the technical solutions in this application essentially or the part contributing to the prior art may be implemented in a form of a software product. The computer software product is stored in a readable storage medium, such as a floppy disk, a hard disk or an optical disc of a computer, and includes several instructions for instructing a computer device (which may be a personal computer, a server, a network device, or the like) to perform the methods described in embodiments of this application.

[00480] The foregoing descriptions are merely specific implementations of this application, but are not intended to limit the protection scope of this application. Any variation or replacement within the technical scope disclosed in this application shall fall within the protection scope of this application. Therefore, the protection scope of this application shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A key management method, comprising:

obtaining, by a terminal device, a target key, wherein the target key comprises at least one of
5 a target multimedia broadcast/multicast service key MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation;

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

10 processing, by the terminal device, the target data by using the target key.

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

15 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:

20 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.

25 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

30 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:

5 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.

10 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

15 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:

20 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.

25 8. The method according to claim 7, wherein

the shared key is an authentication server function key K_{ausf} or a security anchor function key K_{seaf} .

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:

30 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:

5 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.

10 11. A key management method, comprising:

obtaining, by a multicast user-plane processing network element, a target key, wherein the target key comprises at least one of a target multimedia broadcast/multicast service service key MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key
15 is for integrity protection calculation;

performing, by the multicast user-plane processing network element, security protection on multicast service data by using the target key, to obtain target data; and

sending, by the multicast user-plane processing network element, the target data to a terminal device.

20 12. The method according to claim 11, wherein the obtaining, by a multicast user-plane processing network element, a target key comprises:

generating, by the multicast user-plane processing network element, the target key; or

receiving, by the multicast user-plane processing network element, the target key from a key generation network element.

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

sending, by the multicast user-plane processing network element, the target key to the terminal device.

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

30 receiving, by the multicast user-plane processing network element, a multimedia broadcast/multicast service user key MUK from the key generation network element;

encrypting, by the multicast user-plane processing network element, the target key by using

the MUK, to obtain key information; and

sending, by the multicast user-plane processing network element, the key information to the terminal device.

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

sending, by the multicast user-plane processing network element, an identifier of the target MSK to the terminal device; or

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

16. The method according to any one of claims 11 to 15, wherein the method further comprises:

obtaining, by the multicast user-plane processing network element, a security algorithm, wherein the security algorithm comprises at least one of an encryption algorithm and an integrity
15 protection algorithm; and

the performing, by the multicast user-plane processing network element, security protection on multicast service data by using the target key, to obtain target data comprises:

performing, by the multicast user-plane processing network element, security protection on the multicast service data by using the security algorithm and the target key, to obtain the target
20 data.

17. The method according to any one of claims 11 to 16, wherein the method further comprises:

determining, by the multicast user-plane processing network element, security protection status information, wherein the security protection status information indicates a security
25 protection status, and the security protection comprises at least one of data encryption and integrity verification; and

the performing, by the multicast user-plane processing network element, security protection on multicast service data by using the target key, to obtain target data comprises:

if the status indicated by the security protection status information is enabled, performing, by
30 the multicast user-plane processing network element, security protection on the multicast service data by using the target key, to obtain the target data.

18. The method according to any one of claims 11 to 17, wherein the performing, by the multicast user-plane processing network element, security protection on multicast service data by using the target key, to obtain target data comprises:

performing, by the multicast user-plane processing network element, a derivation operation
5 on the target MSK to obtain a derivation key; and

performing, by the multicast user-plane processing network element, security protection on the multicast service data by using the derivation key, to obtain the target data.

19. The method according to claim 18, wherein the performing, by the multicast user-plane processing network element, a derivation operation on the target MSK to obtain a derivation key
10 comprises:

performing, by the multicast user-plane processing network element, 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
15 parameter is a parameter determined based on at least one of a second sequence number and a second timestamp.

20. The method according to claim 19, wherein the method further comprises:

determining, by the multicast user-plane processing network element based on at least one of a transport protocol type, a session type, a quality of service QoS parameter, or a network type, to
20 generate the target MTK, wherein the derivation key comprises the target MTK.

21. A key management method, comprising:

obtaining, by a key generation network element, a multimedia broadcast/multicast service user key MUK; and

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

22. The method according to claim 21, wherein the method further comprises:

obtaining, by the key generation network element, first information, 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 identifier ID of a multicast service, and the
30 first parameter is a parameter determined based on at least one of a first sequence number and a first timestamp; and

the obtaining, by a key generation network element, an MUK comprises:

generating, by the key generation network element, the MUK based on the first information and a shared key, wherein the shared key is a key shared between a terminal device and a core network device; or

5 sending, by the key generation network element, the first information and a subscription permanent identifier SUPI of the terminal device to an authentication server function AUSF network element; and receiving, by the key generation network element, the MUK from the AUSF network element, wherein the MUK is generated based on the first information and the SUPI.

23. The method according to claim 22, wherein the method further comprises:

10 sending, by the key generation network element, the first information to the terminal device.

24. The method according to claim 22 or 23, wherein

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

25. A key management method, comprising:

15 obtaining, by a key generation network element, a target key, wherein the target key comprises at least one of a target multimedia broadcast/multicast service service key MSK, a first sub-key corresponding to the target MSK, or a second sub-key corresponding to the target MSK, the first sub-key is for confidentiality protection calculation, and the second sub-key is for integrity protection calculation; and

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

26. The method according to claim 25, 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

25 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.

27. The method according to claim 25 or 26, wherein the method further comprises:

30 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.

28. A key management method, comprising:

determining, by a key generation network element, a target security policy, wherein the target security policy comprises at least one of a confidentiality protection policy and an integrity protection policy; and

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

29. The method according to claim 28, wherein

the determining, by a key generation network element, a target security policy comprises:

10 determining, by the key generation network element, the target security policy based on a transmission status of a target multimedia broadcast/multicast service transport key MTK and a basic policy, wherein the basic policy comprises a multicast security policy in a multicast context or a user plane security policy in unified data management UDM subscription data.

30. The method according to claim 28 or 29, wherein the method further comprises:

15 determining, by the key generation network element, a security algorithm corresponding to the target security policy, wherein the security algorithm is for data security protection calculation; and

 sending, by the key generation network element, the security algorithm to the multicast user-plane processing network element.

20 31. The method according to any one of claims 28 to 30, wherein the method further comprises:

 sending, by the key generation network element, at least one of the target security policy and a security algorithm to a terminal device, wherein the security algorithm corresponds to the target security policy.

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

 33. 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.

30 34. 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.

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

36. 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.

37. 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 11 to 20.

38. A communication apparatus, comprising units configured to perform the steps according to any one of claims 21 to 24, units configured to perform the steps according to any one of claims 25 to 27, or units configured to perform the steps according to any one of claims 28 to 31.

39. 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 21 to 24, performs the key management method according to any one of claims 25 to 27, or performs the key management method according to any one of claims 28 to 31.

40. 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 21 to 24, perform the key management method according to any one of claims 25 to 27, or perform the key management method according to any one of claims 28 to 31.

41. 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 20 is performed, the key management method according to any one of claims 21 to 24 is performed, the key management method according to any one of claims 25 to 27 is performed, or the key management method according to any one of claims 28 to 31 is performed.

42. 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 20 is performed, the key management method according to any one of claims 21 to 24 is performed, the key management method according to

any one of claims 25 to 27 is performed, or the key management method according to any one of claims 28 to 31 is performed.