

ABSTRACT

Embodiments of this application provide a key management method and a communication apparatus, and relate to the field of communication technologies, to securely transmit multicast service data, and prevent an unauthorized terminal device from obtaining the multicast service data. The method includes: A 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 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.

FIGURE 5