

密钥管理方法及通信装置

5 技术领域

本申请涉及通信技术领域，尤其涉及一种密钥管理方法及通信装置。

背景技术

在长期演进(long term evolution, LTE)网络中,为了满足实时传输协议(real-time transport protocol, RTP)和单向网络文件传输(file delivery over unidirectional transport, FLUTE)协议的要求,多媒体广播多播业务(multimedia broadcast/multicast service, MBMS)采用三层架构的密钥体系来保障数据安全传输。如图 1 所示,一个终端设备对应一个多媒体广播多播业务用户密钥(multimedia broadcast/multicast service user key, MUK)。MUK 用于加密多媒体广播多播业务业务密钥(multimedia broadcast/multicast service service key, MSK),以保护 MSK 的分发。MSK 用于加密多媒体广播多播业务传输密钥(multimedia broadcast/multicast service transport key, MTK),以保护 MTK 的分发。MTK 用于加密业务数据,以保障业务数据的安全传输。业务数据和 MTK 通过多播会话(session)从网络设备传输到终端设备。

然而,为了进一步优化广播多播业务,第五代移动通信(5-generation, 5G)系统与 LTE 网络架构和流程存在差异,但 5G 系统尚未定义 MBMS 的业务数据的安全保护。因此,如何对 MBMS 的业务数据进行安全保护是亟需解决的问题。

发明内容

本申请实施例提供一种密钥管理方法及通信装置,能够简化多播业务数据安全传输的流程,防止非授权的终端设备获取到多播业务数据。

为达到上述目的,本申请实施例采用如下技术方案:

第一方面,本申请实施例提供一种密钥管理方法,该方法的执行主体可以是终端设备,也可以是应用于终端设备中的芯片。下面以执行主体是终端设备为例进行描述。该方法包括:终端设备获取目标密钥,其中,目标密钥包括以下密钥中的至少一个:目标多媒体广播多播业务业务密钥 MSK,目标 MSK 对应的第一子密钥,或目标 MSK 对应的第二子密钥,第一子密钥用于机密性保护计算,第二子密钥用于完整性保护计算。终端设备接收来自多播用户面处理网元的目标数据,其中,目标数据是经过安全保护后的数据。然后,终端设备采用目标密钥对目标数据进行处理。这里,多播用户面处理网元是以下网元中的一种:多播广播服务用户面 MBSU 网元、用户面功能 UPF 网元、用户面分组数据网络网关 UPGW、或多播服务功能 MSF 网元。安全保护包括数据加密和完整性验证中的至少一种。

如此,在终端设备接收多播用户面处理网元的目标数据之后,终端设备采用目标密钥对目标数据进行处理。这里,目标数据是多播业务数据经过安全保护后的数据,以保证数据的安全传输,简化了数据的安全传输的处理流程。获取目标密钥的终端设备才能够对目标数据进行处理,而未获取目标密钥的终端设备无法对目标数据进行处理,也就无法获取到目标数据解保护后的数据,从而防止非授权的终端设备获取到多播业务数据。

在一种可能的设计中,本申请实施例密钥管理方法还包括:终端设备接收来自第一网

元的安全算法，其中，安全算法包括加密算法和完整性保护算法中的至少一种。终端设备采用目标密钥对目标数据进行处理，包括：终端设备采用安全算法和目标密钥对目标数据进行处理。这里，第一网元为多播用户面处理网元或密钥生成网元。密钥生成网元是 SMF 网元、AMF 网元或 AUSF 网元。

5 如此，在第一网元为多播用户面处理网元的情况下，终端设备即可从用户面消息中获取安全算法，或在第一网元为密钥生成网元的情况下，终端设备通过 AMF 网元接收来自密钥生成网元的安全算法，即终端设备可从控制面消息中获取安全算法，进而采用安全算法对目标数据进行处理。

10 在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备接收来自第一网元的安全保护状态信息，其中，安全保护状态信息指示安全保护状态，安全保护包括数据加密和完整性验证中的至少一种。例如，安全保护状态信息指示安全保护状态的开启或关闭，如安全保护状态信息指示数据加密保护处于开启或关闭状态，或安全保护状态信息指示完整性验证处于开启或关闭状态。终端设备采用目标密钥对目标数据进行处理，包括：若安全保护状态信息指示的状态为开启，则终端设备采用目标密钥对目标数据进行处理。

15 这里，第一网元为多播用户面处理网元或密钥生成网元。在第一网元为多播用户面处理网元的情况下，安全保护状态信息由多播用户面处理网元提供。在第一网元为密钥生成网元的情况下，安全保护状态信息是密钥生成网元确定的目标安全策略。终端设备通过 AMF 网元接收来自密钥生成网元的目标安全策略。如此，终端设备即可基于获取到的安全保护状态信息对目标数据进行处理。

20 在一种可能的设计中，终端设备获取目标密钥，包括：终端设备接收来自第一网元的目标密钥。这里，第一网元为多播用户面处理网元或密钥生成网元。也就是说，终端设备可以通过控制面消息或用户面消息中获取目标密钥。

在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备获取目标密钥的标识。终端设备获取目标密钥，包括：终端设备获取与目标密钥的标识对应的目标密钥。

25 如此，终端设备基于目标密钥的标识索引到目标密钥，以采用“与目标密钥的标识对应的目标密钥”来对目标数据进行处理，简化了终端设备侧的处理流程。

在一种可能的设计中，终端设备获取目标密钥的标识，包括：终端设备接收来自第一网元的目标密钥的标识。或者，终端设备接收来自第一网元的密钥序号部分，终端设备根据密钥序号部分和多播服务的标识 ID，确定目标密钥的标识。

30 也就是说，终端设备能够通过两种方式获取目标密钥的标识，若接入网设备为终端设备提供目标密钥的标识，则能够简化终端设备侧“获取目标密钥的标识”的处理流程。若接入网设备为终端设备提供密钥序号部分，与传输“目标密钥的标识”相比，能够节省传输资源开销。

35 在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备接收来自密钥生成网元的第一信息，其中，第一信息包括以下至少一项：多播用户面处理网元的标识，第一参数，或多播服务的 ID。这里，第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数。终端设备根据第一信息和共享密钥，生成多媒体广播多播业务用户密钥 MUK，其中，共享密钥是终端设备与核心网设备之间共享的密钥。终端设备获取目标密钥，包括：终端设备接收来自多播用户面处理网元的密钥信息，其中，密钥信息是目标密钥经过 MUK

加密后的信息。终端设备采用 MUK 解密密钥信息，以得到目标密钥。

如此，在密钥生成网元为终端设备提供第一信息的情况下，终端设备即可自主生成 MUK。在多播用户面处理网元采用 MUK 保护目标密钥的分发的情况下，终端设备即可采用 MUK 解密密钥信息，以得到目标密钥。

- 5 在一种可能的设计中，共享密钥为认证服务器功能密钥 Kausf、安全锚点功能密钥 Kseaf、或由 Kausf 推演出来的密钥。

在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备接收来自密钥生成网元的目标密钥对应的时间信息。其中，目标 MSK 对应的时间信息指示目标 MSK 的有效时间。以目标密钥为目标 MSK 为例，在目标 MSK 的有效时间内，多播用户面处理网元采用
10 目标 MSK 保护第二信息（用于生成目标 MTK 的信息）的分发。如此，终端设备能够得到第二信息，以生成目标 MTK。反之，在目标 MSK 的有效时间外，不再分发第二信息。如此，终端设备无法获取第二信息，也就无法生成目标 MTK。或者，在目标 MSK 的有效时间内，多播用户面处理网元采用目标 MSK 保护多播业务数据的分发。如此，终端设备能够获取到多播业务数据。反之，在目标 MSK 的有效时间外，目标 MSK 不存在，不再分发多播业务数据。
15 如此，终端设备无法获取多播业务数据。

在一种可能的设计中，终端设备采用目标密钥对目标数据进行处理，包括：终端设备采用目标 MSK 或第一子密钥对密文进行解密，以得到第一明文，终端设备根据目标 MSK 和第二子密钥中的至少一项，以及 MAC，确定第一明文的完整性，其中，目标数据包括第一明文和 MAC。或者，终端设备采用目标 MSK 或第一子密钥对密文进行解密。其中，目标数据
20 包括密文。或者，终端设备根据目标 MSK 和第二子密钥中的至少一项，以及消息认证码 MAC，确定第二明文的完整性，其中，目标数据包括 MAC 和第二明文。也就是说，目标 MSK 既能够用于解密，又能够用于完整性验证处理。终端设备对目标数据进行处理类型包括两种，即解密和完整性验证处理。

在一种可能的设计中，终端设备采用目标密钥对目标数据进行处理，包括：终端设备
25 对目标 MSK 进行推演运算，以得到推演密钥。之后，终端设备采用推演密钥对目标数据进行解密或完整性验证。

这里，推演密钥是以下密钥中一种：第一子密钥、第二子密钥、目标多媒体广播多播业务传输密钥 MTK、第三子密钥或第四子密钥。在推演密钥包括第一子密钥的情况下，终端设备对目标 MSK 进行第一推演运算，以得到第一子密钥。在推演密钥包括第二子密钥的情况下，终端设备对目标 MSK 进行第二推演运算，以得到第二子密钥。在推演密钥包括目标 MTK 的情况下，终端设备对目标 MSK 进行第三推演运算，以得到目标 MTK，其中，MTK 用于解密或完整性验证。在推演密钥包括第三子密钥的情况下，终端设备对目标 MSK 进行第三推演运算，以得到目标 MTK，之后，终端设备对目标 MTK 进行第四推演运算，以得到第三子密钥。其中，第三子密钥用于机密性保护计算。在推演密钥包括第四子密钥的情况下，终端设备对目标 MSK 进行第三推演运算，以得到目标 MTK，之后，终端设备对目标 MTK
30 进行第五推演运算，以得到第四子密钥。其中，第四子密钥用于完整性保护计算。

如此，在目标数据是经过推演密钥进行安全保护的情况下，终端设备侧也能够采用目标密钥进行推演，以得到推演密钥，进而采用推演密钥对目标数据进行处理。并且，在推演密钥实现为目标 MTK、第三子密钥或第四子密钥的情况下，终端设备也能够基于目标密

钥进行推演，以得到 MTK 层的密钥，以对目标数据进行处理。与现有技术“终端设备直接接收来自网络侧的 MTK”相比，终端设备采用推演方式得到 MTK 层级的密钥，避免密钥传输泄露的风险。

在一种可能的设计中，终端设备对目标 MSK 进行推演运算，以得到推演密钥，包括：
5 终端设备对目标 MSK 和第二信息进行推演运算，以得到推演密钥。其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。这里，第二信息可以是多播用户面处理网元为终端设备提供的信息。

也就是说，终端设备在获取到目标 MSK 和第二信息的情况下，即可进行推演运算，以
10 得到推演密钥，无需网络侧为终端设备提供目标 MTK，以降低密钥传输泄露的风险。

在一种可能的设计中，第二信息是经过目标 MSK 加密后的信息。本申请实施例密钥管理方法还包括：终端设备采用目标 MSK 解密第二信息，得到解密信息。终端设备对目标 MSK 和第二信息进行推演运算，以得到推演密钥，包括：终端设备对目标 MSK 和解密信息进行第三推演运算，以得到目标 MTK。

15 这里，虽然第二信息是通过多播消息分发的，由于目标 MSK 是通过单播消息传输的，目标 MSK 保护了第二信息的分发过程，且第二信息用于目标 MTK 的推演。如此，基于第二信息推演的目标 MTK 的安全性相当于单播消息传输的安全性。

在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备接收来自第一网元的加密算法。终端设备对目标 MSK 进行第一推演运算，以得到第一子密钥，包括：终端设备采用加密算法对目标 MSK 进行第一推演运算，以得到第一子密钥。终端设备对目标 MTK 进行第四推演运算，以得到第三子密钥，包括：终端设备采用加密算法对目标 MTK 进行第四推演运算，以得到第三子密钥。这里，第一网元为多播用户面处理网元或密钥生成网元。
20

也就是说，终端设备能够从用户面消息或控制面消息中获取加密算法，且加密算法能够用于推演第一子密钥和第三子密钥。
25

在一种可能的设计中，本申请实施例密钥管理方法还包括：终端设备接收来自第一网元的完整性保护算法。终端设备对目标 MSK 进行第二推演运算，以得到第二子密钥，包括：终端设备采用完整性保护算法对目标 MSK 进行第二推演运算，以得到第二子密钥。终端设备对目标 MTK 进行第五推演运算，以得到第四子密钥，包括：终端设备采用完整性保护算法对目标 MTK 进行第五推演运算，以得到第四子密钥。这里，第一网元为多播用户面处理网元或密钥生成网元。
30

也就是说，终端设备能够从用户面消息或控制面消息中获取完整性保护算法，且完整性保护算法能够用于推演第二子密钥和第四子密钥。

第二方面，本申请实施例提供一种密钥管理方法，该方法的执行主体可以是多播用户面处理网元，也可以是应用于多播用户面处理网元中的芯片。下面以执行主体是多播用户面处理网元为例进行描述。该方法包括：多播用户面处理网元获取目标密钥，其中，目标密钥包括以下密钥中的至少一个：目标多媒体广播多播业务业务密钥 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥，第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。之后，多播用户面处理网元采用目标密钥对多播业务数
35

据进行安全保护，以得到目标数据。多播用户面处理网元向终端设备发送目标数据。

在一种可能的设计中，多播用户面处理网元获取目标密钥，包括：多播用户面处理网元生成目标密钥。或者，多播用户面处理网元接收来自密钥生成网元的目标密钥。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元向
5 终端设备发送目标密钥。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接收来自密钥生成网元的多媒体广播多播业务用户密钥 **MUK**。多播用户面处理网元采用 **MUK** 加密目标密钥，以得到密钥信息。然后，多播用户面处理网元向终端设备发送密钥信息。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接
10 收来自密钥生成网元的 **MUK** 对应的时间信息。其中，**MUK** 对应的时间信息指示 **MUK** 的有效时间。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元向终端设备发送目标 **MSK** 的标识。或者，多播用户面处理网元向终端设备发送密钥序号部分，其中，密钥序号部分与目标 **MSK** 的标识具有映射关系。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接
15 收来自密钥生成网元的目标 **MSK** 对应的时间信息。其中，目标 **MSK** 对应的时间信息指示目标 **MSK** 的有效时间。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元获取安全算法。其中，安全算法包括加密算法和完整性保护算法中的至少一种。多播用户面
20 处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据，包括：多播用户面处理网元采用安全算法和目标密钥对多播业务数据进行安全保护，以得到目标数据。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元确定安全保护状态信息。其中，安全保护状态信息指示安全保护状态，安全保护包括数据加密和完整性验证中的至少一种。多播用户面处理网元采用目标密钥对多播业务数据进行安全
25 保护，以得到目标数据，包括：若安全保护状态信息指示的状态为开启，则多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接收来自密钥生成网元的目标安全策略。其中，目标安全策略包括机密性保护策略和完整性保护策略中的至少一种。多播用户面处理网元确定安全保护状态信息，包括：多
30 播用户面处理网元根据目标安全策略确定安全保护状态信息。

在一种可能的设计中，多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据，包括：多播用户面处理网元采用目标 **MSK** 或第一子密钥对多播业务数据进行加密，以得到密文。其中，目标数据包括密文。和/或，多播用户面处理网元根据目标 **MSK** 和第二子密钥中的至少一项，以及多播业务数据，确定消息认证码 **MAC**。其中，
35 目标数据包括 **MAC**。

在一种可能的设计中，多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据，包括：多播用户面处理网元对目标 **MSK** 进行推演运算，以得到推演密钥。多播用户面处理网元采用推演密钥对多播业务数据进行安全保护，以得到目标数据。

这里，推演密钥是以下密钥中一种：第一子密钥、第二子密钥、目标多媒体广播多播

业务传输密钥 MTK、第三子密钥或第四子密钥。在推演密钥包括第一子密钥的情况下，多播用户面处理网元对目标 MSK 进行第一推演运算，以得到第一子密钥。在推演密钥包括第二子密钥的情况下，多播用户面处理网元对目标 MSK 进行第二推演运算，以得到第二子密钥。在推演密钥包括目标 MTK 的情况下，多播用户面处理网元对目标 MSK 进行第三推演运算，以得到目标 MTK，其中，MTK 用于解密或完整性验证。在推演密钥包括第三子密钥的情况下，多播用户面处理网元对目标 MSK 进行第三推演运算，以得到目标 MTK，之后，多播用户面处理网元对目标 MTK 进行第四推演运算，以得到第三子密钥。其中，第三子密钥用于机密性保护计算。在推演密钥包括第四子密钥的情况下，多播用户面处理网元对目标 MSK 进行第三推演运算，以得到目标 MTK，之后，多播用户面处理网元对目标 MTK 进行第五推演运算，以得到第四子密钥。其中，第四子密钥用于完整性保护计算。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元向终端设备发送第二信息。其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。这里，第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。第二信息用于终端设备确定目标 MTK。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元采用目标 MSK 加密第二信息。多播用户面处理网元向终端设备发送第二信息，包括：多播用户面处理网元向终端设备发送加密后的第二信息。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接收来自密钥生成网元的加密算法。多播用户面处理网元对目标 MSK 进行第一推演运算，以得到第一子密钥，包括：多播用户面处理网元采用加密算法对目标 MSK 进行第一推演运算，以得到第一子密钥。多播用户面处理网元对目标 MTK 进行第四推演运算，以得到第三子密钥，包括：多播用户面处理网元采用加密算法对目标 MTK 进行第四推演运算，以得到第三子密钥。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元接收来自密钥生成网元的完整性保护算法。多播用户面处理网元对目标 MSK 进行第二推演运算，以得到第二子密钥，包括：多播用户面处理网元采用完整性保护算法对目标 MSK 进行第二推演运算，以得到第二子密钥。多播用户面处理网元对目标 MTK 进行第五推演运算，以得到第四子密钥，包括：多播用户面处理网元采用完整性保护算法对目标 MTK 进行第五推演运算，以得到第四子密钥。

在一种可能的设计中，多播用户面处理网元对目标 MSK 进行推演运算，以得到推演密钥，包括：多播用户面处理网元对目标 MSK 和第二信息进行推演运算，以得到推演密钥。其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。这里，第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。

在一种可能的设计中，本申请实施例密钥管理方法还包括：多播用户面处理网元根据传输协议类型、会话类型、服务质量 QoS 参数或网络类型中的至少一项，确定生成目标 MTK。其中，推演密钥包括目标 MTK。

也就是说，多播用户面处理网元能够确定是否生成目标 MTK，在生成目标 MTK 的情况下，多播用户面处理网元才推演目标 MTK，采用目标 MTK 对多播业务数据进行安全保护。反之，在无需生成目标 MTK 的情况下，多播用户面处理网元采用目标密钥对多播业务数据

进行安全保护。

在一种可能的设计中，多播用户面处理网元包括以下网元中的一种：多播广播服务用户面 MBSU 网元、用户面功能 UPF 网元、或用户面分组数据网络网关 UPGW。

第三方面，本申请实施例提供一种密钥管理方法，该方法的执行主体可以是密钥生成网元，也可以是应用于密钥生成网元中的芯片。这里，密钥生成网元可以是 SMF 网元、AMF 网元或 AUSF 网元。下面以执行主体是密钥生成网元为例进行描述。该方法包括：密钥生成网元获取多媒体广播多播业务用户密钥 MUK，之后，密钥生成网元向多播用户面处理网元发送 MUK。

如此，在 5G 系统中，密钥生成网元能够获取 MUK，并向多播用户面处理网元提供 MUK，以避免运营商部署 GBA 系统，有助于简化多播业务数据的处理流程。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元获取第一信息。其中，第一信息包括以下至少一项：多播用户面处理网元的标识，第一参数，或多播服务的标识 ID。这里，第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数。密钥生成网元获取 MUK，包括：密钥生成网元根据第一信息和共享密钥，生成 MUK。其中，共享密钥是终端设备与核心网设备之间共享的密钥。

也就是说，在密钥生成网元获取第一信息的情况下，密钥生成网元能够自主生成 MUK，以使 AUSF 网元生成 MUK，SMF 即可从 AUSF 网元中获取 MUK。

需要说明的是，在密钥生成网元实现为 SMF 网元的情况下，SMF 网元获取 MUK，包括：SMF 网元向 AUSF 网元发送第一信息和终端设备的用户永久标识 SUPI，SMF 网元接收来自 AUSF 网元的 MUK。其中，MUK 是基于第一信息和 SUPI 生成的。这里，SMF 网元向 AUSF 网元发送的第一信息和 SUPI 均承载于密钥请求消息。接收来自 AUSF 网元的 MUK 承载于密钥回复消息。也就是说，在 SMF 网元获取第一信息的情况下，SMF 网元也能够为 AUSF 网元提供第一信息，以使 AUSF 网元生成 MUK，SMF 即可从 AUSF 网元中获取 MUK。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向终端设备发送第一信息，以使终端设备生成 MUK。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向多播用户面处理网元发送 MUK 对应的时间信息。其中，MUK 对应的时间信息指示 MUK 的有效时间。

在一种可能的设计中，共享密钥为认证服务器功能密钥 Kausf、安全锚点功能密钥 Kseaf 或由 Kausf 推演的密钥。

第四方面，本申请实施例提供一种密钥管理方法，该方法的执行主体可以是密钥生成网元，也可以是应用于密钥生成网元中的芯片。这里，密钥生成网元可以是 SMF 网元、AMF 网元或 AUSF 网元。下面以执行主体是密钥生成网元为例进行描述。该方法包括：密钥生成网元获取目标密钥。其中，目标密钥包括以下密钥中的至少一个：目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥，第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。密钥生成网元向多播用户面处理网元发送目标密钥。

也就是说，在密钥生成网元获取到目标密钥之后，密钥生成网元也能够为多播用户面处理网元提供目标密钥，以使多播用户面处理网元采用目标密钥对多播业务数据进行安全

保护。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向多播用户面处理网元发送目标密钥的标识。或者，密钥生成网元向多播用户面处理网元发送密钥序号部分。其中，密钥序号部分与目标密钥的标识具有映射关系。

- 5 也就是说，密钥生成网元能够通过两种方式为多播用户面处理网元提供目标密钥的标识，若密钥生成网元为多播用户面处理网元提供目标密钥的标识，则能够简化多播用户面处理网元侧“获取目标密钥的标识”的处理流程。若密钥生成网元为多播用户面处理网元提供密钥序号部分，与传输“目标密钥的标识”相比，能够节省传输资源开销。

- 10 在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向多播用户面处理网元发送目标 MSK 对应的时间信息。其中，目标 MSK 对应的时间信息指示目标 MSK 的有效时间。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向终端设备发送密钥序号部分、目标密钥和目标密钥的标识中的至少一项。其中，密钥序号部分与目标密钥的标识具有映射关系。

- 15 在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向终端设备发送目标 MSK 对应的时间信息。其中，目标 MSK 对应的时间信息指示目标 MSK 的有效时间。

- 第五方面，本申请实施例提供一种密钥管理方法，该方法的执行主体可以是密钥生成网元，也可以是应用于密钥生成网元中的芯片。这里，密钥生成网元可以是 SMF 网元、AMF 网元或 AUSF 网元。下面以执行主体是密钥生成网元为例进行描述。该方法包括：密钥生成网元确定目标安全策略。其中，目标安全策略包括机密性保护策略和完整性保护策略中的至少一种。密钥生成网元向多播用户面处理网元发送目标安全策略。

- 20 如此，在 5G 系统中，密钥生成网元能够确定目标安全策略，以使得多播用户面处理网元和终端设备确定两者之间的安全保护状态是否开启。在安全保护处于开启状态下，多播用户面处理网元才对多播业务数据执行安全保护。

- 在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元确定目标安全策略，包括：密钥生成网元根据目标多媒体广播多播业务传输密钥 MTK 的传输状况和基础策略，确定目标安全策略。其中，基础策略包括多播上下文中的多播安全策略或统一数据管理 UDM 签约数据中的用户面安全策略。例如，在目标 MTK 生成与传输的情况下，密钥生成网元将基础策略作为目标安全策略，或密钥生成网元对基础策略进行修正，以得到目标安全策略。

也就是说，在密钥生成网元获取到基础策略的情况下，密钥生成网元还能够结合目标 MTK 的传输状况来确定目标安全策略。

- 30 在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元确定安全算法。其中，安全算法用于安全保护的计算，安全保护由目标安全策略指示。密钥生成网元向多播用户面处理网元发送安全算法。

在一种可能的设计中，本申请实施例密钥管理方法还包括：密钥生成网元向终端设备发送目标安全策略和安全算法中的至少一项。其中，安全算法用于安全保护的计算，安全保护由目标安全策略指示。

第六方面，本申请实施例提供一种通信装置，该通信装置包括：用于执行上述任一方面中各个步骤的单元。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备，或者实现上述终端设备功能的芯片。所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或手段可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

第七方面，本申请实施例提供一种通信装置，包括处理器和接口电路，处理器用于通过接口电路与其它装置通信，并执行以上任一方面提供的密钥管理方法。该处理器包括一个或多个。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备，或者实现上述终端设备功能的芯片。

第八方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述任一方面所述的方法。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备，或者实现上述终端设备功能的芯片。

第九方面，本申请实施例提供了一种通信装置，包括：处理器；所述处理器用于与存储器耦合，并读取存储器中的指令之后，根据所述指令执行如上述任一方面所述的方法。该通信装置可以为上述第一方面或第一方面任一种可能的设计中的终端设备，或者实现上述终端设备功能的芯片。

第十方面，本申请实施例提供一种通信装置，该通信装置包括：用于执行上述任一方面中各个步骤的单元。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的多播用户面处理网元，或者实现上述多播用户面处理网元功能的芯片。所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或手段可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

第十一方面，本申请实施例提供一种通信装置，包括处理器和接口电路，处理器用于通过接口电路与其它装置通信，并执行以上任一方面提供的密钥管理方法。该处理器包括一个或多个。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的多播用户面处理网元，或者实现上述多播用户面处理网元功能的芯片。

第十二方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述任一方面所述的方法。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的多播用户面处理网元，或者实现上述多播用户面处理网元功能的芯片。

第十三方面，本申请实施例提供了一种通信装置，包括：处理器；所述处理器用于与存储器耦合，并读取存储器中的指令之后，根据所述指令执行如上述任一方面所述的方法。该通信装置可以为上述第二方面或第二方面任一种可能的设计中的多播用户面处理网元，或者实现上述多播用户面处理网元功能的芯片。

第十四方面，本申请实施例提供一种通信装置，该通信装置包括：用于执行上述任一方面中各个步骤的单元。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述

第四方面或第四方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述第五方面或第五方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片。所述通信装置包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或手段可以通过硬件实现，软件实现，
5 或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

第十五方面，本申请实施例提供一种通信装置，包括处理器和接口电路，处理器用于通过接口电路与其它装置通信，并执行以上任一方面提供的密钥管理方法。该处理器包括一个或多个。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述第四方面或
10 第四方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述第五方面或第五方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片。

第十六方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述任一方面所述的方法。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述第四方面或第四方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，
15 该通信装置可以为上述第五方面或第五方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片。

第十七方面，本申请实施例提供了一种通信装置，包括：处理器；所述处理器用于与存储器耦合，并读取存储器中的指令之后，根据所述指令执行如上述任一方面所述的方法。该通信装置可以为上述第三方面或第三方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，该通信装置可以为上述第四方面或第四方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片；或者，
20 该通信装置可以为上述第五方面或第五方面任一种可能的设计中的密钥生成网元，或者实现上述密钥生成网元功能的芯片。

第十八方面，本申请实施例提供一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述任一方面中任一项的密钥管理方法。
30

第十九方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述任一方面中任一项的密钥管理方法。

第二十方面，本申请实施例提供一种电路系统，电路系统包括处理电路，处理电路被配置为执行如上述任一方面中任一项的密钥管理方法。

第二十一方面，本申请实施例提供一种芯片，芯片包括处理器，处理器和存储器耦合，存储器存储有程序指令，当存储器存储的程序指令被处理器执行时实现上述任一方面任一项的密钥管理方法。
35

第二十二方面，本申请实施例提供一种通信系统，该通信系统包括终端设备和多播用户面处理网元。其中，终端设备用于获取目标密钥。其中，目标密钥包括以下密钥中的至

少一个：目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥。第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。终端设备还用于接收来自多播用户面处理网元的目标数据。其中，目标数据是经过安全保护后的数据。终端设备还用于采用目标密钥对目标数据进行处理。多播用户面处理网元用于获取目标密钥。其中，目标密钥包括以下密钥中的至少一个：目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥，第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。多播用户面处理网元还用于采用目标密钥对多播业务数据进行安全保护，以得到目标数据。多播用户面处理网元还用于向终端设备发送目标数据。

10 在一种可能的设计中，本申请实施例通信系统还包括：密钥生成网元。其中，密钥生成网元用于获取 MUK。密钥生成网元还用于向多播用户面处理网元发送 MUK。这里，密钥生成网元可以是 SMF 网元、AMF 网元或 AUSF 网元。

在一种可能的设计中，本申请实施例通信系统还包括：密钥生成网元。其中，密钥生成网元用于获取目标密钥。密钥生成网元还用于向多播用户面处理网元发送目标密钥。

15 在一种可能的设计中，本申请实施例通信系统还包括：密钥生成网元。其中，密钥生成网元确定目标安全策略。其中，目标安全策略包括机密性保护策略和完整性保护策略中的至少一种。密钥生成网元向多播用户面处理网元发送目标安全策略。多播用户面处理网元还用于根据目标安全策略确定安全保护状态信息。其中，安全保护状态信息指示安全保护状态，安全保护包括数据加密和完整性验证中的至少一种。多播用户面处理网元具体用于，若安全保护状态信息指示的状态为开启，则采用目标密钥对多播业务数据进行安全保护，以得到目标数据。

20 其中，第六方面至第二十二方面中任一种设计所带来的技术效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

附图说明

- 25 图 1 为相关技术提供的一种三层架构的密钥体系示意图；
图 2 为相关技术提供的另一种三层架构的密钥体系示意图；
图 3 为相关技术提供的一种数据传输方法的流程示意图；
图 4 (a) 为本申请实施例提供的一种通信系统架构示意图；
图 4 (b) 为本申请实施例提供的再一种通信系统架构示意图；
图 5 为本申请实施例提供的一种密钥管理方法的流程示意图；
30 图 6 (a) 为本申请实施例提供的再一种密钥管理方法的流程示意图；
图 6 (b) 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 7 (a) 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 7 (b) 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 8 为本申请实施例提供的又一种密钥管理方法的流程示意图；
35 图 9 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 10 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 11 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 12 为本申请实施例提供的又一种密钥管理方法的流程示意图；
图 13 为本申请实施例提供的一种通信装置的结构示意图；

图 14 为本申请实施例提供的再一种通信装置的结构示意图。

具体实施方式

本申请的说明书以及附图中的术语“第一”和“第二”等是用于区别不同的对象，或者用于区别对同一对象的不同处理，而不是用于描述对象的特定顺序。此外，本申请的描述中所提到的术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括其他没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。需要说明的是，本申请实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

首先，介绍本申请实施例所涉及的技术术语：

多媒体广播多播业务(multimedia broadcast/multicast service, MBMS)，是指一个数据源，通过共享的一条传输链路，向多个终端设备发送数据的点到多点业务。该业务也可称为多播广播业务(multicast broadcast service, MBS)。

在长期演进(long term evolution, LTE)网络中，用户面(user plane)的安全保护在终端设备和广播/多播服务中心(broadcast-multicast service centre, BM-SC)之间执行。其中，BM-SC能够提供广播/多播承载服务和MBMS用户服务，具备会话传输、代理转发、用户管理、安全等功能。这里，一个MBMS用户服务包括一个或多个MBMS的流会话(session)，和/或，一个MBMS用户服务包括一个或多个MBMS的下载会话。一个流会话包括一个或多个RTP会话。一个下载会话包括一个或多个FLUTE信道。每个流会话或每个下载会话承载于一个或者多个MBMS传输服务。MBMS用户服务与MBMS传输服务是相互独立的，两者之间属于多对多的关系。BM-SC使用多媒体广播多播业务业务密钥(multimedia broadcast/multicast service service key, MSK)保护不同的RTP会话和FLUTE信道。这里，RTP会话和FLUTE信道用于传输多媒体广播多播业务传输密钥(multimedia broadcast/multicast service transport key, MTK)和业务数据。其中，业务数据由MTK加密。如此，MSK用于保护MTK的分发，MTK用于保护业务数据的传输。

参见图1，图1示出了上述三层架构的密钥体系。MUK是终端设备粒度的密钥，一个终端设备对应一个MUK。终端设备和BM-SC中的MUK均是通过通用自举架构(generic bootstrapping architecture, GBA)获得的。不同的MSK密钥组来保护不同的MTK。如图1所示，MSK密钥组A、MSK密钥组B和MSK密钥组C分别保护不同的MTK。不同的MTK来保护不同的RTP会话。如图1所示，MSK密钥组A保护的MTK，用于保护RTP会话1。MSK密钥组B保护的MTK，用于保护RTP会话2。MSK密钥组C保护的MTK，用于保护RTP会话3。

参见图2，图2示出了一个RTP会话的密钥体系。对于同一个RTP会话而言，一个密钥组包括一个或多个MSK，一个密钥组中的不同MSK对应不同的使用时刻。如图2所示，一个密钥组包括n个MSK，分别记为MSK1、MSK2、...、MSKn。其中，MSK1是当前(current)时刻使用的密钥，MSK2是下一(next)时刻使用的密钥，该密钥组中的其他MSK的使用时刻以此类推。

在终端设备完成多播用户服务注册后, BM-SC 选择发送时机, 向终端设备发送多播服务对应的 MSK。传输 MSK 的过程中采用的传输协议是 MIKEY 协议。另外, 不同的 MSK 具备不同的标识。MSK 的标识包括如下部分: 移动国家码 (mobile country code, MCC) || 移动网络码 (mobile network code, MNC) 部分、密钥分组部分 (key group part) 和密钥序号部分 (key number part)。即 MSK 的标识实现为 “MCC || MNC+Key Group part +Key Number part”。其中, “MCC || MNC 部分” 是指: MNC 填充在 MCC 后, 以组成共同的字符串。“MCC || MNC 部分” 用来标识公用陆地移动网 (public land mobile network, PLMN), 密钥分组部分用来标识 BM-SC, 密钥序号部分用来标识密钥序号, 如当前时刻、下一时刻等。

- 10 BM-SC 生成 MTK。MTK 的分发由 MSK 保护。如图 2 所示, MSK1 保护 MTK₁₁、MTK₁₂、...、MTK_{1x} 等的分发。MSK2 保护 MTK₂₁、MTK₂₂、...、MTK_{2y} 等的分发。MSKn 保护 MTK_{n1}、MTK_{n2}、...、MTK_{nk} 等的分发。

- 15 在业务数据的传输过程中, BM-SC 向终端设备发送业务数据和 MTK 密钥标识。相应的, 终端设备接收来自 BM-SC 的业务数据和 MTK 密钥标识。其中, 业务数据是经过 MTK 密钥标识对应 MTK 加密后的数据。终端设备根据 MTK 密钥标识查找对应的 MTK, 采用查找到的 MTK 对业务数据进行解密安全保护。这里, MTK 的标识包括如下部分: 密钥分组部分 (key group part)、密钥序号部分 (key number part) 和 MTK 标识 (identity, ID)。

在第五代移动通信 (5-generation, 5G) 系统中, 多播业务的数据传输过程如图 3 所示, 具体步骤如下:

- 20 步骤 1、终端设备完成在网络的注册, 终端设备与应用功能 (application function, AF) 网元建立协议数据单元 (protocol data unit, PDU) 会话。

步骤 2、AF 网元通过应用层向终端设备发送多播通告 (multicast announcement) 消息。相应的, 终端设备接收来自 AF 网元的多播通告消息。

- 25 其中, 多播通告消息用于告知终端设备开始提供多播服务。多播通告消息还包括多播服务的互联网协议 (internet protocol, IP) 地址。

步骤 3、终端设备通过用户面方式加入多播服务。

其中, 用户面功能 (user plane function, UPF) 网元作为多播路由器。这里, UPF 网元向会话管理功能 (session management function, SMF) 网元发送消息, 以告知 SMF 网元多播服务的 IP 地址。

- 30 步骤 4、终端设备通过信令面方式加入多播服务。

这里, 终端设备向接入和移动性管理功能 (access and mobility management function, AMF) 网元发送 PDU 会话修改请求。相应的, AMF 网元接收来自终端设备的 PDU 会话修改请求。

- 35 AMF 网元向 SMF 网元发送 PDU 会话更新上下文消息 (PDU session update SMcontext)。相应的, SMF 网元接收来自 AMF 网元的 PDU 会话更新上下文消息。

其中, PDU 会话修改请求和 PDU 会话更新上下文消息中均写到多播服务的 IP 地址。如此, SMF 网元即可获取多播服务的 IP 地址。

需要说明的是, 在实际应用过程中, 终端设备可以选择步骤 3 和步骤 4 对应的一种方式加入多播服务。

步骤 5、SMF 网元获取多播服务的 IP 地址对应的多播上下文。

示例性的，SMF 网元向统一数据管理 (unified data management, UDM) 网元发送第一请求消息。相应的，UDM 网元接收来自 SMF 网元的第一请求消息。其中，第一请求消息包括多播服务的 IP 地址，以请求多播服务的 IP 地址对应的多播上下文。若 UDM 网元能够
5 提供多播服务的 IP 地址对应的多播上下文，则 UDM 网元向 SMF 网元发送多播服务的 IP 地址对应的多播上下文。相应的，SMF 网元接收来自 UDM 网元的多播服务的 IP 地址对应的多播上下文。其中，多播上下文包括多播安全策略。反之，若 UDM 网元无法提供多播服务的 IP 地址对应的多播上下文，则 UDM 网元向 SMF 网元发送失败消息。SMF 网元向 UDM 网元发送第二请求消息，以请求签约数据。SMF 网元接收来自 UDM 网元的签约数据。其中，签约
10 数据包括允许的 PDU 会话类型、允许的业务和会话连续性 (service and session continuity, SSC) 模式 (mode)、SMF 关联外部参数、用户面安全策略等。SMF 网元根据签约数据创建多播服务的 IP 地址对应的多播上下文。

步骤 6、SMF 网元向 AMF 网元发送业务配置信息。相应的，AMF 网元接收来自 SMF 网元的业务配置信息。
15 其中，业务配置信息包括上述多播上下文，专用服务质量 (quality of service, QoS) 规则等。

步骤 7、AMF 网元向接入网设备发送 N2 会话修改请求。相应的，接入网设备接收来自 AMF 网元的 N2 会话修改请求。

其中，N2 会话修改请求包括业务配置信息。
20 步骤 8、接入网设备向终端设备发送无线资源控制 (radio resource control, RRC) 重配置消息。相应的，终端设备接收来自接入网设备的 RRC 重配置消息。

示例性的，接入网设备在根据公共信息确定该业务是用于传输多播数据 (如该业务属于多个终端设备共同接收的业务) 的情况下，接入网设备将该业务关联到 UPF 网元到接入网设备之间的公共数据通道。其中，公共数据通道可以是已经建立的通道，也可以是在上述
25 情况下触发建立的通道。此种情况下，接入网设备向终端设备发送 RRC 重配置消息，以告知终端设备接收多播数据的通道为上述公共数据通道。其中，业务配置信息包括公共信息。

在终端设备获取 RRC 重配置消息之后，终端设备向接入网设备发送 RRC 重配置确认。相应的，接入网设备接收来自终端设备的 RRC 重配置确认。

30 步骤 9、接入网设备向 AMF 网元发送会话回复消息。相应的，AMF 网元接收来自接入网设备的会话回复消息。

其中，会话回复消息包括接入网设备的 IP 地址和通用分组无线服务隧道协议用户面 (general packet radio service tunneling protocol-user plane, GTP-U) 的隧道端点标识 (tunnel endpoint identifier, TEID)。

35 步骤 10、AMF 网元向 SMF 网元发送会话更新消息。相应的，SMF 网元接收来自 AMF 网元的会话更新消息。

其中，会话更新消息包括接入网设备的 IP 地址和 GTP-U TEID。

步骤 11、SMF 网元向 UPF 网元发送会话修改消息。相应的，UPF 网元接收来自 SMF 网元的会话修改消息。

其中，会话修改消息包括接入网设备的 IP 地址和 GTP-U TEID。

UPF 网元根据接入网设备的 IP 地址和 GTP-U TEID，建立 UPF 与接入网设备之间的承载，以传输多播数据。

步骤 12、AF 网元向多播/广播服务用户面(multicast/broadcast service user plane, MBSU)网元发送多播数据。相应的，MBSU 网元接收来自 AF 网元的多播数据。

其中，MBSU 网元也可以替换为用户面分组数据网络网关 (user packet data network gateway, UPGW)。MBSU 网元和 UPGW 均可以是独立的网元，也可以是 UPF 网元中的一部分 (即 MBSU 网元和 UPGW 均可与 UPF 网元合设)。

步骤 13、MBSU 网元向 UPF 网元发送多播数据。相应的，UPF 网元接收来自 MBSU 网元的多播数据。

步骤 14、UPF 网元向接入网设备发送多播数据。相应的，接入网设备接收来自 UPF 网元的多播数据。

步骤 15、接入网设备向终端设备发送多播数据。相应的，终端设备接收来自接入网设备的多播数据。

综上可知，在 LTE 网络中，为了满足 RTP/FLUTE 协议的安全要求，采用三层密钥架构体系。与 LTE 的网络架构相比，5G 系统的网络架构存在差异，且 5G 系统尚未定义 MBS 的业务数据的安全保护处理流程。若 5G 系统不采用 RTP 协议和 FLUTE 协议，继续使用上述三层架构的密钥体系，则 5G 系统的信令流程和传输负载存在额外的冗余。与此同时，在 LTE 网络中，MUK 是由终端设备和网络设备通过 GBA 系统协商生成。如此，运营商部署多媒体广播多播业务系统之外，还要额外部署 GBA 系统。因此，在 5G 广播多播业务中，如何简化多播业务数据安全传输的流程，防止非授权用户获得多播业务数据，是需要解决的问题。

有鉴于此，本申请实施例提供了密钥管理方法，首先对本申请实施例密钥管理方法所适用的通信系统进行说明，该通信系统可以是支持 5G 移动通信技术的通信系统，例如新无线 (new radio, NR) 接入技术；或者，该通信系统还可以是支持多种无线技术的通信系统，例如支持 LTE 技术和 NR 接入技术的通信系统。另外，该通信系统也可以适用于面向未来的通信技术。

参见图 4 (a)，以支持 5G 移动通信技术的通信系统为例，对该通信系统的网络架构进行介绍。该 5G 网络架构中的网元包括终端设备、接入网设备、UPF 网元、多播/广播服务用户面(multicast/broadcast service user plane, MBSU)网元、多播服务功能(multicast service function, MSF)网元、应用功能(application function, AF)网元、AMF 网元、SMF 网元、网络暴露功能(network exposure function, NEF)网元、多播/广播服务功能(multicast/broadcast service function, MBSF)网元、策略控制功能(policy control function, PCF)网元等。

其中，终端设备，又称为用户设备 (user equipment, UE)、移动台 (mobile station, MS)、移动终端 (mobile terminal, MT) 等，是一种向用户提供语音/数据连通性的设备，例如，具有无线连接功能的手持式设备或车载设备等。终端设备具体可以为：手机 (mobile phone)、平板电脑、笔记本电脑、掌上电脑、移动互联网设备 (mobile internet device, MID)、可穿戴设备、虚拟现实 (virtual reality, VR) 设备、增强现实 (augmented reality,

AR) 设备、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程手术(remote medical surgery)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、或智慧家庭(smart home)中的无线终端,未来 5G 通信网络或 5G 之后的通信网络中的终端设备等,本申请实施例对此不作限定。

接入网设备可以为无线接入网络(radio access network, RAN),其是一种部署在无线接入网用以提供无线通信功能的装置。可选的,本申请实施例所涉及的 RAN 设备包括例如但不限于如下各种形式的宏基站,微基站(也称为小站),中继站,发送接收点(transmission reception point, TRP),下一代网络节点(g Node B, gNB)、连接下一代核心网的演进型节点 B(ng evolved Node B, ng-eNB)等,还可以包括无线局域网(wireless local area network, WLAN)接入设备等非第三代合作伙伴计划(3rd generation partnership project, 3GPP)系统的 RAN 设备。

UPF 网元是用户面的功能网元,主要负责终端设备中用户数据的转发和接收。UPF 网元可以从数据网络(data network, DN)接收用户数据,通过接入网设备传输给终端设备;UPF 网元还可以通过接入网设备从终端设备接收用户数据,转发到数据网络。UPF 网元具备为终端设备提供服务的传输资源和调度功能,且由 SMF 网元管理控制。支持多播广播会话的 UPF 网元也可称为 MB-UPF 网元。

MBSU 网元主要处理用户面数据,以满足服务层功能和管理要求。这里,MBSU 网元可以是逻辑功能上的网元,与其他网元合设。

MSF 网元主要提供服务层功能。例如,MSF 网元提供信令面功能和用户面功能,具体包括多播服务配置、多播服务管理、数据编码、数据传输等。提供用户面功能的 MSF 网元也可以记为“MSF-U”网元,提供信令面功能的 MSF 网元也可以记为“MSF-C”网元。这里,MSF 网元可以是逻辑功能上的网元,与其他网元合设。

AF 网元可以与 3GPP 核心网络进行交互。AF 网元具体可以为应用服务器,可用于与 PCF 网元交互,为应用定制策略。

AMF 网元具有终端设备的移动性管理、注册管理、连接管理、合法监听、支持传输终端设备和 SMF 网元之间的会话管理(session management, SM)信息、接入认证和接入授权等功能。

SMF 网元具有会话管理、漫游等功能。其中,会话管理功能,例如,会话建立、修改和释放。漫游功能可以包括计费数据收集、支持与外部(external)数据网络进行认证/授权的信令传输。支持多播广播会话的 SMF 网元也可称为 MB-SMF 网元。

NEF 网元能够提供的网络功能包括对外提供网元的服务、能力以及应用功能和边缘计算。可选的,NEF 网元还提供了一种向 3GPP 核心网络提供信息的应用功能,例如,移动模式和通信模式。在这种情况下,NEF 网元还可以提供认证、授权和限制上述应用功能的网络功能。

MBSF 网元可以是 NEF 网元的一部分,也可以是独立网元。MBSF 网元用来处理多播/广播的服务管理、提供核心网到应用服务器的接口、授权终端设备加入多播/广播会话。

PCF 网元包含用户签约信息管理功能、策略控制功能、计费策略控制功能、服务质量(quality of service, QoS)控制等。

其中，终端设备通过 Uu 接口与接入网设备通信，接入网设备通过 N2 接口与 AMF 网元通信，接入网设备通过 N3 接口与 UPF 网元通信，UPF 网元通过 N4 接口与 SMF 网元通信，UPF 网元通过 N6 接口接入 AF 网元和 MBSU 网元，MBSU 网元通过 NxMB-U 接口与 AF 网元通信，MBSU 网元通过 Ny 接口与 NEF 网元通信。AMF 网元通过 N11 接口与 SMF 网元通信。SMF 网元通过 N7 接口与 PCF 网元通信。PCF 网元通过 N30 接口与 NEF 网元通信。NEF 网元通过 N33 接口与 AF 网元通信。

参见图 4 (b)，仍以支持 5G 移动通信技术的通信系统为例，本申请实施例提供另一种网络架构。该 5G 网络架构中的网元包括终端设备、接入网设备、UPF 网元、MSF-U 网元、AF 网元、AMF 网元、SMF 网元、MSF-C 网元、NEF 网元等。这里，各个网元的介绍可以参见图 4 (a) 中的相关说明，此处不再赘述。MSF-U 网元和 MSF-C 网元均可以是逻辑功能上的网元，与其他网元合设。

本申请实施例描述的通信系统以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限制。本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

下面对本申请实施例提供的密钥管理方法进行具体阐述。

需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字。在本申请实施例中，目标密钥包括以下密钥中的至少一个：目标 MSK，第一子密钥，或第二子密钥。其中，第一子密钥和第二子密钥均与目标 MSK 对应，第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。第一子密钥可以记为 MSK_enc，第二子密钥可以记为 MSK_int。第三子密钥和第四子密钥均与目标 MTK 对应，第三子密钥用于机密性保护计算，第四子密钥用于完整性保护计算。第三子密钥可以记为 MTK_enc，第四子密钥可以记为 MTK_int，在此统一说明，以下不再赘述。

本申请实施例提供第一种密钥管理方法，该密钥管理方法应用在 MBS 通信过程中。终端设备完成注册和 PDU 会话建立的过程，且加入多播服务，详见图 3 中的步骤 1 至步骤 5 的相关说明，此处不再赘述。在终端设备加入多播服务之后，执行图 5 所示的密钥管理方法的，具体步骤如下：

第一阶段、MUK 的协商。在此阶段，终端设备和多播用户面网元均获取到 MUK。MUK 的获取过程可以通过 5G GBA 协议或者应用认证和密钥管理协议 (authentication and key management for applications, AKMA) 来实现，在此不再赘述。MUK 的获取过程也可以使用本申请实施例中描述的 MUK 的协商方式，具体实现过程参见 S501 至 S509 的相关说明：S501、密钥生成网元获取 MUK。

其中，密钥生成网元为 SMF 网元、AMF 网元或 AUSF 网元。

示例性的，密钥生成网元在一定的触发条件下才发起“获取 MUK”的处理过程。这里，密钥生成网元根据多播服务认证或者授权结果确定是否发起“获取 MUK”的处理过程。可以理解的是，在密钥生成网元的多播服务认证通过或者已授权的情况下，密钥生成网元发起“获取 MUK”的处理流程。反之，在密钥生成网元的多播服务认证失败或者未授权的情况下，密钥生成网元不发起“获取 MUK”的处理过程。其中，多播服务认证可以是二次认

证,也可以是特定认证流程,本申请实施例对此不作限定。这里,“二次认证”是指,在终端设备和核心网设备之间的主认证通过后,终端设备与 AF 网元之间进行的认证过程,该认证过程使用可扩展身份认证协议(extensible authentication portocol, EAP)认证框架。其中,密钥生成网元(如 SMF 网元)可以作为 EAP 认证节点(authenticator),终端设备作为 EAP 客户端,AF 网元作为 EAP 服务器。“特定认证流程”是指,专门针对多播业务的认证流程,如终端设备与 AF 网元之间进行的认证过程,该认证过程使用 EAP 认证框架或者其他认证协议。

密钥生成网元接收来自 AF 网元或多播用户面处理网元的认证结果,之后,密钥生成网元根据该认证结果确定多播服务认证是否通过。这里,“授权”是指授予终端设备访问多播的权利。密钥生成网元从 UDM 网元获取终端设备的签约数据。其中,终端设备的签约数据包括指示信息,该指示信息指示终端设备是否允许获取多播服务。密钥生成网元根据终端设备的签约数据来确定是否授权。

示例性的, MUK 用于保护 MSK 的分发。MUK 的获取方式有多种,可以例如但不限于如下两种情况:

情况一、在密钥生成网元为 SMF 网元、AMF 网元或 AUSF 网元的情况下,密钥生成网元生成 MUK,具体实现过程如图 6(a)所示:

S5010、密钥生成网元获取第一信息。

其中,第一信息包括以下信息中的至少一项:

第一项、多播用户面处理网元的标识。这里,多播用户面处理网元的标识可以是密钥生成网元上预配置的信息,也可以是密钥生成网元向多播用户面处理网元请求后获取的信息。多播用户面处理网元可以是以下网元中的一种:MBSU 网元、UPF 网元、MSF 网元或 UPGW。在多播用户面处理网元实现为 MBSU 网元的情况下,多播用户面处理网元的标识为 MBSU 网元的标识。多播业务的安全保护在终端设备和 MBSU 网元之间实现。在多播用户面处理网元实现为 UPF 网元的情况下,多播用户面处理网元的标识为 UPF 网元的标识。多播业务的安全保护在终端设备和 UPF 网元之间实现。在多播用户面处理网元实现为 UPGW 的情况下,多播用户面处理网元的标识为 UPGW 的标识。多播业务的安全保护在终端设备和 UPGW 之间实现。UPGW 可以是独立的网元,也可以和“UPF 网元、MBSU 网元、MSF 网元”三者中的一种网元合设。在多播用户面处理网元实现为 MSF 网元的情况下,多播用户面处理网元的标识为 MSF 网元的标识。多播业务的安全保护在终端设备和 MSF 网元之间实现。

第二项、第一参数。这里,第一参数可以是基于第一随机数、第一计数值、或第一时间戳中的至少一项确定的参数。例如,第一参数为上述第一随机数、第一计数值或第一时间戳等。第一参数由密钥生成网元生成和维护。

第三项、多播服务的 ID。这里,多播服务的 ID 可以实现为多播服务的 IP 地址,也可以为多播服务的组标识。在密钥生成网元实现为 SMF 网元的情况下“SMF 网元获取多播服务的 IP 地址”的具体实现过程可以参见图 3 中步骤 1 至步骤 4 的相关说明,此处不再赘述。

S5011、密钥生成网元根据第一信息和共享密钥,生成 MUK。

示例性的,在密钥生成网元推演 MUK 的过程中,计算 MUK 的输入密钥是共享密钥,计算 MUK 的输入参数是第一信息,计算 MUK 的推演算法可以是散列消息鉴别码(hash message

authentication code, HMAC) 算法。

其中, 共享密钥是终端设备与核心网设备之间共享的密钥。这里, 共享密钥为认证服务器功能密钥 Kausf、安全锚点功能密钥 Kseaf 或由 Kausf 推演出来的密钥。

其中, 第一信息中各项信息在 MUK 生成过程中的具体作用如下:

5 多播用户面处理网元的标识是为了隔离不同网元(如 MBSU 网元、UPF 网元、UPGW)之间的安全保护。例如, 在一个 PLMN 中存在多个多播用户面处理网元时, 多播用户面处理网元的标识对应唯一的多播用户面处理网元。在一个 PLMN 中存在唯一的多播用户面处理网元(如 MBSU 网元、UPF 网元、UPGW、MSF 网元)时, 多播用户面处理网元的标识可以置为固定值, 或不作为“计算 MUK 的输入参数”。

10 第一参数是为了隔离不同时序的 MUK。也就是说, 终端设备在时刻 1 被允许接入多播业务, 终端设备和核心网设备均能够基于时刻 1 对应的第一参数推演, 以得到时刻 1 对应的 MUK。时刻 1 对应的 MUK 保护目标 MSK 的分发。如此, 在终端设备具备时刻 1 对应的 MUK 的情况下, 终端设备能够得到目标 MSK。终端设备在时刻 2 未被允许接入多播业务, 终端设备无法基于时刻 2 对应的第一参数推演, 也就无法得到时刻 2 对应的 MUK。由于更新的目标 MSK 的分发是经过时刻 2 对应的 MUK 保护的。如此, 在终端设备不具备时刻 2 对应的 MUK 的情况下, 终端设备无法得到更新的目标 MSK。

多播服务的标识是为了隔离不同多播业务中 MUK。

如此, 密钥生成网元能够基于多播用户面处理网元的标识、第一参数和多播服务的 ID 中的至少一项, 以及共享密钥, 来生成 MUK, 进而向多播用户面处理网元分发 MUK。

20 情况二、在密钥生成网元为 SMF 网元的情况下, SMF 网元从 AUSF 网元获取 MUK, 具体实现过程如图 6(b) 所示:

S5012、SMF 网元获取第一信息。

其中, 关于第一信息的介绍可以参见 S5010 的具体说明, 此处不再赘述。

25 S5013、SMF 网元向 AUSF 网元发送第一信息和用户永久标识(subscription permanent identifier, SUPI)。相应的, AUSF 网元接收来自 SMF 网元的第一信息和 SUPI。

其中, SUPI 能够在 5G 系统中标识终端设备的真实身份。这里, “SMF 网元获取 SUPI” 的具体实现过程可以参见现有技术, 此处不再赘述。

示例性的, 第一信息和 SUPI 可以均承载于密钥请求消息。

S5014、AUSF 网元根据第一信息和 SUPI, 生成 MUK。

30 示例性的, AUSF 网元利用 SUPI 索引到终端设备对应的共享密钥。这里, 共享密钥的介绍可以参见 S5012 的相关说明, 此处不再赘述。AUSF 网元根据第一信息和共享密钥生成 MUK, 其具体实现过程可以参见 S5012 的相关说明, 此处不再赘述。

S5015、AUSF 网元向 SMF 网元发送 MUK。相应的, SMF 网元接收来自 AUSF 网元的 MUK。

示例性的, MUK 承载于密钥回复消息。

35 也就是说, 在密钥生成网元实现为 SMF 网元的情况下, SMF 网元能够向 AUSF 网元提供多播用户面处理网元的标识、第一参数和多播服务的 ID 中的至少一项, 以使 AUSF 网元生成 MUK。如此, SMF 网元即可从 AUSF 网元获取 MUK, 进而向多播用户面处理网元分发 MUK。

需要说明的是, 若 AUSF 网元无法生成 MUK, 则 AUSF 网元向 SMF 网元发送失败消息。相应的, SMF 网元接收来自 AUSF 网元的失败消息。其中, 失败消息包括失败原因值。失败

原因值指示 AUSF 无法生成 MUK 的原因，如 AUSF 网元中存储的推演参数不可用等。

S502、密钥生成网元向多播用户面处理网元发送 MUK。相应的，多播用户面处理网元接收来自密钥生成网元的 MUK。

示例性的，MUK 承载于密钥通知 (notification) 消息。在多播用户面处理网元接收来自密钥生成网元的密钥通知消息之后，多播用户面处理网元向密钥生成网元发送响应消息。相应的，密钥生成网元接收来自多播用户面处理网元的响应消息。其中，响应消息指示多播用户面处理网元已接收 MUK。

在一些实施例中，密钥生成网元向多播用户面处理网元发送 MUK 对应的时间信息。相应的，多播用户面处理网元接收来自密钥生成网元的 MUK 对应的时间信息。其中，MUK 对应的时间信息指示 MUK 的有效时间。也就是说，在 MUK 的有效时间内，多播用户面处理网元采用 MUK 保护目标 MSK 的分发。如此，终端设备能够得到目标 MSK。反之，在 MUK 的有效时间外，MUK 失效，多播用户面处理网元不再分发目标 MSK。如此，终端设备无法获取目标 MSK。

如此，在密钥生成网元为多播用户面处理网元提供 MUK 的情况下，密钥生成网元还能够指示 MUK 的有效时间，以满足多播用户面处理网元在不同时间段的使用需求。

在一些实施例中，密钥生成网元还能够确定目标安全策略，并提供给多播用户面处理网元，具体实现过程如图 5 中的 S503 和 S504 所示：

S503、密钥生成网元确定目标安全策略。

其中，目标安全策略包括机密性保护策略和完整性保护策略中的至少一种。这里，机密性保护策略指示终端设备与多播用户面处理网元之间的数据是否进行加密保护。完整性保护策略指示终端设备与多播用户面处理网元之间的数据是否进行完整性保护。

示例性的，目标安全策略的类型有两种。其中，第一种类型的目标安全策略包括“需要”和“不需要”两种可能的情况。这里，“需要”是指终端设备与多播用户面处理网元之间的安全保护需要执行。“不需要”是指终端设备与多播用户面处理网元之间的安全保护不需要执行。第二种类型的目标安全策略包括“需要”、“不需要”和“偏好 (preferred)”等三种可能的情况。这里，“需要”和“不需要”的含义同“第一种类型的目标安全策略”，此处不再赘述。“偏好”是指终端设备与多播用户面处理网元之间的安全保护可以执行，也可以不执行。

示例性的，S503 的具体实现过程可以例如但不限于如下示例一和示例二：

示例一、密钥生成网元根据目标 MTK 的传输状况和基础策略确定目标安全策略。

其中，目标 MTK 的传输状况包括两种：多播用户面处理网元向终端设备发送目标 MTK (或用于生成目标 MTK 的第二信息，详见 S1002 的描述)，多播用户面处理网元无需向终端设备发送目标 MTK (或用于生成目标 MTK 的第二信息)。

其中，基础策略包括多播上下文中的多播安全策略或 UDM 签约数据中的用户面安全策略。这里，密钥生成网元 (如 SMF 网元) 获取“多播上下文中的多播安全策略”的具体实现过程可以参见图 3 中步骤 5 的相关说明，此处不再赘述。密钥生成网元 (如 SMF 网元) 获取“UDM 签约数据中的用户面安全策略”的具体实现过程可以参见图 3 中步骤 5 的相关说明，此处不再赘述。

这里，在示例一中，S503 可以具体实现为如下步骤 1 和步骤 2：

步骤 1、密钥生成网元根据目标 MTK 的传输状况，确定目标安全策略的类型。

在无需生成和传输目标 MTK 的情况下，密钥生成网元确定目标安全策略的类型为第一种类型，即目标安全策略包括“需要”和“不需要”两种可能的情况。反之，在生成和传输目标 MTK 的情况下，密钥生成网元确定目标安全策略的类型为第二种类型，即目标安全策略包括“需要”、“不需要”和“偏好”等三种可能的情况。

步骤 2、密钥生成网元根据目标安全策略的类型和基础策略，确定目标安全策略。

在密钥生成网元确定目标安全策略的类型为第一种类型的情况下，若基础策略指示终端设备与多播用户面处理网元之间的安全保护需要执行，则目标安全策略与基础策略一致，终端设备与多播用户面处理网元之间的安全保护开启。若基础策略指示终端设备与多播用户面处理网元之间的安全保护不需要执行，则目标安全策略与基础策略一致，终端设备与多播用户面处理网元之间的安全保护关闭。若基础策略指示为“偏好”，即终端设备与多播用户面处理网元之间的安全保护可以执行，也可以不执行，则密钥生成网元根据本地配置确定目标安全策略，即确定“终端设备与多播用户面处理网元之间的安全保护是否需要”。例如，QoS 规则要求时延小于一定阈值时，密钥生成网元确定目标安全策略为“不需要”，即终端设备和多播用户面处理网元之间的安全保护无需执行。如前所述，在“终端设备与多播用户面处理网元之间的安全保护需要执行”的情况下，终端设备与多播用户面处理网元之间的安全保护开启。在“终端设备与多播用户面处理网元之间的安全保护不需要执行”的情况下，终端设备与多播用户面处理网元之间的安全保护关闭。如此，终端设备和多播用户面处理网元之间无需传输指示“安全保护状态”的信令，即终端设备和多播用户面处理网元之间无需协商多播安全激活状态，从而节省了信令开销。

示例性的，在密钥生成网元确定目标安全策略的类型为第二种类型的情况下，密钥生成网元可以确定目标安全策略与基础策略一致。也就是说，若基础策略指示终端设备与多播用户面处理网元之间的安全保护需要执行，则终端设备与多播用户面处理网元之间的安全保护开启。若基础策略指示终端设备与多播用户面处理网元之间的安全保护不需要执行，则终端设备与多播用户面处理网元之间的安全保护关闭。若基础策略指示为“偏好”，即终端设备与多播用户面处理网元之间的安全保护可以执行，也可以不执行，则目标安全策略指示仍为“偏好”。此种情况下，由多播用户面处理网元确定“安全保护是否执行”，再由多播用户面处理网元通知终端设备“安全保护是否执行”，具体参见 S5121 的相关说明，此处不再赘述。

如此，密钥生成网元能够结合基础策略和目标 MTK 的传输状况来确定目标安全策略，从而提供给多播用户面处理网元。

示例二、在密钥生成网元作为决定安全保护状态的网元的情况下，多播用户面处理网元无需确定“安全保护是否执行”，多播用户面处理网元不再通知终端设备“安全保护是否执行”。这里，安全保护的类型包括两种：数据加密和完整性保护。“安全保护状态”是指终端设备与多播用户面处理网元之间的安全保护开启或关闭，如数据加密保护开启或关闭，或完整性保护开启或关闭。此种情况下，密钥生成网元确定目标安全策略的类型为第一种类型，即目标安全策略包括“需要”和“不需要”两种可能的情况。密钥生成网元再根据目标安全策略的类型和基础策略，确定目标安全策略，详见上述“示例一中步骤 2”

的相关描述，此处不再赘述。

需要说明的是，确定目标安全策略的网元和密钥生成网元可以是同一个，如 S503 描述的具体实现过程。当然，确定目标安全策略的网元和密钥生成网元也可以是不同的网元，但具体过程与 S503 和 S504 描述一致，仅执行处理过程的网元不同。

- 5 S504、密钥生成网元向多播用户面处理网元发送目标安全策略。相应的，多播用户面处理网元接收来自密钥生成网元的目标安全策略。

示例性的，在目标安全策略实现为机密性保护策略的情况下，密钥生成网元为多播用户面处理网元指示数据加密保护是否执行，或密钥生成网元指示由多播用户面处理网元确定数据加密保护是否执行。在目标安全策略实现为完整性保护策略的情况下，密钥生成网元为多播用户面处理网元指示数据完整性保护是否执行，或密钥生成网元指示由多播用户面处理网元确定数据完整性保护是否执行。

如此，密钥生成网元也就能够为多播用户面处理网元提供目标安全策略，以使多播用户面处理网元基于目标安全策略对多播业务数据进行安全保护。

- 15 在一些实施例，密钥生成网元还能够向多播用户面处理网元发送安全算法，具体实现过程如图 5 中的 S505 和 S506 所示：

S505、密钥生成网元确定安全算法。

其中，安全算法用于数据安全保护计算。

示例性的，安全算法包括加密算法和完整性保护算法。安全算法可以和目标安全策略耦合。例如，在目标安全策略实现为机密性保护策略的情况下，安全算法为加密算法。在目标安全策略实现为完整性保护策略的情况下，安全算法为完整性保护算法。当然，安全算法也可以和目标安全策略解耦。例如，在密钥生成网元预先为多播用户面处理网元提供安全算法的情况下，安全算法是加密算法和完整性保护算法中的至少一种。

- 25 S506、密钥生成网元向多播用户面处理网元发送安全算法。相应的，多播用户面处理网元接收来自密钥生成网元的安全算法。

示例性的，在目标安全策略实现为机密性保护策略的情况下，密钥生成网元向多播用户面处理网元发送加密算法。在目标安全策略实现为完整性保护策略的情况下，密钥生成网元向多播用户面处理网元发送完整性保护算法。

如此，密钥生成网元也就能够为多播用户面处理网元提供安全算法，以使多播用户面处理网元采用安全算法对多播业务数据进行安全保护。

- 30 需要说明的是，MUK、MUK 对应的时间信息、目标安全策略和安全算法等四者可以承载于同一消息，如密钥通知消息，也可以承载于不同的消息，本申请实施例对此不作限定。

在一些实施例，密钥生成网元还能够向终端设备发送第一信息，以使终端设备确定 MUK，具体实现过程如图 5 中的 S507 至 S509 所示：

- 35 S507、密钥生成网元向接入网设备发送第一信息。相应的，接入网设备接收来自密钥生成网元的第一信息。

其中，“第一信息”的介绍可以参见 S5011 的相关说明，此处不再赘述。可选的，第一信息还包括业务配置信息。这里，“业务配置信息”的介绍可以参见图 3 中步骤 6 的相关说明，此处不再赘述。

例如，在密钥生成网元实现为 SMF 网元的情况下，SMF 网元向 AMF 网元发送第一信息，

相应的，AMF 网元接收来自 SMF 网元的第一信息。AMF 网元向接入网设备发送第一信息。
相应的，接入网设备接收来自 AMF 网元的第一信息。

再如，在密钥生成网元实现为 AMF 网元的情况下，AMF 网元向接入网设备发送第一信息。相应的，接入网设备接收来自 AMF 网元的第一信息。示例性的，第一信息承载于会话

5 修改请求。

又如，在密钥生成网元实现为 AUSF 网元的情况下，AUSF 网元向 SMF 网元发送第一信息，相应的，SMF 网元接收来自 AUSF 网元的第一信息。SMF 网元向 AMF 网元发送第一信息，相应的，AMF 网元接收来自 SMF 网元的第一信息。AMF 网元向接入网设备发送第一信息。相应的，接入网设备接收来自 AMF 网元的第一信息。

10 S508、接入网设备向终端设备发送第一信息。相应的，终端设备接收来自接入网设备的第一信息。

示例性的，第一信息承载于 RRC 重配置消息。这里，“接入网设备向终端设备发送 RRC 重配置消息”的实现过程可以参见图 3 中步骤 8 的相关说明，此处不再赘述。

S509、终端设备根据第一信息和共享密钥，生成 MUK。

15 其中，共享密钥的介绍可以参见 S5012 的相关说明，此处不再赘述。S509 的具体实现过程可以参见 S5012 的相关说明，此处不再赘述。

需要说明的是，在密钥生成网元确定目标安全策略的类型为第一种类型的情况下，密钥生成网元向终端设备发送目标安全策略。相应的，终端设备接收来自密钥生成网元的目标安全策略。在密钥生成网元确定目标安全策略的类型为第二种类型的情况下，密钥生成网元可以不再向终端设备发送目标安全策略。替代性的，终端设备接收来自多播用户面处理网元的安全保护状态信息。类似的，在密钥生成网元确定安全算法的情况下，密钥生成网元向终端设备发送安全算法。相应的，终端设备接收来自密钥生成网元的安全算法。在密钥生成网元确定目标安全策略的类型为第二种类型的情况下，密钥生成网元不再向终端设备发送安全算法。替代性的，终端设备接收来自多播用户面处理网元的安全算法。这里，
20 目标安全策略、安全算法和第一信息可以承载于同一消息，也可以承载于不同消息，本申请实施例对此不作限定。在目标安全策略通过控制面消息传输至终端设备的情况下，多播用户面处理网元无需再向终端设备提供目标安全策略。类似的，在安全算法通过控制面消息传输至终端设备的情况下，多播用户面处理网元无需再向终端设备提供安全算法。

25 当然，容易理解的是，无论目标安全策略属于第一种类型，还是第二种类型，SMF 也可以均不向终端设备发送目标安全策略，以及安全算法，由多播用户面处理网元向终端设备提供目标安全策略，以及安全算法，详见 S512 至 S515 的具体说明，此处不再赘述。

以上，主要是针对“MUK 的协商”的相关说明，在此阶段，终端设备和多播用户面网元均获取到 MUK。

第二阶段、MSK 层级的密钥协商。在此阶段，多播用户面处理网元和终端设备均获取目标密钥，如目标 MSK、第一子密钥、第二子密钥等，具体实现过程参见 S510 至 S515 的相关说明：
35

S510、多播用户面处理网元获取目标密钥。

例如，多播用户面处理网元生成上述目标密钥，具体实现过程可以参见现有技术，此处不再赘述。

再如，密钥生成网元获取目标密钥之后，密钥生成网元向多播用户面处理网元发送目标密钥。相应的，多播用户面处理网元接收来自密钥生成网元的目标密钥，具体参见图 12 中 S1201 和 S1202 的相关说明，此处不再赘述。

5 S511、多播用户面处理网元向终端设备发送目标密钥。相应的，终端设备接收来自多播用户面处理网元的目标密钥。

示例性的，目标密钥承载于密钥分发消息。这里，密钥分发消息属于多媒体互联网密钥(multimedia internet key, MIKEY)消息。在多播用户面处理网元为终端设备提供目标密钥的情况下，目标密钥即承载于用户面消息，终端设备从用户面消息中获取目标密钥。

10 在一些实施例中，MUK 保护目标密钥的分发，S511 具体实现过程也可以替换为图 7(a) 中所所示的 S5111 至 S5113：

S5111、多播用户面处理网元采用 MUK 加密目标密钥，以得到密钥信息。

示例性的，在时刻 1，终端设备被允许接入多播业务。多播用户面处理网元采用时刻 1 对应的 MUK 加密目标密钥，以得到密钥信息。这里，时刻 1 处于 MUK 的有效时间范围内。

15 S5112、多播用户面处理网元向终端设备发送密钥信息。相应的，终端设备接收来自多播用户面处理网元的密钥信息。

示例性的，密钥信息承载于密钥分发消息。

S5113、终端设备采用 MUK 解密密钥信息，以得到目标密钥。

示例性的，在时刻 1，终端设备被允许接入多播业务。终端设备拥有时刻 1 对应的 MUK，如此，终端设备采用时刻 1 对应的 MUK 解密密钥信息，即可得到目标密钥。

20 也就是说，多播用户面处理网元向不同终端设备发送的密钥信息采用不同的 MUK 加密，如此，终端设备基于自身拥有的 MUK 即可得到目标密钥，以提升目标密钥传输的可靠性。

在一些实施例中，为了使得终端设备获取目标 MSK 的标识，本申请实施例提供两种可能的实现方式，具体如下情况一和情况二的相关说明：

25 情况一、多播用户面处理网元向终端设备发送目标 MSK 的标识。相应的，终端设备接收来自多播用户面处理网元的目标 MSK 的标识。

例如，目标 MSK 的标识包括“多播服务的 ID”和“密钥序号部分(key number part)”两部分。即目标 MSK 的标识实现为“多播服务的 ID+密钥序号部分”的情况下，“多播服务的 ID+密钥序号部分”从多播用户面处理网元传输至终端设备。这里，“多播服务的 ID”的介绍可以参见 S5011 的相关说明，此处不再赘述。

30 如此，终端设备即可从多播用户面处理网元获取目标 MSK 的标识。

情况二、首先，多播用户面处理网元向终端设备发送密钥序号部分。相应的，终端设备接收来自多播用户面处理网元的密钥序号部分。然后，终端设备根据密钥序号部分和多播服务的 ID，确定目标 MSK 的标识。

35 例如，仍以目标 MSK 的标识实现为“多播服务的 ID+密钥序号部分”的情况为例，密钥序号部分从多播用户面处理网元传输至终端设备。终端设备可以结合已获取的“多播服务的 ID”和密钥序号部分，恢复出目标 MSK 的标识。

如此，在多播用户面处理网元向终端设备提供密钥序号部分的情况下，终端设备也能够确定目标 MSK 的标识，与传输“目标 MSK 的标识”相比，节省了传输资源开销。

在一些实施例中，多播用户面处理网元还能够确定安全保护状态信息，并提供给终端

设备，具体实现过程如图 5 中的 S512 和 S513 所示：

S512、多播用户面处理网元确定安全保护状态信息。

其中，安全保护状态信息指示安全保护状态。安全保护包括数据加密和完整性验证中的至少一种。例如，安全保护状态信息指示数据加密保护的开启或关闭，和/或，安全保护状态信息指示完整性验证的开启或关闭。

示例性的，在多播用户面处理网元执行 S504 的情况下，S512 的具体实现过程可以例但但不限于图 7 (b) 所示的 S504 和 S5121，其中，S5121 的具体说明如下：

S5121、多播用户面处理网元根据目标安全策略确定安全保护状态信息。

示例性的，在目标安全策略的类型为第一种类型的情况下，多播用户面处理网元可以确定安全保护状态信息与目标安全策略一致。也就是说，若目标安全策略指示终端设备与多播用户面处理网元之间的安全保护需要执行，则终端设备与多播用户面处理网元之间的安全保护开启。若目标安全策略指示终端设备与多播用户面处理网元之间的安全保护不需要执行，则终端设备与多播用户面处理网元之间的安全保护关闭。

示例性的，在目标安全策略的类型为第二种类型的情况下，若目标安全策略指示终端设备与多播用户面处理网元之间的安全保护需要执行或不需要执行，则多播用户面处理网元可以确定安全保护状态信息与目标安全策略一致，具体参见“目标安全策略的类型为第一种类型”的相关说明，此处不再赘述。若目标安全策略指示为“偏好”，即终端设备与多播用户面处理网元之间的安全保护可以执行，也可以不执行，则多播用户面处理网元根据本地配置确定安全保护状态信息，即多播用户面处理网元根据本地配置确定“终端设备与多播用户面处理网元之间的安全保护开启或关闭”。

可选的，在密钥生成网元未向终端设备提供目标安全策略的情况下，多播用户面处理网元执行 S513：

S513、多播用户面处理网元向终端设备发送安全保护状态信息。相应的，终端设备接收来自多播用户面处理网元的安全保护状态信息。

示例性的，在安全保护状态信息对应数据加密保护的情况下，多播用户面处理网元为终端设备指示数据加密保护是否执行。在安全保护状态信息对应完整性验证的情况下，多播用户面处理网元为终端设备指示完整性验证是否执行。

如此，多播用户面处理网元能够为终端设备提供安全保护状态信息，以使终端设备基于安全保护状态信息对目标数据进行处理。

在一些实施例，在密钥生成网元未向终端设备提供安全算法的情况下，多播用户面处理网元还能够确定安全算法，并提供给终端设备，具体实现过程如图 5 中的 S514 和 S515 所示：

S514、多播用户面处理网元确定安全算法。

其中，安全算法用于数据安全保护计算。

示例性的，安全算法包括加密算法和完整性保护算法。安全算法可以和安全保护状态信息耦合。例如，在安全保护状态信息对应机密性保护的情况下，安全算法为加密算法。在安全保护状态信息对应完整性保护的情况下，安全算法为完整性保护算法。当然，安全算法也可以和安全保护状态信息解耦。例如，在多播用户面处理网元预先为终端设备提供安全算法的情况下，安全算法是加密算法和完整性保护算法中的至少一种。

S515、多播用户面处理网元向终端设备发送安全算法。相应的，终端设备接收来自多播用户面处理网元的安全算法。

示例性的，在安全保护状态信息对应机密性保护的情况下，多播用户面处理网元向终端设备发送加密算法。在安全保护状态信息对应完整性保护的情况下，多播用户面处理网元向终端设备发送完整性保护算法。

如此，多播用户面处理网元也就能够为终端设备提供安全算法，以使终端设备采用安全算法对目标数据进行处理。

需要说明的是，目标密钥、密钥信息、目标 MSK 的标识、密钥序号部分、安全保护状态信息和安全算法等六者可以承载于同一消息，如 MIKEY 消息，也可以承载于不同的消息，本申请实施例对此不作限定。

以上，主要是针对“MSK 层级的密钥协商”的相关说明，在此阶段，多播用户面网元获取到目标密钥之后，还能够向终端设备提供目标密钥。如此，多播用户面处理网元和终端设备均获取目标密钥。当然，容易理解的是，图 5 所示的“第二阶段、MSK 层级的密钥协商”也可以替换为图 12 所示的“第一阶段、MSK 层级的密钥协商”，具体实现过程详见图 12 中 S1201 至 S1204 的相关说明，此处不再赘述。

第三阶段、数据的传输。在此阶段，多播用户面处理网元为终端设备提供目标数据，具体实现过程参见 S516 至 S518 的相关说明：

S516、多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据。

其中，目标密钥的介绍可以参见 S510 的相关说明，此处不再赘述。若多播用户面处理网元执行“数据加密”保护，但未执行“完整性验证”，则目标数据包括密文，不包括消息认证码（message authentication code，MAC）。若多播用户面处理网元未执行“数据加密”保护，但执行“完整性验证”，则目标数据包括多播业务数据（也可以称为明文）和 MAC。若多播用户面处理网元执行“数据加密”保护和“完整性验证”，则目标数据包括密文和 MAC。

其中，S516 的具体实现方式有多种，可以例如但不限于如下四个方面的介绍：

第一方面、从安全保护的触发条件上来说，多播用户面处理网元在“安全保护状态信息指示的状态为开启”的情况下，才执行安全保护，即 S516 具体实现为：若安全保护状态信息指示的状态为开启，则多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据。也就是说，在终端设备和多播用户面处理网元之间的安全保护开启的情况下，多播用户面处理网元才对多播业务数据执行安全保护，以保证多播业务数据的安全传输。

第二方面、从安全保护对应的安全算法上来说，多播用户面处理网元在获取到“安全算法”的情况下，才执行安全保护。示例性的，在“多播用户面处理网元执行 S506”或“多播用户面处理网元接收来自 AMF 网元的安全算法”的情况下，S516 具体实现为：多播用户面处理网元采用安全算法和目标密钥对多播业务数据进行安全保护，以得到目标数据。这里，在安全算法实现为“加密算法”的情况下，多播用户面处理网元采用加密算法和目标密钥对多播业务数据进行加密，以得到密文。在安全算法实现为“完整性保护算法”的情况下，多播用户面处理网元根据完整性保护算法和多播业务数据，确定 MAC。也就是说，

在多播用户面处理网元具备安全算法的情况下，多播用户面处理网元才对多播业务数据执行安全保护，以保证多播业务数据的安全传输。

第三方面、从安全保护的类型上来说，安全保护包括数据加密和完整性验证两种类型。

5 在多播用户面处理网元执行“数据加密”保护的情况下，多播用户面处理网元采用目标 MSK 或第一子密钥对多播业务数据进行加密，以得到密文。其中，目标数据包括密文。这里，加密的具体实现过程可以是：将目标 MSK（或第一子密钥）和多播业务数据输入至加密算法中进行运算，以得到密文。在实际应用过程中，多播用户面处理网元还将其他信元输入至加密算法中，具体实现过程可以参见现有技术，此处不再赘述。

10 在多播用户面处理网元执行“完整性验证”的情况下，多播用户面处理网元根据目标 MSK 和第二子密钥中的至少一项，以及多播业务数据，确定 MAC。其中，目标数据包括 MAC。这里，“确定 MAC”的具体实现过程可以是：将目标 MSK（或第二子密钥）和多播业务数据输入至完整性保护算法，以得到 MAC。在实际应用过程中，多播用户面处理网元还将其他信元输入至完整性保护算法中，具体实现过程可以参见现有技术，
15 此处不再赘述。

如此，若多播用户面处理网元对多播业务数据执行“数据加密”保护，则可以达到隐藏数据的效果。若多播用户面处理网元对多播业务数据执行“完整性验证”，则可以避免数据篡改。

20 第四方面、从执行安全保护的密钥上来说，执行安全保护的密钥可以是目标 MSK 本身，也可以是基于目标 MSK 确定的第一推演密钥，如目标 MSK 对应的第一子密钥、目标 MSK 对应的第二子密钥等。以“采用第一推演密钥对多播业务数据进行安全保护”为例，参见图 8，S516 可以具体实现为 S5161 和 S5162：

S5161、多播用户面处理网元对目标 MSK 进行推演运算，以得到第一推演密钥。

25 其中，推演运算的算法可以是 HMAC 算法。这里，第一推演密钥包括第一子密钥和第二子密钥。示例性的，S5161 可以具体实现为如下示例一和示例二：

示例一、多播用户面处理网元对目标 MSK 进行第一推演运算，以得到第一子密钥。

其中，第一推演密钥包括第一子密钥，第一子密钥用于机密性保护计算，记为 MSK_enc。例如，多播用户面处理网元将目标 MSK 作为输入密钥，将加密算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第一子密钥，具体实现过程可以参见现有技术，此处不再赘述。

30 如此，多播用户面处理网元利用目标 MSK，采用推演方式，即可得到第一子密钥，以对多播业务数据进行安全保护。

示例二、多播用户面处理网元对目标 MSK 进行第二推演运算，以得到第二子密钥。

其中，第一推演密钥包括第二子密钥，第二子密钥用于完整性保护计算，记为 MSK_int。例如，多播用户面处理网元将目标 MSK 作为输入密钥，将完整性保护算法作为输入参数，
35 采用 HMAC 算法进行推演运算，以得到第二子密钥，具体实现过程可以参见现有技术，此处不再赘述。

如此，多播用户面处理网元利用目标 MSK，采用推演方式，即可得到第二子密钥，以对多播业务数据进行安全保护。

S5162、多播用户面处理网元采用第一推演密钥对多播业务数据进行安全保护，以得

到目标数据。

例如，多播用户面处理网元采用第一子密钥对多播业务数据进行加密保护，以得到密文。此种情况下，目标数据包括密文。

再如，多播用户面处理网元采用第二子密钥对多播业务数据进行完整性保护，以得到
5 MAC。此种情况下，目标数据包括 MAC。

如此，多播用户面处理网元还能够对目标 MSK 进行推演，采用第一推演密钥执行安全保护。

S517、多播用户面处理网元向终端设备发送目标数据。相应的，终端设备接收来自多播用户面处理网元的目标数据。

10 在实际应用过程中，多播用户面处理网元向接入网设备发送目标数据。相应的，接入网设备接收来自多播用户面处理网元的目标数据。接入网设备向终端设备发送目标数据。相应的，终端设备接收来自接入网设备的目标数据。

S518、终端设备采用目标密钥对目标数据进行处理，以得到目标数据的处理结果。

其中，目标密钥的介绍可以参见 S510 的相关说明，此处不再赘述。

15 示例性的，目标数据包括目标密钥（如目标 MSK）的标识，终端设备根据目标数据中的目标密钥的标识，索引到目标密钥。终端设备采用索引到的目标密钥（即与目标密钥的标识对应的目标密钥）对目标数据进行处理。也就是说，在目标数据携带目标密钥的标识的情况下，目标数据中的目标密钥的标识能够指示终端设备采用哪一密钥来对该目标数据进行处理，方便终端设备索引到与目标数据中的目标密钥的标识对应的目标密钥。

20 若目标数据包括密文，不包括 MAC，则终端设备执行“数据解密”，以得到多播业务数据（也可以称为明文）。若目标数据包括多播业务数据（也可以称为明文）和 MAC，则终端设备执行“完整性验证”，以验证多播业务数据的完整性。若目标数据包括密文和 MAC，则终端设备执行“数据解密”和“完整性验证”，验证密文对应的多播业务数据的完整性。

其中，S518 的具体实现方式有多种，可以例如但不限于如下四个方面的介绍：

25 第一方面、从终端设备执行处理的触发条件上来说，终端设备在“安全保护状态信息指示的状态为开启”的情况下，才执行处理，即 S518 具体实现为：若安全保护状态信息指示的状态为开启，则终端设备采用目标密钥对目标数据进行处理，以得到目标数据的处理结果。或者，终端设备在“目标安全策略指示安全保护的状态为开启”的情况下，才执行处理，即 S518。也就是说，在终端设备和多播用户面处理网元之间的安全保护开启的情况下，
30 终端设备才对目标数据执行处理，提高数据处理效率。

第二方面、从终端设备执行处理所采用的安全算法上来说，终端设备在获取到“安全算法”的情况下，才执行处理。示例性的，终端设备从密钥生成网元获取安全算法或执行 S515 的情况下，S518 具体实现为：终端设备采用安全算法和目标密钥对目标数据进行处理，以得到目标数据的处理结果。这里，在安全算法实现为“加密算法”的情况下，终端设备采用加密算法和目标密钥对目标数据进行解密，以得到明文。在安全算法实现为“完整性保护算法”的情况下，终端设备根据完整性保护算法和 MAC，验证多播业务数据的完整性。也就是说，在终端设备具备安全算法的情况下，终端设备才对目标数据执行处理，
35 以得到目标数据的处理结果。

第三方面、从终端设备执行处理的处理类型上来说，终端设备所执行的处理的类型类

型包括数据解密和完整性验证两种类型。

在目标数据包括密文，不包括 MAC 的情况下，终端设备执行“数据解密”，即终端设备采用目标 MSK 或第一子密钥对密文进行解密，以得到第一明文。其中，目标数据的处理结果包括第一明文。这里，解密的具体实现过程可以是：将目标 MSK（或第一子密钥）和密文输入至加密算法中进行处理，以得到第一明文，具体实现过程可以参见现有技术，此处不再赘述。

在目标数据包括第二明文和 MAC 的情况下，终端设备执行“完整性验证”，即终端设备根据目标 MSK 和第二子密钥中的至少一项，以及 MAC，确定第二明文的完整性。其中，目标数据的处理结果包括第二明文的完整性。这里，完整性验证的具体实现过程可以是：将目标 MSK（或第二子密钥）和第二明文输入至完整性保护算法，以得到 MAC。终端设备对比接收到的 MAC 与自身计算的 MAC 是否相同。若相同，则验证成功，具体实现过程可以参见现有技术，此处不再赘述。

在目标数据包括密文和 MAC 的情况下，终端设备执行“数据解密”和“完整性验证”，即终端设备采用目标 MSK 或第一子密钥对密文进行解密，以得到第一明文。终端设备根据目标 MSK 和第二子密钥中的至少一项，以及 MAC，确定第一明文的完整性。

如此，在数据隐藏的情况下，即目标数据包括密文，终端设备能够对目标数据解密，以获取明文。在目标数据包括 MAC 的情况下，终端设备能够对目标数据执行“完整性验证”，以验证数据完整性，避免数据篡改。

第四方面、从执行处理的密钥上来说，执行处理的密钥可以是基于目标 MSK 确定的第一推演密钥，如目标 MSK 对应的第一子密钥、目标 MSK 对应的第二子密钥等。以“采用第一推演密钥对目标数据进行处理”为例，参见图 9，S518 可以具体实现为 S5181 和 S5182：

S5181、终端设备对目标 MSK 进行推演运算，以得到第一推演密钥。

其中，推演运算的算法可以是 HMAC 算法。这里，第一推演密钥包括第一子密钥和第二子密钥。这里，S5181 的具体实现过程与 S5161 一致，即执行主体为终端设备，具体通过示例一和示例二进行说明：

示例一、终端设备对目标 MSK 进行第一推演运算，以得到第一子密钥。

其中，第一推演密钥包括第一子密钥，第一子密钥用于机密性保护计算，记为 MSK_enc。例如，终端设备将目标 MSK 作为输入密钥，将加密算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第一子密钥，具体实现过程可以参见现有技术，此处不再赘述。

如此，终端设备利用目标 MSK，采用推演方式，即可得到第一子密钥，以对目标数据进行解密。

示例二、终端设备对目标 MSK 进行第二推演运算，以得到第二子密钥。

其中，第一推演密钥包括第二子密钥，第二子密钥用于完整性保护计算，记为 MSK_int。例如，终端设备将目标 MSK 作为输入密钥，将完整性保护算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第二子密钥，具体实现过程可以参见现有技术，此处不再赘述。

如此，终端设备利用目标 MSK，采用推演方式，即可得到第二子密钥，以对目标数据进行完整性验证。

S5182、终端设备采用第一推演密钥对目标数据进行处理，以得到目标数据的处理结果。

例如，在目标数据包括密文的情况下，终端设备采用第一子密钥对目标数据进行处理，以得到密文。

再如，在目标数据包括 MAC 的情况下，终端设备根据第二子密钥和 MAC，验证多播业务数据的完整性。

5 如此，终端设备还能够对目标 MSK 进行推演，采用第一推演密钥执行处理。

以上，主要是针对“数据的传输”的相关说明，在此阶段，多播用户面网元向终端设备提供经过安全保护后的目标数据，以达到隐藏数据的效果，或降低数据篡改的可能性。

在一些实施例，多播用户面处理网元还能够确定目标 MTK 的生成状况，如图 5 所示的 S519：

10 S519、多播用户面处理网元确定目标 MTK 的生成状况。

例如，多播用户面处理网元接收来自终端设备的消息。其中，来自终端设备的消息包括会话类型或传输协议类型。多播用户面处理网元以会话类型或传输协议类型作为判断依据。若会话类型是下载类型或流类型，则多播用户面处理网元确定生成目标 MTK。反之，若传输协议类型不是下载类型和流类型，则多播用户面处理网元确定无需目标 MTK。若传输协议类型为 RTP 或 FLUTE 或其他协议，则多播用户面处理网元确定生成目标 MTK。反之，若传输协议类型不是 RTP 和 FLUTE，则多播用户面处理网元确定无需目标 MTK。

再如，多播用户面处理网元接收来自 SMF 网元的消息。其中，来自 SMF 网元的消息包括传输协议指示或服务质量（quality of service, QoS）参数。或者，多播用户面处理网元接收来自 AF 网元的消息。其中，来自 AF 网元的消息包括传输协议指示。若传输协议指示的传输协议类型为 RTP 或 FLUTE 或其他协议，则多播用户面处理网元确定生成目标 MTK。反之，若传输协议指示的传输协议类型不是 RTP 和 FLUTE，则多播用户面处理网元确定无需目标 MTK。若 QoS 参数中流量类型参数是下载类型或者流类型，则多播用户面处理网元确定生成目标 MTK。反之，若 QoS 参数中流量类型参数不是下载类型和者流类型，则多播用户面处理网元确定无需生成目标 MTK。

25 又如，多播用户面处理网元根据网络类型确定目标 MTK 的生成状况。若网络类型为 LTE 网络或 LTE 网络之前的网络，则多播用户面处理网元确定生成目标 MTK。若网络类型为 5G 网络或 5G 网络之后的网络，则多播用户面处理网元确定无需生成目标 MTK。

这里，多播用户面处理网元可以在执行第三阶段之前，执行 S519，以确定目标 MTK 的生成状况。

30 也就是说，多播用户面处理网元能够自主确定是否生成目标 MTK。若不生成目标 MTK，则多播用户面处理网元执行“第三阶段、数据的传输”，采用目标密钥对多播业务数据进行安全保护，以得到目标数据。

下面，以生成目标 MTK 为例，对本申请实施例提供的第二种密钥管理方法进行说明。该密钥管理方法应用在 MBS 通信过程中。终端设备完成注册和 PDU 会话建立的过程，且加入多播服务，详见图 3 中的步骤 1 至步骤 5 的相关说明，此处不再赘述。在终端设备加入多播服务之后，执行图 10 所示的密钥管理方法的，具体步骤如下：

35 第一阶段和第二阶段的介绍可以参见“第一种密钥管理方法”的相关说明，此处不再赘述。

第三阶段、MTK 层级的密钥协商。在此阶段，多播用户面处理网元和终端设备均获取

目标 MTK 或目标 MTK 对应的子密钥，具体过程如图 10 所示的 S1001 至 S1006：

S1001、多播用户面处理网元对目标 MSK 和第二信息进行推演运算，以得到第二推演密钥。

其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。

- 5 这里，协议名称可以是 RTP 或 FULTE。目标 MTK 的标识可以是多播用户面处理网元生成并维护的。目标 MTK 的标识可以是 1 开始的计数。第二参数可以是基于第二随机数、第二计数值、或第二时间戳中的至少一项确定的参数。例如，第二参数为上述第二随机数、第二计数值或第二时间戳等。第二参数由多播用户面处理网元生成和维护。

- 10 其中，第二推演密钥包括目标 MTK、第三子密钥或第四子密钥。示例性的，S1001 可以具体实现为如下示例一至示例三：

示例一、多播用户面处理网元对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK。

- 15 例如，多播用户面处理网元将目标 MSK 作为输入密钥，将第二信息作为输入参数，采用 HMAC 算法进行第二推演运算，以得到目标 MTK，具体实现过程可以参见现有技术，此处不再赘述。

如此，多播用户面处理网元利用目标 MSK，采用推演方式，即可得到目标 MTK，以对多播业务数据进行加密保护或完整性保护。

- 20 示例二、首先，多播用户面处理网元通过对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK，或者多播用户面处理网元本地生成目标 MTK。然后，多播用户面处理网元对目标 MTK 进行第四推演运算，以得到第三子密钥。例如，多播用户面处理网元将目标 MTK 作为输入密钥，将加密算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第三子密钥，具体实现过程可以参见现有技术，此处不再赘述。其中，第三子密钥用于机密性保护计算。

- 25 如此，多播用户面处理网元利用目标 MSK，采用推演方式，即可得到第三子密钥，以对多播业务数据进行加密保护。

- 30 示例三、首先，多播用户面处理网元通过对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK，或者多播用户面处理网元本地生成目标 MTK。然后，多播用户面处理网元对目标 MTK 进行第五推演运算，以得到第四子密钥。例如，多播用户面处理网元将目标 MTK 作为输入密钥，将完整性保护算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第四子密钥，具体实现过程可以参见现有技术，此处不再赘述。其中，第四子密钥用于完整性保护计算。

如此，多播用户面处理网元利用目标 MSK，采用推演方式，即可得到第四子密钥，以对多播业务数据进行完整性保护。

- 35 S1002、多播用户面处理网元向终端设备发送第二信息。相应的，终端设备接收来自多播用户面处理网元的第二信息。

示例性的，多播用户面处理网元向接入网设备发送第二信息。相应的，接入网设备接收来自多播用户面处理网元的第二信息。接入网设备向终端设备发送第二信息。相应的，终端设备接收来自接入网设备的第二信息。这里，第二信息可以承载于多播消息。

可选的，如图 11 所示，S1002 也可以替换为 S1003 至 S1005：

S1003、多播用户面处理网元采用目标 MSK 加密第二信息，以得到加密信息。

示例性的，加密信息承载于多播消息。其中，多播消息包括两部分，一部分是保护部分，另一部分是未保护部分。保护部分为上述加密信息，未保护部分包括目标 MSK 的标识，

5 该标识对应的目标 MSK 是对第二信息加密的密钥。

S1004、多播用户面处理网元向终端设备发送加密信息。相应的，终端设备接收来自多播用户面处理网元的加密信息。

示例性的，加密信息承载于多播消息。多播消息还包括目标 MSK 的标识。多播消息中的标识所对应的目标 MSK 即为对第二信息解密的密钥。

10 示例性的，多播用户面处理网元通过接入网设备向终端设备发送加密信息。相应的，终端设备通过接入网设备接收来自多播用户面处理网元的加密信息。

S1005、终端设备采用目标 MSK 对加密信息进行解密，以得到第二信息。

示例性的，在多播消息还包括目标 MSK 的标识的情况下，终端设备根据多播消息中的目标密钥的标识索引到目标 MSK，采用索引到的目标 MSK（即与目标 MSK 的标识对应的目标 MSK）解密上述加密信息，以得到第二信息。

这里，虽然第二信息是通过多播消息分发的，由于目标 MSK 是通过单播消息传输的，目标 MSK 保护了第二信息的分发过程，且第二信息用于目标 MTK 的推演。如此，基于第二信息推演的目标 MTK 的安全性相当于单播消息传输的安全性。

需要说明的是，目标 MTK 还可以是多播用户面处理网元本地生成的随机数或其他形式。

20 在目标 MTK 为随机数的情况下，多播用户面处理网元向终端设备发送多播消息。相应的，终端设备接收来自多播用户面处理网元的多播消息。其中，多播消息仍包括保护部分和未保护部分。保护部分是由目标 MSK 对目标 MTK 和目标 MTK 的标识加密后的部分，未保护部分包括目标 MSK 的标识。另外，在执行“MTK 层级的密钥协商”阶段的情况下，“安全保护状态信息”和“安全算法”中的至少一项可以在“MSK 层级的密钥协商”阶段传输，也可以在“MTK 层级的密钥协商”阶段传输。例如，“安全保护状态信息”和“安全算法”中的至少一项承载于多播消息，本申请实施例对此不作限定。

S1006、终端设备对目标 MSK 和第二信息进行推演运算，以得到第二推演密钥。

其中，第二信息的相关说明可以参见 S1001 的相关说明，此处不再赘述。

其中，第二推演密钥包括目标 MTK、第三子密钥或第四子密钥。S1006 的具体实现过程与 S1001 的过程一致，即执行主体为终端设备，具体通过如下示例一至示例三进行说明：

示例一、终端设备对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK。

例如，终端设备将目标 MSK 作为输入密钥，将第二信息作为输入参数，采用 HMAC 算法进行第二推演运算，以得到目标 MTK，具体实现过程可以参见现有技术，此处不再赘述。

35 如此，终端设备利用目标 MSK，采用推演方式，即可得到目标 MTK，以对目标数据进行解密或完整性验证。

示例二、首先，终端设备通过对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK，或者，终端设备本地生成目标 MTK。然后，终端设备对目标 MTK 进行第四推演运算，以得到第三子密钥。例如，终端设备将目标 MTK 作为输入密钥，将加密算法作为

输入参数，采用 HMAC 算法进行推演运算，以得到第三子密钥，具体实现过程可以参见现有技术，此处不再赘述。

如此，终端设备利用目标 MSK，采用推演方式，即可得到第三子密钥，以对目标数据进行解密。

5 示例三、首先，终端设备通过对目标 MSK 和第二信息进行第三推演运算，以得到目标 MTK，或者，终端设备本地生成目标 MTK。然后，终端设备对目标 MTK 进行第五推演运算，以得到第四子密钥。例如，终端设备将目标 MTK 作为输入密钥，将完整性保护算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第四子密钥，具体实现过程可以参见现有技术，此处不再赘述。其中，第四子密钥用于完整性保护计算。

10 如此，终端设备利用目标 MSK，采用推演方式，即可得到第四子密钥，以对目标数据进行完整性保护。

以上，主要是针对“MTK 层级的密钥协商”的相关说明。在此阶段，多播用户面网元能够获取到 MTK 层级的密钥，如目标 MTK、第三子密钥或第四子密钥。之后，多播用户面处理网元还能够向终端设备提供第二信息，以使终端设备确定 MTK 层级的密钥。如此，多播用户面处理网元和终端设备均获取 MTK 层级的密钥。

15 第四阶段、数据的传输。在此阶段，多播用户面处理网元为终端设备提供目标数据，具体实现过程参见 S1007 至 S1009 的相关说明：

S1007、多播用户面处理网元采用目标密钥对多播业务数据进行安全保护，以得到目标数据。

20 这里，“安全保护的触发条件”、“安全保护对应的安全算法”和“安全保护的类型”三个方面与 S516 一致，从执行安全保护的密钥上来说，执行安全保护的目标密钥实现为第二推演密钥，如目标 MTK、第三子密钥或第四子密钥。关于“目标 MTK、第三子密钥或第四子密钥”的介绍可以参见 S1001 的相关说明，此处不再赘述。

25 S1008、多播用户面处理网元向终端设备发送目标数据。相应的，终端设备接收来自多播用户面处理网元的目标数据。

其中，S1008 的具体实现过程可以参见 S517 的介绍，此处不再赘述。

S1009、终端设备采用目标密钥对目标数据进行处理，以得到目标数据的处理结果。

30 这里，“终端设备执行处理的触发条件”、“终端设备执行处理所采用的安全算法”和“终端设备执行处理的处理类型”三个方面与 S518 一致，从执行处理的密钥上来说，执行安全保护的目标密钥实现为第二推演密钥，如目标 MTK、第三子密钥或第四子密钥。关于“目标 MTK、第三子密钥或第四子密钥”的介绍可以参见 S1006 的相关说明，此处不再赘述。

35 示例性的，目标数据还包括目标 MTK 的标识，终端设备基于目标数据中的标识索引到目标 MTK，终端设备采用索引到的目标 MTK（与目标 MTK 的标识对应的目标 MTK）对目标数据进行处理。

以上，主要是针对“数据的传输”的相关说明，在此阶段，多播用户面网元向终端设备提供经过安全保护后的目标数据，以达到隐藏数据的效果，或降低数据篡改的可能性。

本申请实施例提供第三种密钥管理方法，该密钥管理方法应用在 MBS 通信过程中。终端设备完成注册和 PDU 会话建立的过程，且加入多播服务，详见图 3 中的步骤 1 至步骤 5

的相关说明，此处不再赘述。在终端设备加入多播服务之后，执行图 12 所示的密钥管理方法的，具体步骤如下：

第一阶段、MSK 层级的密钥协商。在此阶段，终端设备和多播用户面网元均获取到目标密钥，如目标 MSK、第一子密钥或第二子密钥，具体实现过程参见 S1201 至 S1204 的相关说明：

5 相关说明：

S1201、密钥生成网元获取目标密钥。

示例性的，密钥生成网元在一定的触发条件下才发起“获取目标密钥”的处理过程。这里，密钥生成网元根据多播服务认证或者授权结果确定是否发起“获取目标密钥”的处理过程。可以理解的是，在密钥生成网元的多播服务认证通过或者已授权的情况下，密钥生成网元发起“获取目标密钥”的处理流程。反之，在密钥生成网元的多播服务认证失败或者未授权的情况下，密钥生成网元不发起“获取目标密钥”的处理过程。其中，“多播服务认证”和“授权”的介绍可以参见 S501 的相关说明，此处不再赘述。

示例性的，“密钥生成网元获取目标密钥”的具体实现过程可以例如但不限于如下介绍：

15 密钥生成网元根据多播服务的标识，向 UDM 网元进行多播传输会话检查，即检查多播服务的标识对应的多播上下文（比如 QoS 信息，目标密钥）是否存在。例如，以密钥生成网元实现为 SMF 网元为例，SMF 网元向 UDM 网元发送多播服务的标识（例如多播服务的 IP 地址）。相应的，UDM 网元接收来自 SMF 网元的多播服务的标识。之后，UDM 网元检查是否存在该多播服务的标识对应的多播上下文。

20 如果 UDM 网元确定该多播服务的标识对应的多播上下文存在，UDM 网元向 SMF 网元发送该多播服务的标识对应的多播上下文。相应的，SMF 网元接收来自 UDM 网元的该多播服务的标识对应的多播上下文。其中，该多播服务的标识对应的多播上下文包括目标密钥。

如果 UDM 网元确定该多播服务的标识对应的多播上下文不存在，SMF 网元可以通过如下两种方式获取目标密钥，具体说明如下：

25 方式一、SMF 网元生成上述目标密钥。例如，SMF 网元利用随机数生成目标 MSK，具体实现过程可以参见现有技术，此处不再赘述。可选的，在 SMF 网元生成目标 MSK 之后，SMF 网元对目标 MSK 进行第一推演运算，以得到第一子密钥，如 SMF 网元将目标 MSK 作为输入密钥，将加密算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第一子密钥。或者，SMF 网元对目标 MSK 进行第二推演运算，以得到第二子密钥，如 SMF 网元将目标 MSK 作为输入密钥，将完整性保护算法作为输入参数，采用 HMAC 算法进行推演运算，以得到第二子密钥。

30 方式二、AUSF 网元生成上述目标密钥。SMF 网元向 AUSF 网元发送密钥请求消息。相应的，AUSF 网元接收来自 SMF 网元的密钥请求消息。其中，密钥请求消息用于请求目标密钥。AUSF 网元接收密钥请求消息之后，向 SMF 网元发送目标密钥。如此，SMF 网元即可获取到目标密钥。这里，若 AUSF 网元无法生成目标密钥，则 AUSF 网元向 SMF 网元发送失败消息。相应的，SMF 网元接收来自 AUSF 网元的失败消息。其中，失败消息包括失败原因值。失败原因值包括以下至少一项：AUSF 网元中存储的 Kausf 不可用，或 AUSF 网元中存储的推演参数不可用等。

需要说明的是，在 UDM 网元确定该多播服务的标识对应的多播上下文不存在的情况下，

SMF 网元获取目标密钥之后，SMF 网元向 UDM 网元发送目标密钥和多播服务的标识。相应的，UDM 网元接收并存储来自 SMF 网元的目标密钥和多播服务的标识。

S1202、密钥生成网元向多播用户面处理网元发送目标密钥。

示例性的，目标密钥承载于密钥通知消息。在多播用户面处理网元接收来自密钥生成网元的密钥通知消息之后，多播用户面处理网元向密钥生成网元发送响应消息。相应的，密钥生成网元接收来自多播用户面处理网元的响应消息。其中，响应消息指示多播用户面处理网元已接收目标密钥。

在一些实施例中，密钥生成网元向多播用户面处理网元发送目标 MSK 对应的时间信息。相应的，多播用户面处理网元接收来自密钥生成网元的目标 MSK 对应的时间信息。其中，目标 MSK 对应的时间信息指示目标 MSK 的有效时间。也就是说，在目标 MSK 的有效时间内，多播用户面处理网元采用目标 MSK 保护第二信息（用于生成目标 MTK 的信息）的分发。如此，终端设备能够得到第二信息，以生成目标 MTK。反之，在目标 MSK 的有效时间外，不再分发第二信息。如此，终端设备无法获取第二信息，也就无法生成目标 MTK。或者，在目标 MSK 的有效时间内，多播用户面处理网元采用目标 MSK 保护多播业务数据的分发。如此，终端设备能够获取到多播业务数据。反之，在目标 MSK 的有效时间外，目标 MSK 不存在，不再分发多播业务数据。如此，终端设备无法获取多播业务数据。

如此，在密钥生成网元为多播用户面处理网元提供目标 MSK 的情况下，密钥生成网元还能够指示目标 MSK 的有效时间，以满足多播用户面处理网元在不同时间段的使用需求。

在一些实施例中，密钥生成网元还能够确定目标安全策略，并提供给多播用户面处理网元，具体可以参见 S503 和 S504 的介绍，此处不再赘述。或者，密钥生成网元还能够为多播用户面处理网元提供安全算法，具体可以参见 S505 和 S506 的介绍，此处不再赘述。

在一些实施例中，密钥生成网元还能够向多播用户面处理网元提供目标 MSK 的标识，本申请实施例提供两种可能的实现方式，具体如下方式一和方式二的相关说明：

方式一、密钥生成网元向多播用户面处理网元发送目标 MSK 的标识。相应的，多播用户面处理网元接收来自密钥生成网元的目标 MSK 的标识。

例如，目标 MSK 的标识包括“多播服务的 ID”和“密钥序号部分”两部分。即目标 MSK 的标识实现为“多播服务的 ID+密钥序号部分”的情况下，“多播服务的 ID+密钥序号部分”从密钥生成网元传输至多播用户面处理网元。这里，“多播服务的 ID”的介绍可以参见 S5011 的相关说明，此处不再赘述。

方式二、首先，密钥生成网元向多播用户面处理网元发送密钥序号部分。相应的，多播用户面处理网元接收来自密钥生成网元的密钥序号部分。然后，多播用户面处理网元根据密钥序号部分和多播服务的 ID，确定目标 MSK 的标识。

例如，仍以目标 MSK 的标识实现为“多播服务的 ID+密钥序号部分”的情况为例，密钥序号部分从密钥生成网元传输至多播用户面处理网元。多播用户面处理网元可以结合已获取的“多播服务的 ID”和密钥序号部分，恢复目标 MSK 的标识。

如此，在密钥生成网元向多播用户面处理网元提供密钥序号部分的情况下，多播用户面处理网元也能够确定目标 MSK 的标识，与传输“目标 MSK 的标识”相比，节省了传输资源开销。

在一些实施例中，密钥生成网元还能够为终端设备提供目标密钥。也就是说，终端设

备通过控制面消息获取目标密钥，具体参见 S1203 至 S1204 的相关说明：

S1203、密钥生成网元向接入网设备发送目标密钥。相应的，接入网设备接收来自密钥生成网元的目标密钥。

例如，在密钥生成网元实现为 SMF 网元的情况下，SMF 网元向 AMF 网元发送目标密钥。

- 5 相应的，AMF 网元接收来自 SMF 网元的目标密钥。AMF 网元向接入网设备发送目标密钥。
相应的，接入网设备接收来自 AMF 网元的目标密钥。

再如，在密钥生成网元实现为 AMF 网元的情况下，AMF 网元向接入网设备发送目标密钥。相应的，接入网设备接收来自 AMF 网元的目标密钥。

- 又如，在密钥生成网元实现为 AUSF 网元的情况下，AUSF 网元向 SMF 网元发送目标密
10 钥。相应的，SMF 网元接收来自 AUSF 网元的目标密钥。SMF 网元向 AMF 网元发送目标密钥。
相应的，AMF 网元接收来自 SMF 网元的目标密钥。AMF 网元向接入网设备发送目标密钥。
相应的，接入网设备接收来自 AMF 网元的目标密钥。

S1204、接入网设备向终端设备发送目标密钥。相应的，终端设备接收来自接入网设备的目标密钥。

- 15 在一些实施例中，密钥生成网元还能够为终端设备提供目标安全策略和安全算法中的至少一项，具体可以参见 S512 至 S515 的相关说明，此处不再赘述。

在一些实施例中，密钥生成网元还能够向终端设备提供目标 MSK 的标识，本申请实施例仍提供两种可能的实现方式，具体如下示例一和示例二的相关说明：

- 示例一、密钥生成网元向终端设备发送目标 MSK 的标识。相应的，终端设备接收来自
20 密钥生成网元的目标 MSK 的标识。

示例二、首先，密钥生成网元向终端设备发送密钥序号部分。相应的，终端设备接收来自密钥生成网元的密钥序号部分。然后，终端设备根据密钥序号部分和多播服务的 ID，确定目标 MSK 的标识。

- 如此，在密钥生成网元向终端设备提供密钥序号部分的情况下，终端设备也能够确定
25 目标 MSK 的标识，与传输“目标 MSK 的标识”相比，节省了传输资源开销。

需要说明的是，对于终端设备来说，终端设备也可以接收来自多播用户面处理网元的目标密钥、安全保护状态信息、安全算法和目标密钥的标识中的至少一项，具体可以参见“第一种密钥管理方法”中的“第一阶段”和“第二阶段”的介绍。

- 以上，主要是针对“MSK 层级的密钥协商”的相关说明，在此阶段，终端设备和多播
30 用户面网元均获取到目标密钥。当然，容易理解的是，图 12 所示的“第一阶段、MSK 层级的密钥协商”也可以替换为图 5 所示的“第二阶段、MSK 层级的密钥协商”，具体实现过程详见图 5 中 S510 至 S515 的相关说明，此处不再赘述。

- 在多播用户面处理网元获取到目标密钥之后，在无需生成目标 MTK 的情况下，则执行
“第一种密钥管理方法”中的“第三阶段、数据的传输”，如图 12 所示。在生成目标 MTK
35 的情况下，则执行“第一种密钥管理方法”中的“第三阶段、MTK 层级的密钥协商”和“第四阶段、数据的传输”，图 12 未示出。

需要说明的是，在本申请实施例提供的密钥管理方法中，仅以“MUK、MSK 和 MTK”等名称作为示例，对密钥管理处理流程进行说明，并不构成对于本申请实施例提供的技术方案的限定。本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，

MUK、MSK 和 MTK 中的至少一项被定义为其他的名称，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

另外，再对“S503 至 S506 的执行时机”进行说明：S503 至 S506 可以在“MUK 的协商”这一阶段执行，具体如图 5 所示，S503 至 S506 也可以在“MSK 层级的密钥协商”这一阶段执行（图 5 所示的第二阶段和图 12 所示的第一阶段均为），S503 至 S506 还可以在“MTK 层级的密钥协商”这一阶段（如图 10 所示的第三阶段执行，即在“数据的传输”阶段之前执行 S503 至 S506 即可。若在“MUK 的协商”或“MSK 层级的密钥协商”阶段执行 S503 至 S506，则 S512 至 S515 可以在“MSK 层级的密钥协商”这一阶段执行（如图 5 所示），S512 至 S515 也可以在“MTK 层级的密钥协商”这一阶段执行（如图 10 未示出）。若在“MTK 层级的密钥协商”阶段执行 S503 至 S506，则 S512 至 S515 在“MTK 层级的密钥协商”这一阶段执行（如图 10 未示出）。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。相应的，本申请实施例还提供了通信装置，该通信装置可以为上述方法实施例中的网元，或者包含上述网元的装置，或者为可用于网元的部件。可以理解的是，该通信装置为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

图 13 示出了一种通信装置 1300 的结构示意图。该通信装置 1300 包括通信单元 1303 和处理单元 1302。

比如，以通信装置 1300 为上述方法实施例图中 5、图 10 或图 12 的终端设备为例，则处理单元 1302 用于获取目标密钥。其中，目标密钥包括以下密钥中的至少一个：目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥。第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。通信单元 1303 用于接收来自多播用户面处理网元的目标数据。其中，目标数据是经过安全保护后的数据。处理单元 1302 还用于采用目标密钥对目标数据进行处理。这里，多播用户面处理网元为以下网元中的一种：MBSU 网元、UPF 网元、UPGW、或 MSF 网元。

在一种可能的设计中，通信单元 1303 还用于接收来自第一网元的安全算法。其中，安全算法包括加密算法和完整性保护算法中的至少一种。处理单元 1302 具体用于：采用安全算法和目标密钥对目标数据进行处理。这里，第一网元是多播用户面处理网元或密钥生成网元。密钥生成网元为 AMF 网元、SMF 网元或 AUSF 网元。

在一种可能的设计中，通信单元 1303 还用于接收来自第一网元的安全保护状态信息。其中，安全保护状态信息指示安全保护状态，安全保护包括数据加密和完整性验证中的至少一种。处理单元 1302 具体用于：若安全保护状态信息指示的状态为开启，则采用目标密钥对目标数据进行处理。这里，第一网元是多播用户面处理网元或密钥生成网元。

在一种可能的设计中，通信单元 1303 还用于接收来自第一网元的目标密钥。处理单元 1302 具体用于：通过通信单元 1303 获取目标密钥。

在一种可能的设计中，处理单元 1302 还用于获取目标密钥的标识；处理单元 1302 具

体用于：获取与目标密钥的标识对应的目标密钥。

在一种可能的设计中，通信单元 1303 还用于接收来自第一网元的目标密钥的标识。处理单元 1302 具体用于：通过通信单元 1303 获取目标密钥的标识。或者，通信单元 1303 还用于接收来自第一网元的密钥序号部分。处理单元 1302 具体用于：根据密钥序号部分
5 和多播服务的标识 ID，确定目标密钥的标识。

在一种可能的设计中，通信单元 1303 还用于接收来自密钥生成网元的第一信息。其中，第一信息包括以下至少一项：多播用户面处理网元的标识，第一参数，或多播服务的 ID。这里，第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数。处理单元 1302 还用于根据第一信息和共享密钥，生成 MUK。其中，共享密钥是通信装置 1300 与核
10 心网设备之间共享的密钥。通信单元 1303 还用于接收来自多播用户面处理网元的密钥信息。其中，密钥信息是目标密钥经过 MUK 加密后的信息。处理单元 1302 具体用于：采用 MUK 解密密钥信息，以得到目标密钥。

在一种可能的设计中，处理单元 1302 具体用于：对目标 MSK 进行推演运算，以得到推演密钥，采用推演密钥对目标数据进行解密或完整性验证。

15 在一种可能的设计中，处理单元 1302 具体用于：对目标 MSK 和第二信息进行推演运算，以得到推演密钥，其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。这里，第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。

比如，以通信装置 1300 为上述方法实施例图中图 5、图 10 或图 12 的多播用户面处理网元为例，处理单元 1302 用于获取目标密钥。其中，目标密钥包括以下密钥中的至少一个：
20 目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥。第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。处理单元 1302 还用于采用目标密钥对多播业务数据进行安全保护，以得到目标数据。通信单元 1303 用于向终端设备发送目标数据。

在一种可能的设计中，处理单元 1302 具体用于：生成目标密钥。或者，通信单元 1303
25 还用于接收来自密钥生成网元的目标密钥。处理单元 1302 具体用于：通过通信单元 1303 获取目标密钥。

在一种可能的设计中，通信单元 1303 还用于向终端设备发送目标密钥。

在一种可能的设计中，通信单元 1303 还用于接收来自密钥生成网元的 MUK。处理单元 1302 还用于采用 MUK 加密目标密钥，以得到密钥信息。通信单元 1303 还用于向终端设备
30 发送密钥信息。

在一种可能的设计中，通信单元 1303 还用于向终端设备发送目标 MSK 的标识。或者，通信单元 1303 还用于向终端设备发送密钥序号部分。其中，密钥序号部分与目标 MSK 的标识具有映射关系。

在一种可能的设计中，处理单元 1302 还用于获取安全算法。其中，安全算法包括加
35 密算法和完整性保护算法中的至少一种。处理单元 1302 具体用于：采用安全算法和目标密钥对多播业务数据进行安全保护，以得到目标数据。

在一种可能的设计中，处理单元 1302 还用于确定安全保护状态信息。其中，安全保护状态信息指示安全保护状态，安全保护包括数据加密和完整性验证中的至少一种。处理单元 1302 具体用于：若安全保护状态信息指示的状态为开启，则采用目标密钥对多播业

务数据进行安全保护，以得到目标数据。

在一种可能的设计中，处理单元 1302 具体用于：对目标 MSK 进行推演运算，以得到推演密钥，采用推演密钥对多播业务数据进行安全保护，以得到目标数据。

在一种可能的设计中，处理单元 1302 具体用于：对目标 MSK 和第二信息进行推演运算，以得到推演密钥。其中，第二信息包括以下至少一项：协议名称、目标 MTK 的标识、或第二参数。这里，第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。

在一种可能的设计中，处理单元 1302 还用于根据传输协议类型、会话类型、服务质量 QoS 参数或网络类型中的至少一项，确定生成目标 MTK。其中，推演密钥包括目标 MTK。

比如，以通信装置 1300 为上述方法实施例图中图 5 的密钥生成网元为例，处理单元 1302 用于获取 MUK。通信单元 1303 用于向多播用户面处理网元发送 MUK。

在一种可能的设计中，处理单元 1302 还用于获取第一信息。其中，第一信息包括以下至少一项：多播用户面处理网元的标识，第一参数，或多播服务的标识 ID。这里，第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数。处理单元 1302 具体用于：根据第一信息和共享密钥，生成 MUK。其中，共享密钥是终端设备与核心网设备之间共享的密钥。

在一种可能的设计中，通信单元 1303 还用于向终端设备发送第一信息。

在一种可能的设计中，处理单元 1302 还用于确定目标安全策略。其中，目标安全策略包括机密性保护策略和完整性保护策略中的至少一种。通信单元 1303 还用于向多播用户面处理网元发送目标安全策略。

在一种可能的设计中，处理单元 1302 具体用于：根据目标 MTK 的传输状况和基础策略，确定目标安全策略。其中，基础策略包括多播上下文中的多播安全策略或 UDM 签约数据中的用户面安全策略。

在一种可能的设计中，处理单元 1302 还用于确定安全算法。其中，安全算法用于安全保护的计算，安全保护由目标安全策略指示。通信单元 1303 还用于向多播用户面处理网元发送安全算法。

在一种可能的设计中，通信单元 1303 还用于向终端设备发送目标安全策略和安全算法中的至少一项。其中，安全算法用于安全保护的计算，安全保护由目标安全策略指示。

比如，以通信装置 1300 为上述方法实施例图中图 12 的密钥生成网元为例，处理单元 1302 用于获取目标密钥。其中，目标密钥包括以下密钥中的至少一个：目标 MSK，目标 MSK 对应的第一子密钥，或目标 MSK 对应的第二子密钥，第一子密钥用于机密性保护计算，第二子密钥用于完整性保护计算。通信单元 1303 还用于向多播用户面处理网元发送目标密钥。

在一种可能的设计中，通信单元 1303 还用于向多播用户面处理网元发送目标密钥的标识。或者，通信单元 1303 还用于向多播用户面处理网元发送密钥序号部分。其中，密钥序号部分与目标密钥的标识具有映射关系。

在一种可能的设计中，通信单元 1303 还用于向终端设备发送密钥序号部分、目标密钥和目标密钥的标识中的至少一项。其中，密钥序号部分与目标密钥的标识具有映射关系。

比如，以通信装置 1300 为上述方法实施例图中图 5 的 AUSF 网元为例，通信单元 1303 用于接收来自密钥生成网元的第一信息和终端设备的 SUPI。其中，第一信息包括以下至少一项：多播用户面处理网元的标识，第一参数，或多播服务的标识 ID。这里，第一参数是

基于第一序列号和第一时间戳中的至少一项确定的参数。处理单元 1302 用于根据第一信息和 SUPI，生成 MUK。通信单元 1303 还用于向密钥生成网元发送 MUK。

在一种可能的设计中，处理单元 1302 具体用于：根据 SUPI，确定共享密钥，其中，共享密钥是终端设备与核心网设备之间共享的密钥，根据共享密钥和第一信息，生成 MUK。

5 其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。

可选的，通信装置 1300 还包括存储单元 1301，用于存储通信装置 1300 的程序代码和数据，数据可以包括不限于原始数据或者中间数据等。

其中，处理单元 1302 可以是处理器或控制器，例如可以是中央处理单元（central processing unit, CPU），通用处理器，数字信号处理器（digital signal processor, DSP），专用集成电路（application specific integrated circuit, ASIC），现成可编程门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。

通信单元 1303 可以是通信接口、收发器或收发电路等，其中，该通信接口是统称，在具体实现中，该通信接口可以包括多个接口，例如可以包括：第一接入网设备和第二接入网设备之间的接口和/或其他接口。

存储单元 1301 可以是存储器。

20 当处理单元 1302 为处理器，通信单元 1303 为通信接口，存储单元 1301 为存储器时，本申请实施例所涉及的通信装置 1400 可以为图 14 所示。

参阅图 14 所示，该通信装置 1400 包括：处理器 1402、收发器 1403、存储器 1401。

其中，收发器 1403 可以为独立设置的发送器，该发送器可用于向其他设备发送信息，该收发器也可以为独立设置的接收器，用于从其他设备接收信息。该收发器也可以是将发送、接收信息功能集成在一起的部件，本申请实施例对收发器的具体实现不做限制。

25 可选的，通信装置 1400 还可以包括总线 1404。其中，收发器 1403、处理器 1402 以及存储器 1401 可以通过总线 1404 相互连接；总线 1404 可以是外设部件互连标准（peripheral component interconnect, PCI）总线或扩展工业标准结构（extended industry standard architecture, EISA）总线等。所述总线 1404 可以分为地址总线、数据总线、控制总线等。为便于表示，图 14 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本领域普通技术人员可以理解：在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line, DSL））或无线

(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包括一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质, (例如, 软盘、硬盘、磁带)、光介质(例如, 数字视频光盘(digital video disc, DVD))、或者半导体介质(例如固态硬盘(solid state disk, SSD))等。

在本申请所提供的几个实施例中, 应该理解到, 所揭露的系统, 装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 所述单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个系统, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络设备上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外, 在本申请各个实施例中的各功能单元可以集成在一个处理单元中, 也可以是各个功能单元独立存在, 也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用硬件加软件功能单元的形式实现。

通过以上的实施方式的描述, 所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现, 当然也可以通过硬件, 但很多情况下前者是更佳的实施方式。基于这样的理解, 本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来, 该计算机软件产品存储在可读取的存储介质中, 如计算机的软盘, 硬盘或光盘等, 包括若干指令用以使得一台计算机设备(可以是个人计算机, 服务器, 或者网络设备等等)执行本申请各个实施例所述的方法。

以上所述, 仅为本申请的具体实施方式, 但本申请的保护范围并不局限于此, 在本申请揭露的技术范围内的变化或替换, 都应涵盖在本申请的保护范围之内。因此, 本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种密钥管理方法，其特征在于，包括：

终端设备获取目标密钥，其中，所述目标密钥包括以下密钥中的至少一个：目标多媒体广播多播业务业务密钥 MSK，所述目标 MSK 对应的第一子密钥，或所述目标 MSK 对应的第二子密钥；所述第一子密钥用于机密性保护计算；所述第二子密钥用于完整性保护计算；

所述终端设备接收来自多播用户面处理网元的目标数据，其中，所述目标数据是经过安全保护后的数据；

所述终端设备采用所述目标密钥对所述目标数据进行处理。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述终端设备接收来自第一网元的安全算法，其中，所述安全算法包括加密算法和完整性保护算法中的至少一种；

所述终端设备采用所述目标密钥对所述目标数据进行处理，包括：

所述终端设备采用所述安全算法和所述目标密钥对所述目标数据进行处理。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述方法还包括：

所述终端设备接收来自第一网元的安全保护状态信息，其中，所述安全保护状态信息指示安全保护状态，所述安全保护包括数据加密和完整性验证中的至少一种；

所述终端设备采用所述目标密钥对所述目标数据进行处理，包括：

若所述安全保护状态信息指示的状态为开启，则所述终端设备采用所述目标密钥对所述目标数据进行处理。

4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，

所述终端设备获取目标密钥，包括：

所述终端设备接收来自第一网元的所述目标密钥。

5、根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述方法还包括：

所述终端设备获取所述目标密钥的标识；

所述终端设备获取目标密钥，包括：

所述终端设备获取与所述目标密钥的标识对应的所述目标密钥。

6、根据权利要求 5 所述的方法，其特征在于，所述终端设备获取所述目标密钥的标识，包括：

所述终端设备接收来自第一网元的所述目标密钥的标识；

或者，所述终端设备接收来自第一网元的密钥序号部分；所述终端设备根据所述密钥序号部分和多播服务的标识 ID，确定所述目标密钥的标识。

7、根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述方法还包括：

所述终端设备接收来自密钥生成网元的第一信息，其中，所述第一信息包括以下至少一项：所述多播用户面处理网元的标识，第一参数，或多播服务的 ID；所述第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数；

所述终端设备根据所述第一信息和共享密钥，生成多媒体广播多播业务用户密钥 MUK，其中，所述共享密钥是所述终端设备与核心网设备之间共享的密钥；

所述终端设备获取目标密钥，包括：

所述终端设备接收来自所述多播用户面处理网元的密钥信息，其中，所述密钥信息是

所述目标密钥经过所述 MUK 加密后的信息；

所述终端设备采用所述 MUK 解密所述密钥信息，以得到所述目标密钥。

8、根据权利要求 7 所述的方法，其特征在于，

所述共享密钥为认证服务器功能密钥 Kausf 或安全锚点功能密钥 Kseaf。

- 5 9、根据权利要求 1 至 8 任一项所述的方法，其特征在于，所述终端设备采用所述目标密钥对所述目标数据进行处理，包括：

所述终端设备对所述目标 MSK 进行推演运算，以得到推演密钥；

所述终端设备采用所述推演密钥对所述目标数据进行解密或完整性验证。

- 10 10、根据权利要求 9 所述的方法，其特征在于，所述终端设备对所述目标 MSK 进行推演运算，以得到推演密钥，包括：

所述终端设备对所述目标 MSK 和第二信息进行推演运算，以得到所述推演密钥，其中，所述第二信息包括以下至少一项：协议名称、目标多媒体广播多播业务传输密钥 MTK 的标识、或第二参数；所述第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。

11、一种密钥管理方法，其特征在于，包括：

- 15 多播用户面处理网元获取目标密钥，其中，所述目标密钥包括以下密钥中的至少一个：目标多媒体广播多播业务业务密钥 MSK，所述目标 MSK 对应的第一子密钥，或所述目标 MSK 对应的第二子密钥；所述第一子密钥用于机密性保护计算；所述第二子密钥用于完整性保护计算；

- 20 所述多播用户面处理网元采用所述目标密钥对多播业务数据进行安全保护，以得到目标数据；

所述多播用户面处理网元向终端设备发送所述目标数据。

12、根据权利要求 11 所述的方法，其特征在于，所述多播用户面处理网元获取目标密钥，包括：

所述多播用户面处理网元生成所述目标密钥；

- 25 或者，所述多播用户面处理网元接收来自密钥生成网元的所述目标密钥。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述方法还包括：

所述多播用户面处理网元向所述终端设备发送所述目标密钥。

14、根据权利要求 11 或 12 所述的方法，其特征在于，所述方法还包括：

- 30 所述多播用户面处理网元接收来自密钥生成网元的多媒体广播多播业务用户密钥 MUK；
所述多播用户面处理网元采用所述 MUK 加密所述目标密钥，以得到密钥信息；
所述多播用户面处理网元向所述终端设备发送所述密钥信息。

15、根据权利要求 11 至 14 任一项所述的方法，其特征在于，所述方法还包括：

所述多播用户面处理网元向所述终端设备发送所述目标 MSK 的标识；

- 35 或者，所述多播用户面处理网元向所述终端设备发送密钥序号部分，其中，所述密钥序号部分与所述目标 MSK 的标识具有映射关系。

16、根据权利要求 11 至 15 任一项所述的方法，其特征在于，所述方法还包括：

所述多播用户面处理网元获取安全算法，其中，所述安全算法包括加密算法和完整性保护算法中的至少一种；

所述多播用户面处理网元采用所述目标密钥对多播业务数据进行安全保护，以得到目

标数据, 包括:

所述多播用户面处理网元采用所述安全算法和所述目标密钥对所述多播业务数据进行安全保护, 以得到所述目标数据。

17、根据权利要求 11 至 16 任一项所述的方法, 其特征在于, 所述方法还包括:

- 5 所述多播用户面处理网元确定安全保护状态信息, 其中, 所述安全保护状态信息指示安全保护状态, 所述安全保护包括数据加密和完整性验证中的至少一种;

所述多播用户面处理网元采用所述目标密钥对多播业务数据进行安全保护, 以得到目标数据, 包括:

- 10 若所述安全保护状态信息指示的状态为开启, 则所述多播用户面处理网元采用所述目标密钥对所述多播业务数据进行安全保护, 以得到所述目标数据。

18、根据权利要求 11 至 17 任一项所述的方法, 其特征在于, 所述多播用户面处理网元采用所述目标密钥对多播业务数据进行安全保护, 以得到目标数据, 包括:

所述多播用户面处理网元对所述目标 MSK 进行推演运算, 以得到推演密钥;

- 15 所述多播用户面处理网元采用所述推演密钥对所述多播业务数据进行安全保护, 以得到所述目标数据。

19、根据权利要求 18 所述的方法, 其特征在于, 所述多播用户面处理网元对所述目标 MSK 进行推演运算, 以得到推演密钥, 包括:

- 20 所述多播用户面处理网元对所述目标 MSK 和第二信息进行推演运算, 以得到所述推演密钥, 其中, 所述第二信息包括以下至少一项: 协议名称、目标多媒体广播多播业务传输密钥 MTK 的标识、或第二参数; 所述第二参数是基于第二序列号和第二时间戳中的至少一项确定的参数。

20、根据权利要求 19 所述的方法, 其特征在于, 所述方法还包括:

所述多播用户面处理网元根据传输协议类型、会话类型、服务质量 QoS 参数或网络类型中的至少一项, 确定生成所述目标 MTK, 其中, 所述推演密钥包括所述目标 MTK。

- 25 21、一种密钥管理方法, 其特征在于, 包括:

密钥生成网元获取多媒体广播多播业务用户密钥 MUK;

所述密钥生成网元向多播用户面处理网元发送所述 MUK。

22、根据权利要求 21 所述的方法, 其特征在于, 所述方法还包括:

- 30 所述密钥生成网元获取第一信息, 其中, 所述第一信息包括以下至少一项: 所述多播用户面处理网元的标识, 第一参数, 或多播服务的标识 ID; 所述第一参数是基于第一序列号和第一时间戳中的至少一项确定的参数;

所述密钥生成网元获取 MUK, 包括:

所述密钥生成网元根据所述第一信息和共享密钥, 生成所述 MUK, 其中, 所述共享密钥是终端设备与核心网设备之间共享的密钥;

- 35 或者, 所述密钥生成网元向认证服务器功能 AUSF 网元发送所述第一信息和所述终端设备的用户永久标识 SUPI; 所述密钥生成网元接收来自所述 AUSF 网元的所述 MUK; 其中, 所述 MUK 是基于所述第一信息和所述 SUPI 生成的。

23、根据权利要求 22 所述的方法, 其特征在于, 所述方法还包括:

所述密钥生成网元向所述终端设备发送所述所述第一信息。

24、根据权利要求 22 或 23 所述的方法，其特征在于，

所述共享密钥为认证服务器功能密钥 **Kausf**、安全锚点功能密钥 **Kseaf** 或由所述 **Kausf** 推演的密钥。

25、一种密钥管理方法，其特征在于，包括：

- 5 密钥生成网元获取目标密钥，其中，所述目标密钥包括以下密钥中的至少一个：目标多媒体广播多播业务业务密钥 **MSK**，所述目标 **MSK** 对应的第一子密钥，或所述目标 **MSK** 对应的第二子密钥；所述第一子密钥用于机密性保护计算；所述第二子密钥用于完整性保护计算；

所述密钥生成网元向多播用户面处理网元发送所述目标密钥。

- 10 26、根据权利要求 25 所述的方法，其特征在于，所述方法还包括：

所述密钥生成网元向所述多播用户面处理网元发送所述目标密钥的标识；

或者，所述密钥生成网元向所述多播用户面处理网元发送密钥序号部分，其中，所述密钥序号部分与所述目标密钥的标识具有映射关系。

27、根据权利要求 25 或 26 所述的方法，其特征在于，所述方法还包括：

- 15 所述密钥生成网元向终端设备发送密钥序号部分、所述目标密钥和所述目标密钥的标识中的至少一项，其中，所述密钥序号部分与所述目标密钥的标识具有映射关系。

28、一种密钥管理方法，其特征在于，包括：

密钥生成网元确定目标安全策略，其中，所述目标安全策略包括机密性保护策略和完整性保护策略中的至少一种；

- 20 所述密钥生成网元向多播用户面处理网元发送所述目标安全策略。

29、根据权利要求 28 所述的方法，其特征在于，

所述密钥生成网元确定目标安全策略，包括：

所述密钥生成网元根据目标多媒体广播多播业务传输密钥 **MTK** 的传输状况和基础策略，确定所述目标安全策略，其中，所述基础策略包括多播上下文中的多播安全策略或统一数

- 25 据管理 **UDM** 签约数据中的用户面安全策略。

30、根据权利要求 28 或 29 所述的方法，其特征在于，所述方法还包括：

所述密钥生成网元确定所述目标安全策略对应的安全算法，其中，所述安全算法用于数据安全保护计算；

所述密钥生成网元向所述多播用户面处理网元发送所述安全算法。

- 30 31、根据权利要求 28 至 30 任一项所述的方法，其特征在于，所述方法还包括：

所述密钥生成网元向终端设备发送所述目标安全策略和安全算法中的至少一项，其中，所述安全算法与所述目标安全策略对应。

32、一种通信装置，其特征在于，包括：用于执行权利要求 1 至 10 任一项所述的各个步骤的单元。

- 35 33、一种通信装置，其特征在于，包括：处理器，用于调用存储器中的程序，以使得所述通信装置执行权利要求 1 至 10 任一项所述的密钥管理方法。

34、一种通信装置，其特征在于，包括：处理器和接口电路，所述接口电路用于与其它装置通信，所述处理器用于执行权利要求 1 至 10 任一项所述的密钥管理方法。

35、一种通信装置，其特征在于，包括：用于执行权利要求 11 至 20 任一项所述

的各个步骤的单元。

36、一种通信装置，其特征在于，包括：处理器，用于调用存储器中的程序，以使得所述通信装置执行权利要求 11 至 20 任一项所述的密钥管理方法。

5 37、一种通信装置，其特征在于，包括：处理器和接口电路，所述接口电路用于与其它装置通信，所述处理器用于执行权利要求 11 至 20 任一项所述的密钥管理方法。

38、一种通信装置，其特征在于，包括：用于执行权利要求 21 至 24 任一项所述的各个步骤的单元，或用于执行权利要求 25 至 27 任一项所述的各个步骤的单元，或用于执行权利要求 28 至 31 任一项所述的各个步骤的单元。

10 39、一种通信装置，其特征在于，包括：处理器，用于调用存储器中的程序，以使得所述通信装置执行权利要求 21 至 24 任一项所述的密钥管理方法，或执行权利要求 25 至 27 任一项所述的密钥管理方法，或执行权利要求 28 至 31 任一项所述的密钥管理方法。

15 40、一种通信装置，其特征在于，包括：处理器和接口电路，所述接口电路用于与其它装置通信，所述处理器用于执行权利要求 21 至 24 任一项所述的密钥管理方法，或执行权利要求 25 至 27 任一项所述的密钥管理方法，或执行权利要求 28 至 31 任一项所述的密钥管理方法。

20 41、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储程序，所述程序被处理器调用时，权利要求 1 至 10 任一项所述的密钥管理方法被执行，或者权利要求 11 至 20 任一项所述的密钥管理方法被执行，或者权利要求 21 至 24 任一项所述的密钥管理方法被执行，或者权利要求 25 至 27 任一项所述的密钥管理方法被执行，或者权利要求 28 至 31 任一项所述的密钥管理方法被执行。

25 42、一种计算机程序，其特征在于，当所述程序被处理器调用时，权利要求 1 至 10 任一项所述的密钥管理方法被执行，或者权利要求 11 至 20 任一项所述的密钥管理方法被执行，或者权利要求 21 至 24 任一项所述的密钥管理方法被执行，或者权利要求 25 至 27 任一项所述的密钥管理方法被执行，或者权利要求 28 至 31 任一项所述的密钥管理方法被执行。

30

35