

说明书

发明名称: 通信方法和装置

[0001] 相关申请的交叉引用

[0002] 本申请要求在2022年05月06日提交中国专利局、申请号为202210488548.X、申请名称为“通信方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0003] 本申请涉及通信技术领域，尤其涉及一种通信方法和装置。

背景技术

[0004] 为了多播通信的安全，网络侧通常会在多播通信之前向终端设备分发多播密钥，以对业务数据进行安全保护。目前，网络侧可以通过多种不同的多播密钥传输流程向用户设备(user equipment, UE)发送多播密钥，如会话管理功能(session management function, SMF)网元与UE之间的信令面通信流程、多播/广播服务传输功能(multicast/broadcast service transport function, MBSTF)和UE之间基于应用认证与密钥管理(authentication and key management for applications, AKMA)的用户面通信流程以及MBSTF和UE之间基于通用引导构架(generic bootstrapping architecture, GBA)的用户面通信流程等，而根据第三代合作伙伴计划(3rd Generation Partnership Project, 3GPP)标准规范，这些流程对网络侧和UE而言都不是必须支持的。如何在这样多种可选流程并存的情况下，降低UE无法获取业务数据的可能性是当前需要考虑的问题。

[0005] 发明内容

[0006] 本申请提供了一种通信方法和装置，可以提高终端设备获取业务数据的可能性。

[0007] 第一方面，提供了一种通信方法，该方法可以由终端设备执行，或者，也可以由终端设备的组成部件(例如芯片或者电路)执行，对此不作限定。为了便于描述，下面以由终端设备执行为例进行说明。

- [0008] 该通信方法包括：终端设备获取第一指示信息，该第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向该终端设备传输多播密钥的通信流程，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [0009] 基于上述方案，一方面，终端设备可以基于自身对网络侧支持的至少一种多播密钥传输流程的支持情况从核心网获取业务数据，其中，从核心网获取业务数据的会话路径是基于该支持情况确定的，从而避免了终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的的数据进行解安全保护)的情况，可以提高用户体验；另一方面，本申请实施例提供的方案由终端设备自行判断自身对网络侧所支持的至少一种多播密钥传输流程的支持情况，从而无需让网络侧来判断或决策采用哪种多播密钥传输流程向终端设备分发多播密钥，从而可以降低网络侧的开销。
- [0010] 结合第一方面，在第一方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据，包括：该终端设备确定该终端设备支持该至少一种多播密钥传输流程中的目标多播密钥传输流程；该终端设备通过该目标多播密钥传输流程获取该多播密钥；该终端设备基于该多播密钥从该第一内容分发网元获取该业务数据。
- [0011] 在上述方案中，在终端设备支持至少一种为网络侧支持的多播密钥传输流程中的目标多播密钥传输流程的情况下，终端设备可以通过该目标多播密钥传输流程获取多播密钥，从而可以使得终端设备利用该多播密钥获取业务数据。同时由终端侧执行判断，还可以降低网络侧的开销。
- [0012] 结合第一方面，在第一方面的某些实现方式中，该终端设备基于该多播密钥从该第一内容分发网元获取该业务数据，包括：该终端设备使用该多播密钥对通过该多播会话从该第一内容分发网元接收的安全保护的的数据解安全保护，得到该业务数据。

- [0013] 可以理解的是，这里的第一内容分发网元可以是多播用户面功能网元。也就是说，终端设备获取了多播密钥之后，可以根据该多播密钥，通过多播会话获取业务数据。
- [0014] 结合第一方面，在第一方面的某些实现方式中，该目标多播密钥传输流程为会话管理网元和该终端设备之间的信令面通信流程，该终端设备通过该目标多播密钥传输流程获取该多播密钥，包括：该终端设备从来自该会话管理网元的多播会话加入响应消息获取该多播密钥；或者，该目标多播密钥传输流程为多播服务网元和该终端设备之间基于应用认证与密钥管理的用户面通信流程，该终端设备通过该目标多播密钥传输流程获取该多播密钥，包括：该终端设备基于通过认证与密钥管理机制生成的应用密钥，从来自该多播服务网元的多媒体因特网密钥管理消息获取该多播密钥；或者，该目标多播密钥传输流程为多播服务网元和该终端设备之间基于通用引导架构的用户面通信流程，该终端设备通过该目标多播密钥传输流程获取该多播密钥，包括：该终端设备基于通过通用引导架构机制生成的应用密钥，从来自该多播服务网元的多媒体因特网密钥管理消息获取该多播密钥。
- [0015] 结合第一方面，在第一方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从网络侧获取业务数据，包括：该终端设备确定该终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程；该终端设备通过单播会话从第二内容分发网元接收该业务数据。
- [0016] 在上述方案中，终端设备确定不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，确定通过单播会话获取业务数据，从而避免了终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验。
- [0017] 结合第一方面，在第一方面的某些实现方式中，该第二内容分发网元为用户面功能网元。
- [0018] 结合第一方面，在第一方面的某些实现方式中，该终端设备已加入该多播会话，该方法还包括：该终端设备向会话管理网元请求离开该多播会话。

- [0019] 在上述方案中，终端设备确定不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，离开已加入的多播会话，防止网络侧通过多播会话向终端设备发送业务数据，从而可以避免终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，提高用户体验。
- [0020] 结合第一方面，在第一方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从网络侧获取业务数据，包括：该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况选择用于从核心网获取业务数据的会话。
- [0021] 结合第一方面，在第一方面的某些实现方式中，该第一内容分发网元为多播用户面功能网元，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况选择用于从核心网获取业务数据的会话，包括：该终端设备确定该终端设备支持该至少一种多播密钥传输流程中的目标多播密钥传输流程；该终端设备选择该终端设备与该第一内容分发网元之间的多播会话作为用于获取该业务数据的会话。
- [0022] 结合第一方面，在第一方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况选择用于从核心网获取业务数据的会话，包括：该终端设备确定该终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程；该终端设备选择该终端设备与第二内容分发网元之间的单播会话作为用于获取该业务数据的会话。
- [0023] 结合第一方面，在第一方面的某些实现方式中，该终端设备获取指示信息，包括：该终端设备从来自多播服务功能网元的第一消息中获取该指示信息。
- [0024] 结合第一方面，在第一方面的某些实现方式中，该第一消息为服务宣告消息。
- [0025] 结合第一方面，在第一方面的某些实现方式中，该终端设备获取指示信息，包括：该终端设备从来自接入网设备的第二消息中获取该指示信息。
- [0026] 结合第一方面，在第一方面的某些实现方式中，该第二消息为系统消息。
- [0027] 结合第一方面，在第一方面的某些实现方式中，该终端设备获取指示信息，包括：该终端设备从来自应用功能网元的第三消息中获取该指示信息。

- [0028] 结合第一方面，在第一方面的某些实现方式中，该终端设备获取指示信息，包括：该终端设备从来自会话管理网元的第四消息中获取该指示信息。
- [0029] 结合第一方面，在第一方面的某些实现方式中，该第四消息为多播会话加入响应消息。
- [0030] 结合第一方面，在第一方面的某些实现方式中，该至少一种多播密钥传输流程，包括以下一项或多项：会话管理网元与该终端设备之间的信令面通信流程，多播服务网元与该终端设备之间基于应用认证与密钥管理的用户面通信流程，以及多播服务网元与该终端设备之间基于通用引导架构的用户面通信流程。
- [0031] 结合第一方面，在第一方面的某些实现方式中，该单播会话为该终端与该用户面功能网元之间的数据连接会话，该方法还包括：该终端设备确定该单播会话建立完成；该终端设备向应用功能网元发送第二指示信息，该第二指示信息指示该单播会话建立成功。
- [0032] 结合第一方面，在第一方面的某些实现方式中，该方法还包括：该终端设备确定该多播会话建立完成；该终端设备向应用功能网元发送第三指示信息，该第三指示信息指示该多播会话建立成功。
- [0033] 第二方面，提供了一种通信方法，该方法可以由网络设备执行，或者，也可以由网络设备的组成部件(例如芯片或者电路)执行，对此不作限定。为了便于描述，下面以由网络设备执行为例进行说明。
- [0034] 该通信方法包括：网络设备确定第一指示信息，该第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向终端设备传输多播密钥的通信流程，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；该网络设备向该终端设备发送该第一指示信息。
- [0035] 基于上述方案，网络设备向终端设备指示为网络侧支持的至少一种多播密钥传输流程，以便终端设备可以根据自身对该一种或多种多播密钥传输流程的支持情况从核心网获取业务数据，其中，可以避免终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护的情况，可以提高用户体验；另一方面，本申请实施例提供

的方案中，网络设备将第一指示信息发送给终端设备，由终端设备自行判断自身对网络侧所支持的至少一种多播密钥传输流程的支持情况，从而无需让网络侧来判断或决策采用哪种多播密钥传输流程向终端设备分发多播密钥，从而可以降低网络侧的开销。

- [0036] 结合第二方面，在第二方面的某些实现方式中，该网络设备为多播服务网元，该网络设备向该终端设备发送该第一指示信息，包括：该多播服务网元向该终端设备发送第一消息，该第一消息包含该指示信息。
- [0037] 结合第二方面，在第二方面的某些实现方式中，该第一消息为服务宣告消息。
- [0038] 结合第二方面，在第二方面的某些实现方式中，该网络设备为接入网设备，该网络设备向该终端设备发送该指示信息，包括：该接入网设备向该终端设备发送第二消息，该第二消息包含该指示信息。
- [0039] 结合第二方面，在第二方面的某些实现方式中，该第二消息为系统消息。
- [0040] 结合第二方面，在第二方面的某些实现方式中，该网络设备为应用功能网元，该网络设备向该终端设备发送该指示信息，包括：该应用功能网元向该终端设备发送第三消息，该第三消息包含该指示信息。
- [0041] 结合第二方面，在第二方面的某些实现方式中，该网络设备为会话管理网元，该网络设备向该终端设备发送该指示信息，包括：该会话管理网元向该终端设备发送第四消息，该第四消息包含该指示信息。
- [0042] 结合第二方面，在第二方面的某些实现方式中，该第四消息为多播会话加入响应消息。
- [0043] 结合第二方面，在第二方面的某些实现方式中，该至少一种多播密钥传输流程，包括以下一种或多种：会话管理网元与该终端设备之间的信令面通信流程，多播服务网元和该终端设备之间基于应用认证与密钥管理的用户面通信流程，以及多播服务网元和该终端设备之间基于通用引导架构的用户面通信流程。
- [0044] 第三方面，提供了一种通信方法，该方法可以由会话管理网元执行，或者，也可以由会话管理网元的组成部件(例如芯片或者电路)执行，对此不作限定。为了便于描述，下面以由会话管理网元执行为例进行说明。

- [0045] 该通信方法包括：会话管理网元接收来自终端设备的请求消息，该请求消息用于请求加入该终端设备与第一内容分发网元之间的多播会话；该会话管理网元确定该终端设备不支持至少一种为网络侧所支持的多播密钥传输流程中的所有多播密钥传输流程；该会话管理网元向该终端设备发送第三指示信息，该第三指示信息指示该会话管理网元拒绝该终端设备加入该多播会话或者指示该终端设备通过单播会话获取业务数据。
- [0046] 基于上述方法，会话管理网元可以在确定终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，拒绝终端设备加入多播会话，使得终端设备后续可以通过单播会话接收业务数据，从而可以避免由于终端设备无法获取网络侧下发的多播密钥，而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验。
- [0047] 结合第三方面，在第三方面的某些实现方式中，该第一内容分发网元为多播用户面功能网元。
- [0048] 第四方面，提供了一种通信方法，该方法可以由终端设备执行，或者，也可以由终端设备的组成部件(例如芯片或者电路)执行，对此不作限定。为了便于描述，下面以由终端设备执行为例进行说明。
- [0049] 该通信方法包括：终端设备向会话管理网元发送请求消息，该请求消息用于请求加入该终端设备与第一内容分发网元之间的多播会话；该终端设备接收来自该会话管理网元的第三指示信息，该第三指示信息指示该会话管理功能拒绝该终端设备加入该多播会话或者指示该终端设备通过单播会话获取业务数据；该终端设备根据该第三指示信息确定加入多播会话失败。
- [0050] 基于上述方案，会话管理网元可能拒绝终端设备加入多播会话，在这种情况下，终端设备确定加入多播会话失败，从而不通过多播会话接收业务数据，可以减少获取业务数据失败的情况，减少资源浪费。
- [0051] 结合第四方面，在第四方面的某些实现方式中，该方法还包括：该终端设备根据该第三指示信息选择通过该终端设备与第二内容分发网元之间的单播会话获取业务数据。

- [0052] 基于上述方案，会话管理网元拒绝了终端设备加入多播会话的情况下，终端设备可以确定通过单播会话获取业务数据，从而避免了终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验。
- [0053] 结合第四方面，在第四方面的某些实现方式中，该第一内容分发网元为多播用户面功能网元，该第二内容分发网元为用户面功能网元。
- [0054] 结合第四方面，在第四方面的某些实现方式中，该终端设备接收来自该会话管理网元的第三指示信息，包括：该终端设备接收来自该会话管理网元的该请求消息对应的响应消息，该响应消息包括该第三指示信息。
- [0055] 结合第四方面，在第四方面的某些实现方式中，该方法还包括：该终端设备向应用功能网元发送第四指示信息，该第四指示信息指示通过单播会话向该终端设备发送业务数据。
- [0056] 第五方面，提供了一种通信方法，该方法可以由终端设备执行，或者，也可以由终端设备的组成部件(例如芯片或者电路)执行，对此不作限定。为了便于描述，下面以由终端设备执行为例进行说明。
- [0057] 该通信方法包括：终端设备确定从网络侧获取多播密钥失败，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；该终端设备向会话管理网元请求离开该终端设备已加入的多播会话。
- [0058] 基于上述方法，一方面，终端设备确定获取多播密钥失败后，离开已加入的多播会话，从而可以避免由于终端设备无法获取网络侧下发的多播密钥，而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验；另一方面，本申请实施例提供的方案无需让网络侧来判断或决策采用哪种多播密钥传输流程向终端设备分发多播密钥，从而可以降低网络侧的开销。结合第五方面，在第五方面的某些实现方式中，该终端设备确定从网络侧获取多播密钥失败，包括：该终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败，该第一种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第一通信流程。

- [0059] 结合第五方面，在第五方面的某些实现方式中，该第一种多播密钥传输流程为会话管理网元与该终端设备之间的信令面通信流程，该终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败，包括：该终端设备向会话管理网元请求加入该多播会话；该终端设备接收来自该会话管理网元的响应消息；该终端设备确定从该响应消息中获取该多播密钥失败。
- [0060] 结合第五方面，在第五方面的某些实现方式中，该终端设备确定从网络侧获取多播密钥失败，还包括：该终端设备确定通过第二种多播密钥传输流程从网络侧获取多播密钥失败，该第二种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第二通信流程。
- [0061] 结合第五方面，在第五方面的某些实现方式中，该第二种多播密钥传输流程为多播服务网元与该终端设备之间的用户面通信流程，该终端设备确定通过第二种多播密钥传输流程从网络侧获取多播密钥失败，包括：该终端设备向该网络侧发起安全能力开放机制协商流程；该终端设备确定该安全能力开放机制协商失败；该终端设备根据该安全能力开放机制协商失败的结果确定从网络侧获取多播密钥失败。
- [0062] 结合第五方面，在第五方面的某些实现方式中，该第二种多播密钥传输流程为多播服务网元与该终端设备之间基于应用认证与密钥管理的用户面通信流程，该终端设备确定通过第二种多播密钥传输流程从网络侧获取多播密钥失败，包括：该终端设备基于应用认证与密钥管理机制向多播服务网元发起用户服务注册流程；该终端设备确定该用户服务注册流程失败；该终端设备根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败。
- [0063] 结合第五方面，在第五方面的某些实现方式中，该终端设备确定从网络侧获取多播密钥失败，还包括：该终端设备确定通过第三种多播密钥传输流程从网络侧获取多播密钥失败，该第三种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第三通信流程。
- [0064] 结合第五方面，在第五方面的某些实现方式中，该第三种多播密钥传输流程为多播服务网元与该终端设备之间基于通用引导架构的用户面通信流程，该终端设备确定通过第三种多播密钥传输流程从网络侧获取多播密钥失败，包括：该

终端设备基于通用引导架构机制向多播服务网元发起用户服务注册流程；该终端设备确定该用户服务注册流程失败；该终端设备根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败。

- [0065] 结合第五方面，在第五方面的某些实现方式中，该方法还包括：该终端设备选择通过单播会话从第二内容分发网元接收业务数据。
- [0066] 结合第五方面，在第五方面的某些实现方式中，该第二内容分发网元为用户面功能网元。
- [0067] 结合第五方面，在第五方面的某些实现方式中，该方法还包括：该终端设备向应用功能网元发送第四指示信息，该第四指示信息指示通过单播会话向该终端设备发送业务数据。
- [0068] 结合第五方面，在第五方面的某些实现方式中，该第一内容分发网元为多播用户面功能网元。
- [0069] 第六方面，提供通信装置，该装置用于执行上述第一方面至第五方面提供的任一方法。具体地，该装置可以包括用于执行第一方面至第五方面提供的方法的单元和/或模块，如处理模块和/或收发模块(也可以成为通信模块)。在一种实现方式中，该装置为网络设备，或者是网络设备中的芯片、芯片系统或电路，例如该装置为移动管理网元，或应用功能网元，或多播服务传输功能网元，或接入网设备。当该装置为网络设备时，通信模块可以是收发器，或，输入/输出接口；处理模块可以是处理器。
- [0070] 一种可能情况，该装置为终端设备或终端设备中的芯片、芯片系统或电路。在该情况下，该装置可以包括用于执行第一方面或第四方面中任一方面提供的方法的单元和/或模块，如处理模块和/或收发模块。
- [0071] 一种可能情况，该装置为网络设备或网络设备中的芯片、芯片系统或电路。在该情况下，该装置可以包括用于执行第二方面提供的方法的单元和/或模块，如处理单元和/或通信单元。
- [0072] 另一种可能情况，该装置为会话管理网元，或者会话管理网元中的芯片、芯片系统或电路。在该情况下，该装置可以包括用于执行第三方面或第五方面中任一方面提供的方法的单元和/或模块，如处理模块和/或收发模块。

- [0073] 可选地，上述收发器可以为收发电路。可选地，上述输入/输出接口可以为输入/输出电路。
- [0074] 可选地，上述收发器可以为收发电路。可选地，上述输入/输出接口可以为输入/输出电路。
- [0075] 第七方面，提供一种通信装置，该装置包括：存储器，用于存储程序；处理器，用于执行存储器存储的程序，当存储器存储的程序被执行时，处理器用于执行上述第一方面至第五方面提供的任一方法。
- [0076] 第八方面，本申请提供一种处理器，用于执行上述各方面提供的方法。在执行这些方法的过程中，上述方法中有关发送上述信息和获取/接收上述信息的过程，可以理解为由处理器输出上述信息的过程，以及处理器接收输入的上述信息的过程。在输出上述信息时，处理器将该上述信息输出给收发器，以便由收发器进行发射。该上述信息在由处理器输出之后，还可能需要进行其他的处理，然后再到达收发器。类似的，处理器接收输入的上述信息时，收发器获取/接收该上述信息，并将其输入处理器。更进一步的，在收发器收到该上述信息之后，该上述信息可能需要进行其他的处理，然后再输入处理器。
- [0077] 基于上述原理，举例来说，前述方法中提及的接收请求消息可以理解为处理器接收输入的信息。
- [0078] 对于处理器所涉及的发射、发送和获取/接收等操作，如果没有特殊说明，或者，如果未与其在相关描述中的实际作用或者内在逻辑相抵触，则均可以更加一般性的理解为处理器输出和接收、输入等操作，而不是直接由射频电路和天线所进行的发射、发送和接收操作。
- [0079] 在实现过程中，上述处理器可以是专门用于执行这些方法的处理器，也可以是执行存储器中的计算机指令来执行这些方法的处理器，例如通用处理器。上述存储器可以为非瞬时性(non-transitory)存储器，例如只读存储器(read only memory, ROM)，其可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型以及存储器与处理器的设置方式不做限定。

- [0080] 第九方面，提供一种计算机可读存储介质，该计算机可读介质存储用于设备执行的程序代码，该程序代码包括用于执行上述第一方面至第五方面提供的任一方法。
- [0081] 第十方面，提供一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行上述第一方面至第五方面提供的任一方法。
- [0082] 第十一方面，提供一种芯片，该芯片包括处理器与通信接口，该处理器通过该通信接口读取存储器上存储的指令，执行上述第一方面至第五方面提供的任一方法。
- [0083] 可选地，作为一种实现方式，该芯片还可以包括存储器，该存储器中存储有指令，该处理器用于执行该存储器上存储的指令，当该指令被执行时，该处理器用于执行上述第一方面至第五方面提供的任一方法。
- [0084] 第十二方面，提供了一种通信系统，该通信系统包括如第一方面所述的终端设备和如第二方面所述的网络设备。
- [0085] 第十三方面，提供了一种通信方法，该方法包括：网络设备确定第一指示信息，该第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向终端设备传输多播密钥的通信流程，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；该网络设备向该终端设备发送该第一指示信息；该终端设备接收来自该网络设备的该第一指示信息；该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [0086] 结合第十三方面，在第十三方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据，包括：该终端设备确定该终端设备支持该至少一种多播密钥传输流程中的目标多播密钥传输流程；该终端设备通过该目标多播密钥传输流程获取该多播密钥；该终端设备基于该多播密钥从该第一内容分发网元获取该业务数据。
- [0087] 结合第十三方面，在第十三方面的某些实现方式中，该终端设备基于该多播密钥从该第一内容分发网元获取该业务数据，包括：该终端设备使用该多播密钥

对通过该多播会话从该第一内容分发网元接收的安全保护的数据解安全保护，得到该业务数据。

[0088] 结合第十三方面，在第十三方面的某些实现方式中，该终端设备基于该终端设备对该至少一种多播密钥传输流程的支持情况从网络侧获取业务数据，包括：该终端设备确定该终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程；该终端设备通过单播会话从第二内容分发网元接收该业务数据。

[0089] 结合第十三方面，在第十三方面的某些实现方式中，该终端设备已加入该多播会话，该方法还包括：该终端设备向会话管理网元请求离开该多播会话。

附图说明

[0090] 图1和图2示出了本申请实施例适用的网络架构的示意图。

[0091] 图3示出了一种多播会话的配置过程示意图。

[0092] 图4是安全能力开放机制协商流程即用户服务注册流程示意图。

[0093] 图5A示出了本申请实施例提供的方法500的示意性流程图。

[0094] 图5B示出了本申请实施例提供的方法520的示意性流程图。

[0095] 图5C示出了本申请实施例提供的方法540的示意性流程图。

[0096] 图6示出了本申请实施例提供的方法600的示意性流程图。

[0097] 图7示出了本申请实施例提供的方法700的示意性流程图。

[0098] 图8示出了本申请实施例提供的方法800的示意性流程图。

[0099] 图9A示出了本申请实施例提供的方法900的示意性流程图。

[0100] 图9B和图9C示出了本申请实施例提供的两种逻辑判断流程图。

[0101] 图10示出了本申请实施例提供的方法1000的示意性流程图。

[0102] 图11是本申请一个实施例提供的通信装置的示意性框图。

[0103] 图12是本申请另一个实施例提供的通信装置的示意性框图。

[0104] 图13是本申请又一个实施例提供的通信装置的示意性框图。

具体实施方式

- [0105] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。
- [0106] 在本申请的各个实施例中，如果没有特殊说明以及逻辑冲突，不同的实施例之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。
- [0107] 可以理解的是，在本申请中涉及的各种数字编号仅为描述方便进行的区分，并不用来限制本申请的范围。上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定。
- [0108] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”以及其他各种术语标号等(如果存在)是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排除他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。
- [0109] 本申请提供的技术方案可以应用于各种通信系统，例如：第五代(5th generation, 5G)或新无线(new radio, NR)系统、长期演进(long term evolution, LTE)系统、LTE频分双工(frequency division duplex, FDD)系统、LTE时分双工(time division duplex, TDD)系统等。本申请提供的技术方案还可以应用于未来的通信系统，如第六代移动通信系统。本申请提供的技术方案还可以应用于设备到设备(device to device, D2D)通信，车到万物(vehicle-to-everything, V2X)通信，机器到机器(machine to machine, M2M)通信，机器类型通信(machine type communication, MTC)，以及物联网(internet of things, IoT)通信系统或者其他通信系统。

[0110] 下面将结合图1举例说明本申请实施例适用的5G系统。应理解，本文中描述的5G系统仅是示例，不应对本申请构成任何限定。

[0111] 如图1所示，该网络架构例如是第三代合作伙伴计划(3rd Generation Partnership Project, 3GPP)协议TS23.501中定义的5G系统(the 5th generation system, 5GS)。该网络架构可以分为接入网(access network, AN)和核心网(core network, CN)两部分。其中，接入网可用于实现无线接入有关的功能，核心网主要包括以下几个关键逻辑网元：接入和移动性管理功能(access and mobility management function, AMF)、会话管理功能(session management function, SMF)、用户面功能(user plane function, UPF)、策略控制功能(policy control function, PCF)和统一数据管理(unified data management, UDM)等。

[0112] 下面对图1中示出的各网元进行简单介绍：

[0113] 1、UE：可以称为终端设备(terminal equipment)、终端装置、接入终端、用户单元、用户站、移动站、移动台(mobile station, MS)、移动终端(mobile terminal, MT)、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。终端设备可以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、车载设备等。目前，一些终端的举例可以为：手机(mobile phone)、平板电脑(pad)、带无线收发功能的电脑(如笔记本电脑、掌上电脑等)、移动互联网设备(mobile internet device, MID)、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、远程医疗(remote medical)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、智慧家庭(smart home)中的无线终端、蜂窝电话、无绳电话、会话启动协议(session initiation protocol, SIP)电话、无线本地环路(wireless local loop, WLL)站、个人数字助理(personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，5G网络中的终端设备或者未来演进的公用陆地移动通信网络(public land mobile network, PLMN)中的终端设备等。

- [0114] 此外，终端设备还可以是物联网(Internet of things, IoT)系统中的终端设备。IoT是未来信息技术发展的重要组成部分，其主要技术特点是将物品通过通信技术与网络连接，从而实现人机互连，物-物互连的智能化网络。IoT技术可以通过例如窄带(narrow band, NB)技术，做到海量连接，深度覆盖，终端省电。
- [0115] 此外，终端设备还可以包括智能打印机、火车探测器等，主要功能包括收集数据(部分终端设备)、接收网络设备的控制信息与下行数据，并发送电磁波，向网络设备传输上行数据。
- [0116] 应理解，用户设备可以是任何可以接入网络的设备。终端设备与接入网设备之间可以采用某种空口技术相互通信。
- [0117] 可选地，用户设备可以用于充当基站。例如，用户设备可以充当调度实体，其在V2X或D2D等中的用户设备之间提供侧行链路信号。比如，蜂窝电话和汽车利用侧行链路信号彼此通信。蜂窝电话和智能家居设备之间通信，而无需通过基站中继通信信号。
- [0118] 2、(无线)接入网((radio)access network, (R)AN)设备：用于为特定区域的授权用户设备提供入网功能，并能够根据用户设备的级别，业务的需求等使用不同服务质量的传输隧道。
- [0119] (R)AN能够管理无线资源，为用户设备提供接入服务，进而完成控制信号和用户设备数据在用户设备和核心网之间的转发，(R)AN也可以理解为传统网络中的基站。
- [0120] 示例性地，本申请实施例中的接入网设备可以是用于与用户设备通信的任意一种具有无线收发功能的通信设备。该接入网设备包括但不限于为演进型节点B(evolved Node B, eNB)或5G，如，NR，系统中的gNB，或，传输点(TRP或TP)，5G系统中的基站的一个或一组(包括多个天线面板)天线面板，或者，还可以为构成gNB或传输点的网络节点，如基带单元(BBU)，或，分布式单元(distributed unit, DU)等。
- [0121] 在一些部署中，gNB可以包括集中式单元(centralized unit, CU)和DU。gNB还可以包括有源天线单元(active antenna unit, AAU)。CU实现gNB的部分功

能，DU实现gNB的部分功能。比如，CU负责处理非实时协议和服务，实现无线资源控制(radio resource control, RRC)，分组数据汇聚层协议(packet data convergence protocol, PDCP)层的功能。DU负责处理物理层协议和实时服务，实现无线链路控制(radio link control, RLC)层、媒体接入控制(media access control, MAC)层和物理(physical, PHY)层的功能。AAU实现部分物理层处理功能、射频处理及有源天线的相关功能。由于RRC层的信息最终会变成PHY层的信息，或者，由PHY层的信息转变而来，因而，在这种架构下，高层信令，如RRC层信令，也可以认为是由DU发送的，或者，由DU+AAU发送的。可以理解的是，接入网设备可以为包括CU节点、DU节点、AAU节点中一项或多项的设备。此外，可以将CU划分为接入网(radio access network, RAN)中的接入网设备，也可以将CU划分为核心网(core network, CN)中的接入网设备，本申请对此不做限定。

[0122] 3、用户面功能(user plane function, UPF)网元：用于分组路由和转发以及用户面数据的服务质量(quality of service, QoS)处理等。为叙述方便，本申请实施例中，用户面功能网元被简称为“UPF”。

[0123] 在未来通信系统中，用户面网元仍可以是UPF网元，或者，还可以有其它的名称，本申请不做限定。

[0124] 4、接入和移动管理功能(access and mobility management function, AMF)网元：接入和移动管理功能网元主要用于移动性管理和接入管理等，可以用于实现MME功能中除会话管理之外的其它功能，例如，接入授权/鉴权等功能。为叙述方便，本申请实施例中，接入和移动管理功能网元被简称为“AMF”。

[0125] 在未来通信系统中，接入和移动管理设备仍可以是AMF，或者，还可以有其它的名称，本申请不做限定。

[0126] 5、会话管理功能(session management function, SMF)网元：主要用于会话管理、用户设备的网络互连协议(internet protocol, IP)地址分配和管理、选择可管理用户平面功能、策略控制和收费功能接口的终结点以及下行数据通知等。为叙述方便，本申请实施例中，会话管理功能网元被简称为“SMF”。

- [0127] SMF为会话管理网元的一种。在未来通信系统中，会话管理网元仍可以是SMF，或者，还可以有其它的名称，本申请不做限定。
- [0128] 6、策略控制功能(policy control function, PCF)网元：用于指导网络行为的统一策略框架，为控制面功能网元(例如AMF，SMF等)提供策略规则信息等。
- [0129] 在未来通信系统中，策略控制网元仍可以是PCF网元，或者，还可以有其它的名称，本申请不做限定。
- [0130] 7、应用功能(application function, AF)网元：用于进行应用影响的数据路由，无线接入网络开放功能网元，与策略框架交互进行策略控制等。为叙述方便，本申请实施例中，应用功能网元被简称为“AF”。
- [0131] 在未来通信系统中，应用功能网元仍可以是AF网元，或者，还可以有其它的名称，本申请不做限定。
- [0132] 8、统一数据管理(unified data management, UDM)网元：用于处理UE标识，接入鉴权，注册以及移动性管理等。
- [0133] 在未来通信系统中，统一数据管理仍可以是UDM网元，或者，还可以有其它的名称，本申请不做限定。
- [0134] 9、认证服务器(authentication server function, AUSF)网元：用于鉴权服务、产生密钥实现对用户设备的双向鉴权，支持统一的鉴权框架。
- [0135] 在未来通信系统中，认证服务器功能网元仍可以是AUSF网元，或者，还可以有其它的名称，本申请不做限定。
- [0136] 10、网络数据分析功能(network data analytics function, NWDAF)网元：用于识别网络切片实例、加载网络切片实例的负载级别信息。网络数据分析功能可使NF消费者订阅或取消订阅定期通知，并在超过阈值的情况下，通知消费者。
- [0137] 在未来通信系统中，网络数据分析功能网元仍可以是NWDAF网元，或者，还可以有其它的名称，本申请不做限定。
- [0138] 11、数据网络(data network, DN)：DN是位于运营商网络之外的网络，运营商网络可以接入多个DN，DN上可部署多种业务，可为终端设备提供数据和/或语音等服务。例如，DN是某智能工厂的私有网络，智能工厂安装在车间的传感器可为终端设备，DN中部署了传感器的控制服务器，控制服务器可为传感器提供

服务。传感器可与控制服务器通信，获取控制服务器的指令，根据指令将采集的传感器数据传送给控制服务器等。又例如，DN是某公司的内部办公网络，该公司员工的手机或者电脑可为终端设备，员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。

[0139] 在图1所示的网络架构中，各网元之间可以通过图中所示的接口通信。如图所示，UE和AMF之间可以通过N1接口进行交互，交互消息例如可以称为N1消息(N1Message)。RAN和AMF之间可以通过N2接口进行交互，N2接口可以用于非接入层(non-access stratum, NAS)消息的发送等。RAN和UPF之间可以通过N3接口进行交互，N3接口可以用于传输用户面的数据等。SMF和UPF之间可以通过N4接口进行交互，N4接口可以用于传输例如N3连接的隧道标识信息，数据缓存指示信息，以及下行数据通知消息等信息。UPF和DN之间可以通过N6接口进行交互，N6接口可以用于传输用户面的数据等。其他接口与各网元之间的关系如图1中所示，为了简洁，这里不一一详述。下面简单介绍各个网元之间的接口名称及功能如下：

- [0140] 1)N7：PCF与SMF之间的接口，用于下发对应协议数据单元(protocol data unit, PDU)会话或者对应业务数据流的控制策略。
- [0141] 2)N15：PCF与AMF之间的接口，用于下发UE策略及接入控制相关策略。
- [0142] 3)N5：AF与PCF之间的接口，用于应用业务请求下发以及网络事件上报。
- [0143] 4)N4：SMF与UPF之间的接口，用于控制面与用户面之间传递信息，包括控制面向用户面的转发规则、QoS控制规则、流量统计规则等的下发以及用户面的信息上报。
- [0144] 5)N11：SMF与AMF之间的接口，用于传递RAN和UPF之间的PDU会话隧道信息、传递发送给UE的控制消息、传递发送给RAN的无线资源控制信息等。
- [0145] 6)N2：AMF与RAN之间的接口，用于传递核心网侧至RAN的无线承载控制信息等。
- [0146] 7)N1：AMF与UE之间的接口，接入无关，用于向UE传递QoS控制规则等。
- [0147] 8)N8：AMF与UDM间的接口，用于AMF向UDM获取接入与移动性管理相关签约数据与鉴权数据，以及AMF向UDM注册UE当前移动性管理相关信息等。

- [0148] 9)N10: SMF与UDM间的接口,用于SMF向UDM获取会话管理相关签约数据,以及SMF向UDM注册UE当前会话相关信息等。
- [0149] 10)N35: UDM与UDR间的接口,用于UDM从UDR中获取用户签约数据信息。
- [0150] 11)N36: PCF与UDR间的接口,用于PCF从UDR中获取策略相关签约数据以及应用数据相关信息。
- [0151] 12)N12: AMF和AUSF间的接口,用于AMF向AUSF发起鉴权流程,其中可携带SUCI作为签约标识;
- [0152] 13)N13: UDM和AUSF间的接口,用于AUSF向UDM获取用户鉴权向量,以执行鉴权流程。
- [0153] 图2是适用于本申请实施例提供的方法的多播广播业务架构的示意图。图2所示的多播广播业务架构和功能是在单播网络架构和功能的基础上增强而定义的。下面对图2中各个网元特定于多播广播业务的功能做简单介绍。
- [0154] 1、UE: UE主要功能为通过PTM/PTP接收多播数据、通过PTM接收组/广播数据、处理QoS、发起会话加入(session join)和会话离开(session leave)、以及5G MBS的终端侧的资源管理。
- [0155] 2、RAN: RAN主要负责处理MBS QoS流、通过点到多点(point to multipoint, PTM)、点到点(point to point, PTP)向UE发送数据、配置AS层接收广播流、在PTM和PTP之间切换、支持多播会话的Xn和N2切换、处理会话信令、以及建立空口广播和多播资源等。
- [0156] 3、AMF: AMF主要负责信令路由(NG-RAN ~ MB-SMF)、以及选择广播的NG-RANs等。
- [0157] 4、SMF: SMF为支持5G MBS特性,单播SMF需要增强,主要体现在增加:发现MB-SMF、UE加入的认证、与MB-SMF交互管理多播会话上下文、与RAN交互建立多播传输资源等功能。
- [0158] 5、UPF: UPF主要负责与MB-UPF交互接收通过单独传递模式传输的多播数据、通过PDU会话向UE传输单独传递模式传输的多播数据。

- [0159] 6、PCF：PCF主要负责多播广播业务(multicast and broadcast service, MBS)会话的QoS处理、向多播广播SMF(multicast and broadcast SMF, MB-SMF)提供策略信息、以及与用户数据存储库(user data repository, UDR)交互获取QoS信息等。PCF是可选网元, 仅在使用动态策略计费控制(policy charging control, PCC)时, 才需要该功能实体。
- [0160] 7、多播/广播会话管理功能(multicast/broadcast-session management function, MB-SMF)网元：MB-SMF是一个具备支持广播特性的实体。MB-SMF还可以同时具备单播SMF的功能。具体地, MB-SMF负责：MBS会话的管理, 包括QoS控制等；配置多播广播(multicast and broadcast UPF, MB-UPF)；与RAN交互控制广播流(flow)传输(广播会话特定功能)；与SMF交互关联协议数据单元(protocol data unit, PDU)会话；和RAN交互控制多播流的传输(多播会话特定功能)等。为叙述方便, 本申请实施例中, 多播/广播会话管理功能网元被简称为多播会话管理功能网元, 或“MB-SMF”。MB-SMF为多播会话管理网元中的一种, 在未来通信系统中, 多播会话管理网元仍可以是MB-SMF, 或者, 还可以有其它的名称, 本申请不做限定。
- [0161] 8、多播/广播用户面功能(multicast/broadcast-user plane function, MB-UPF)网元：MB-UPF是5G MBS的数据面的网关, 主要负责：与MB-SMF交互获取数据转发规则、向RAN通过共享传递方法(shared delivery method)传输多播数据；向UPF通过单独传递方法(individual delivery method)传输多播数据。为叙述方便, 本申请实施例中, 多播/广播用户面功能网元被简称为多播用户面功能网元或“MB-UPF”。
- [0162] 9、多播/广播服务功能(multicast and broadcast service function, MBSF)：MBSF主要支持以下功能：业务层功能、与LTE MBS的互通、与AF和MB-SMF交互以支持MBS会话的操作、确定传输参数和MBS会话的类型、选择MB-SMF控制MBSF、以及确定发送者的IP多播地址等。MBSF为可选网元。为叙述方便, 本申请实施例中, 多播/广播服务功能网元被简称为多播服务功能网元或“MBSF”。

- [0163] 10、多播/广播服务传输功能(multicast/broadcast service transport function, MBSTF): MBSTF主要支持以下功能: MBS数据的锚点、作为IP多播的源、支持例如帧、多流、前向纠错(forward error correction, FEC)等通用传输功能、将输入的文件作为目标(object)或目标流(object flow)以多播或广播的方式发送等。MBSTF为可选网元。为叙述方便, 本申请实施例中, 多播/广播服务传输功能网元被简称为多播服务传输功能网元或“MBSTF”。
- [0164] 11、AF: AF主要支持以下功能向5G核心网(5G core network, 5GC)提供业务信息并请求多播或广播服务、以及指示(instruct)与5GC的MBS会话操作等。
- [0165] 12、UDM: UDM主要支持多播会话的订阅/签约管理等。
- [0166] 13、NRF: NRF主要是核心网网元的信息, 在支持MBS特性上, 主要包括以下功能: 支持对服务MBS会话的MB-SMF的管理, 具体包括保存MB-SMF服务的MBS会话ID。
- [0167] 14、NEF: NEF在支持MBS特性上, 主要负责以下功能: 选择MB-SMF, 与AF以及MB-SMF交互实现MBS会话操作、确定传输参数等, 向AF提供5G MBS流程的接口如服务配置、MBS会话配置和QoS管理等接口。
- [0168] 图2中Nausf、Nnef、Npcf、Nudm、Naf、Namf、Nsmf、N1、N2、N3、N4, 以及N6为接口序列号。这些接口序列号的含义可参见3GPP标准协议中定义的含义, 在此不做限制。
- [0169] 应理解, 上述应用于本申请实施例的网络架构仅是举例说明的从传统点到点的架构和服务化架构的角度描述的网络架构, 适用本申请实施例的网络架构并不局限于此, 任何能够实现上述各个网元的功能的网络架构都适用于本申请实施例。
- [0170] 还应理解, 图1和图2中所示各个核心网网元可以理解为核心网中用于实现不同功能的网元, 例如可以按需组合成网络切片。这些核心网网元可以各自独立的设备, 也可以集成于同一设备中实现不同的功能, 本申请对于上述网元的具体形态不作限定。
- [0171] 还应理解, 上述命名仅为便于区分不同的功能而定义, 不应对本申请构成任何限定。本申请并不排除在5G网络以及未来其它的网络中采用其他命名的可能。

例如，在6G网络中，上述各个网元中的部分或全部可以沿用5G中的术语，也可能采用其他名称等。图1中的各个网元之间的接口名称只是一个示例，具体实现中接口的名称可能为其他的名称，本申请对此不作具体限定。此外，上述各个网元之间的所传输的消息(或信令)的名称也仅仅是一个示例，对消息本身的功能不构成任何限定。

[0172] 可以理解的是，上述网元或者功能既可以是硬件设备中的网络元件，也可以是在专用硬件上运行软件功能，或者是平台(例如，云平台)上实例化的虚拟化功能。为方便说明，本申请后续，以网络设备为接入和移动管理网元AMF，基站为无线接入网络RAN为例进行说明。

[0173] 本申请实施例描述的网络架构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，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。

[0174] 本申请实施例的各个方面或特征可以用于实现成方法，或者通过装置或标准编程和/或工程技术的制品进行实现。本申请中使用的术语“制品”涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。例如，计算机可读介质可以包括，但不限于：磁存储器件(例如，硬盘、软盘或磁带等)，光盘(例如，压缩盘(compact disc, CD)、数字通用盘(digital versatile disc, DVD)等)，智能卡和闪存器件(例如，可擦写可编程只读存储器(erasable programmable read-only memory, EPROM)、卡、棒或钥匙驱动器等)。另外，本文描述的各种存储介质可代表用于存储信息的一个或多个设备和/或其它机器可读介质。术语“机器可读介质”可包括但不限于，无线信道和能够存储、包含和/或承载指令和/或数据的各种其它介质。

[0175] 为了便于理解本申请实施例的技术方案，在以5G架构为基础介绍本申请实施例的方案之前，首先对本申请实施例可能涉及到的5G中的一些术语或概念，以及本申请可能涉及但上述网络架构未示出的网元进行简单描述。

[0176] 1、单播会话

[0177] 本申请实施例所述的单播会话，是指内容分发网元(即，负责分发业务数据的核心网网元)与单个UE之间的会话，内容分发网元通过该会话将内容(数据报文)分发/传输给该UE。

[0178] 示例性地，单播会话对应的内容分发网元可以是3GPP架构中的用户面功能网元(UPF)，相应地，单播会话可以是3GPP架构中的协议数据单元(protocol data unit, PDU)会话；可以理解的是，单播会话也可以是其他形式的、内容分发网元与单个UE之间的会话，本申请实施例在此不做限定。

[0179] 2、多播会话

[0180] 本申请实施例所述的多播会话，是指内容分发网元(即，负责分发业务数据的核心网网元)与多个UE之间的会话，内容分发网元通过该会话将同一内容(数据报文)分发/传输给该多个UE，接收同一多播会话传输的同一内容的这个UE可以属于一个业务、一个应用或一个群组。也就是说，一个多播会话的数据可以对应一个业务，一个应用或一个群组(例如紧急业务即按即说中的群组，车联网应用中的群组)，或者说，一个业务，一个应用或一个群组可以对应于一个多播会话。终端设备可以通过加入某多播会话，以接收内容分发网元通过该多播会话分发/传输的内容；示例性地，多播会话可以是组播会话，也可以是广播会话；组播会话为内容分发网元与一组UE之间的会话，内容分发网元通过该会话将同一内容(数据报文)分发/传输给该组UE；广播会话为内容分发网元与一个区域中所有UE之间的会话，内容分发网元通过该会话将同一内容(数据报文)分发/传输给该区域中所有UE；可以理解的是，多播会话还可以是其他形式的内容分发网元与多个UE之间的会话，本申请实施例不作限定。

[0181] 示例性地，多播会话对应的内容分发网元可以是3GPP架构中的多播用户面功能网元(MB-UPF)，或者是3GPP架构中的多播服务传输功能网元或多播服务功能网元，相应地，多播会话可以是3GPP架构中的MBS会话。为了便于区分，本申请实施例将多播会话对应的内容分发网元称为第一内容分发网元，将单播会话对应的内容分发网元称为第二内容分发网元。

[0182] 3、多播业务数据的传输

- [0183] 在3GPP网络中，用户服务/应用存在向多个用户设备(UE)发送相同数据的需求，即需要单点对多点的数据传输。该用户服务/应用包括多媒体消息服务、数据流服务、组通信服务等。
- [0184] 通过建立多播/广播/单播会话，网络提供一条被多个接收方共享的承载，发送方仅需发送一份数据，在网络侧按需将发送数据复制并传输至多个接收方或者使用多播的传输方式发送一份数据给多个接收方。
- [0185] 用户服务可以由一个或多个会话承载。对应性的，一个用户服务标识对应1个或多个MBS会话标识。
- [0186] 4、多播密钥
- [0187] 多播密钥为终端设备与多播用户面功能网元之间的多播会话的安全传输密钥，也就是说，该多播密钥用于对终端设备和内容分发网元之间的多播会话进行安全保护。该多播密钥还可以称为多播通信密钥、多播会话密钥等，本申请不作限定。
- [0188] 示例性地，多播密钥包括多播服务密钥(MBS Service Key, MSK)和多播传输密钥(MBS traffic key, MTK)，其中，MTK用于对业务数据进行安全保护，MSK用于对MTK进行安全保护。也就是说，上述“对终端设备和内容分发网元之间的多播会话进行安全保护”可以指的是利用MTK对业务数据进行安全保护，以及利用MSK对MTK进行安全保护。
- [0189] 可以理解的是，本申请实施例中的多播密钥，还可以表达为多播会话上下文，该多播会话上下文包括MSK、MTK，以及MSK、MTK对应的密钥标识符、密钥生命周期中的一个或多个。
- [0190] 5、多播密钥传输流程
- [0191] 多播密钥传输流程是网络侧用于向终端设备传输多播密钥的通信流程。可以理解的是，多播密钥传输流程不限于用于传输多播密钥，也就是说，多播密钥传输流程不一定是专门用来传输多播密钥的通信流程，例如，本申请实施例中的多播密钥传输流程可以是复用现有的通信流程来传输多播密钥的流程。
- [0192] 有多种多播密钥传输流程，包括但不限于：

- [0193] 第一种多播密钥传输流程是会话管理网元与终端设备之间的信令面(也叫“控制面”)通信流程(control-plane procedure),具体指的是多播服务网元通过用户信令面消息向终端设备传输多播密钥的通信流程;为叙述方便,本申请实施例将该通信流程称为“信令面多播密钥传输流程”,记为“C流程”;这里的多播服务网元例如可以是多播服务传输功能网元。
- [0194] 第二种多播密钥传输流程是指多播服务网元与终端设备之间基于应用认证与密钥管理的用户面通信流程(authentication and key management for applications-based user-plane procedure, AKMA-based user-plane procedure),具体指的是多播服务网元和终端设备基于应用认证与密钥管理生成的认证凭据建立的密钥传输安全通道,传输多播密钥的通信流程;为叙述方便,本申请实施例将其称为“第一种用户面多播密钥传输流程”,记为“U1流程”;
- [0195] 第三种多播密钥传输流程是多播服务网元与终端设备之间基于通用引导架构的用户面通信流程(generic bootstrapping architecture-based user-plane procedure, GBA-based user-plane procedure),具体指的是多播服务网元和终端设备基于通用引导架构生成的认证凭据建立的密钥传输安全通道,传输多播密钥的通信流程;为叙述方便,本申请实施例将其称为“第二种用户面多播密钥传输流程”,记为“U2流程”。
- [0196] 其中,第一种用户面多播密钥传输流程、第二种用户面多播密钥传输流程可以统称为用户面多播密钥传输流程(简称“用户面流程”, user-plane procedure)。换句话说,本申请实施例中的用户面多播密钥传输流程指的是第一种用户面多播密钥传输流程或第二种用户面多播密钥传输流程。
- [0197] 可以理解的是,本申请实施例中的多播密钥传输流程可以看成设备间交互消息的集合,包含与网络侧用于向终端设备传输多播密钥有关的一条或多条消息的交互过程。以图3中的方法300为例,C流程包括图3中的多播会话加入响应消息(S311),U1流程包括图3中的多媒体因特网密钥管理(multimedia internet keying, MIKEY)消息(S314)。但可以理解的是,在一种实现方式中,除了S311,C流程还可以包括其他消息,如图3中的MBS会话创建请求消息(S302)等,本申请不作限定;除了S314,U1流程或U2流程也可以包括其他消息,如安全能

力开放机制协商流程及用户服务注册流程中的消息(S313)，本申请不作限定。上述各条消息的含义可参考方法300部分的描述。

[0198] 本申请后续实施例中，会提及网络侧/终端设备支持/不支持某多播密钥传输流程，先作如下解释，后续将不再赘述。

[0199] 所谓网络侧支持C流程，是指网络侧的网元(如会话管理网元)能够通过C流程中的信令面消息(如S311中的响应消息)将多播密钥发送给终端设备，或者网络侧的网元(如会话管理网元)能够在终端设备加入多播会话的流程中将多播密钥发送给终端设备，或者网络侧的网元(如会话管理网元)能够通过非接入层消息(如S311中的响应消息)将多播密钥发送给终端设备；对应地，所谓网络侧不支持C流程，是指网络侧的网元(如会话管理网元)不能通过C流程中的信令面消息将多播密钥发送给终端设备，或者网络侧的网元不能在终端设备加入多播会话的流程中将多播密钥发送给终端设备，或者网络侧的网元不能通过非接入层消息将多播密钥发送给终端设备。所谓终端设备支持C流程，是指终端设备能够通过C流程中的信令面消息(如S311中的响应消息)获取多播密钥，或者终端设备能够在加入多播会话的流程中获取多播密钥，或者终端设备能够通过非接入层消息接收多播密钥；对应地，终端设备不支持C流程，表示终端设备不能通过信令面消息获取多播密钥，或者终端设备不能在加入多播会话的流程中获取多播密钥，或者终端设备不能通过非接入层消息接收多播密钥。

[0200] 所谓网络侧支持U1流程，是指网络侧的网元(如多播服务网元)能够通过U1流程将通过应用认证与密钥管理机制保护的多播密钥发送给终端设备，或者网络侧的网元能够通过用户面消息(如S314的MIKEY消息)将通过应用认证与密钥管理机制保护的多播密钥发送给终端设备，或者网络侧的网元(如多播服务网元)能够在终端设备的用户服务注册流程(如S313)完成之后将通过应用认证与密钥管理机制保护的多播密钥发送给终端设备，或者网络侧的网元(如多播服务网元)能够通过多媒体因特网密钥管理消息(如S314的MIKEY消息)将通过应用认证与密钥管理机制保护的多播密钥发送给终端设备。对应地，终端设备支持U1流程，是指终端设备能够通过U1流程获取通过应用认证与密钥管理机制保护的多播密钥，或者终端设备能够通过用户面消息(如S314的MIKEY消息)接收通过应用认证与密钥管

理机制保护的多播密钥，或者终端设备能够在用户服务注册流程(如S313)完成之后接收通过应用认证与密钥管理机制保护的多播密钥，或者终端设备能够通过多媒体因特网密钥管理消息(如S314的MIKEY消息)接收通过应用认证与密钥管理机制保护的多播密钥。

[0201] 所谓网络侧支持U2流程，是指网络侧的网元(如多播服务网元)能够通过U2流程将通过通用引导架构机制机制保护的多播密钥发送给终端设备，或者网络侧的网元能够通过用户面消息(如S314的MIKEY消息)将通过通用引导架构机制机制保护的多播密钥发送给终端设备，或者网络侧的网元(如多播服务网元)能够在终端设备的用户服务注册流程(如S313)完成之后将通过通用引导架构机制保护的多播密钥发送给终端设备，或者网络侧的网元(如多播服务网元)能够通过多媒体因特网密钥管理消息(如S314的MIKEY消息)将通过通用引导架构机制保护的多播密钥发送给终端设备。对应地，终端设备支持U2流程，是指终端设备能够通过U2流程获取通过通用引导架构机制保护的多播密钥，或者终端设备能够通过用户面消息(如S314的MIKEY消息)接收通过通用引导架构机制保护的多播密钥，或者终端设备能够在用户服务注册流程(如S313)完成之后接收通过通用引导架构机制保护的多播密钥，或者终端设备能够通过多媒体因特网密钥管理消息(如S314的MIKEY消息)接收通过通用引导架构机制保护的多播密钥。

[0202] 6、业务数据

[0203] 本申请中，业务数据是指服务提供者(如应用服务提供商)为提供服务而通过应用服务器发送给UE的数据。5G系统有多种发送业务数据的方式，例如，单播发送方式、多播发送方式。其中，单播发送方式是指应用服务器使业务数据通过PDU会话发送给UE；具体地，在该形式下，UE和应用服务器使用独立的IP地址，应用服务器将业务数据发送给UPF，由UPF处理后通过PDU会话的承载发送给UE。多播发送方式是指应用服务器使业务数据通过多播会话发送给UE；在该形式下，应用服务器发送1份数据包到MB-UPF，由MB-UPF处理后发送给UE，具体可以通过5GC单独的数据发送方式，也可以是5GC共享的数据发送方式，其中，所谓单独的数据发送方式是指MB-UPF触发与其级联的UPF通过

PDU会话向UE发送业务数据，所谓共享的数据发送方式是指MB-UPF通过多播会话向UE发送业务数据。

[0204] 上文结合图1和图2介绍了本申请实施例能够应用的示例性系统架构，还简单介绍了本申请中涉及的基本概念，下文中将结合附图详细介绍本申请提供的通信方法和装置。

[0205] 下文示出的实施例并未对本申请实施例提供的方法的执行主体的具体结构特别限定，只要能够通过运行记录有本申请实施例的提供的方法的代码的程序，以根据本申请实施例提供的方法进行通信即可，例如，本申请实施例提供的方法的执行主体可以是核心网设备和终端设备，或者是核心网设备或者终端设备中能够调用程序并执行程序的功能模块。

[0206] 为了便于理解本申请实施例，做出以下几点说明。

[0207] 第一，在本申请中，“用于指示”可以理解为“使能”，“使能”可以包括直接使能和间接使能。当描述某一信息用于使能A时，可以包括该信息直接使能A或间接使能A，而并不代表该信息中一定携带有A。

[0208] 将信息所使能的信息称为待使能信息，则具体实现过程中，对待使能信息进行使能的方式有很多种，例如但不限于，可以直接使能待使能信息，如待使能信息本身或者该待使能信息的索引等。也可以通过使能其他信息来间接使能待使能信息，其中该其他信息与待使能信息之间存在关联关系。还可以仅仅使能待使能信息的一部分，而待使能信息的其他部分则是已知的或者提前约定的。例如，还可以借助预先约定(例如协议规定)的各个信息的排列顺序来实现对特定信息的使能，从而在一定程度上降低使能开销。同时，还可以识别各个信息的通用部分并统一使能，以降低单独使能同样的信息而带来的使能开销。

[0209] 第二，在本申请中示出的第一、第二以及各种数字编号(例如，“#1”、“#2”等)仅为描述方便，用于区分的对象，并不用来限制本申请实施例的范围。例如，区分不同消息等。而不是用于描述特定的顺序或先后次序。应该理解这样描述的对象在适当情况下可以互换，以便能够描述本申请的实施例以外的方案。

- [0210] 第三，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排除他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。
- [0211] 第四，在本申请中，“预配置”可包括预先定义，例如，协议定义。其中，“预先定义”可以通过在设备(例如，包括各个网元)中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现，本申请对于其具体的实现方式不做限定。
- [0212] 第五，本申请实施例中涉及的“保存”，可以是指的保存在一个或者多个存储器中。所述一个或者多个存储器，可以是单独的设置，也可以是集成在编码器或者译码器，处理器、或通信装置中。所述一个或者多个存储器，也可以是一部分单独设置，一部分集成在译码器、处理器、或通信装置中。存储器的类型可以是任意形式的存储介质，本申请并不对此限定。
- [0213] 第六，本申请实施例中涉及的“协议”可以是指通信领域的标准协议，例如可以包括5G协议、新空口(new radio, NR)协议以及应用于未来的通信系统中的相关协议，本申请对此不做限定。
- [0214] 第七，本申请说明书附图部分的方法流程图中的虚线框表示可选的步骤。
- [0215] 以下，以网元之间的交互为例详细说明本申请实施例提供的通信方法。应理解，本申请中的各实施例中术语和步骤可以互相参考。
- [0216] 图3示出了一种多播会话的配置过程。下面结合图3中的各个步骤对方法300做示例性说明。
- [0217] S301，AF向MBSF发送MBS会话创建请求(Nnef_MBSSession_create_request)消息。对应地，MBSF接收来自AF的该MBS会话创建请求消息。
- [0218] 示例性地，AF向MBSF发送MBS会话创建请求消息以请求创建MBS会话，该MBS会话创建请求消息中携带MBS会话标识(MBS session ID)、QoS参数和安全策略等信息。其中，该QoS参数表示当前会话的服务质量要求，该QoS参数包括5G QoS标识符、分配保持优先级等参数。该安全策略用于指示当前会话是否需要(包括需要和不需要)核心网提供机密性和/或完整性安全保护。

- [0219] S302, MBSF向MB-SMF发送MBS会话创建请求(Nmb-smf-MBSSession-creation-request)消息。对应地, MB-SMF接收来自MBSF/NEF的该MBS会话创建请求消息。
- [0220] 示例性地, MBSF/NEF向MB-SMF发送MBS会话创建请求消息, 以请求MB-SMF创建MBS会话, 并配置MBS会话参数。该MBS会话创建请求消息中携带MBS会话标识、QoS参数等信息。
- [0221] S303, MB-SMF向MBSF发送MBS会话创建响应(Nmb-smf-MBSSession-creation-response)消息。对应地, MBSF接收来自MB-SMF的该MBS会话创建响应消息。
- [0222] 示例性地, MB-SMF接收来自MBSF的MBS会话创建请求消息之后, 对MB-UPF进行配置, 具体过程可参考现有协议, 本申请不作限定。然后MB-SMF向MBSF发送MBS会话创建响应消息, MB-SMF在该MBS会话创建响应消息中携带分配给MBSF的入口地址(ingress address)。
- [0223] S304, MBSF向MBSTF发送会话请求(Session request)消息, 该会话请求消息包括ingress address和MBS会话标识。对应地, MBSTF接收来自MBSF的该会话请求消息。
- [0224] S305, MBSTF向MBSF/NEF发送会话响应(Session response)消息。对应地, MBSF接收来自MBSTF的该会话响应消息。
- [0225] 示例性地, MBSTF接收来自MBSF/NEF的会话请求消息之后, 选择一个入口地址(IP地址和端口), 并通过会话响应消息将选择的入口地址提供给MBSF。
- [0226] S306, MBSF向AF发送MBS会话创建响应(Nnef-MBSSession-Create-response)消息。对应地, AF接收来自MBSF的该会话创建响应消息。
- [0227] 示例性地, MBSF通过会话创建响应消息, 向AF指示可能分配的入口地址和其他参数(例如TMGI), 详细过程本申请不作限定。
- [0228] S307, MBSF生成并配置服务宣告。
- [0229] 示例性地, MBSF生成服务宣告(service announcement), 该服务宣告用于向UE分发关于服务接收所需服务的信息(例如, IP多播地址(es)) and可能的其他服务相关参数(例如, 服务开始时间)。服务宣告包括用户服务标识(user service

ID)、MBS会话标识、服务区域、开始时间、安全服务描述等参数。安全服务描述包括MBSTF IP地址、用户服务需要的服务密钥MSK的标识符等参数。当Service announcement中包括安全服务描述时,表示当前用户服务需要安全保护,当Service announcement中不包括安全服务描述时,表示当前用户服务不需要安全保护。

[0230] 进一步地,MBSF向UE发送service announcement,该消息可以是通过短信、单播会话、多播会话等形式发送给UE,此处不做限定。应理解,MBSF生成该service announcement之后,可以发送给AF,由AF将该service announcement发送给UE,本申请不作限定。

[0231] 应理解,S307可以在S301之前执行,也可以在S301之后的任意时刻执行,本申请不作限定。

[0232] S308,UE通过网络侧建立PDU会话。具体过程本申请不作限定。

[0233] S309,UE向SMF发送多播会话加入请求消息。对应地,SMF接收来自UE的多播会话加入请求消息。

[0234] 示例性地,UE建立了PDU会话之后,可以根据service announcement发起MBS会话加入流程。例如,UE向SMF发送多播会话加入请求消息,该多播会话消息中携带MBS会话标识,该MBS会话标识是UE从service announcement中获取的,该多播会话加入请求消息也可以称作UE加入请求(UE_join_request)消息。该多播会话加入请求消息由UE发送给AMF,AMF处理后发送给SMF。具体的,该UE加入请求消息可以是PDU会话修改请求(PDU Session Modification Request)消息。

[0235] 应理解,UE也可以在PDU会话建立过程中,请求加入MBS会话,也就是说,S308和S309可以合并为一个步骤。示例性地,UE可以在PDU会话建立请求消息中携带MBS会话标识以请求加入该MBS会话标识对应的MBS会话。具体过程本申请不作限定。

[0236] S310,SMF通过MB-SMF获取MBS会话上下文。

[0237] 示例性地,如果SMF没有所述MBS会话的上下文时,SMF向MB-SMF请求获取所述MBS会话的上下文,具体过程本申请不作限定。

- [0238] 可以理解的是，如果MB-SMF在S302接收到了来自MBSF的多播密钥，则该MBS会话上下文中包括该多播密钥。
- [0239] S311，SMF向UE发送多播会话加入响应消息。对应地，UE接收来自SMF的该UE加入响应消息。
- [0240] 示例性地，SMF检查UE的授权后，配置MBS会话的承载，然后通过AMF向UE发送多播会话加入响应消息。该多播会话加入响应消息也可以称作UE加入响应(UE_join_response)消息。具体的，该消息可以是PDU会话修改命令(PDU Session Modification Command)消息。
- [0241] 可以理解的是，如果SMF在S310从MB-SMF获取的MBS会话上下文中包括多播密钥，则SMF在该UE加入响应消息中携带该多播密钥。对应地，UE接收来自SMF的该UE加入响应消息之后，从该UE加入响应消息中获取该多播密钥。通过这种方式，网络侧通过信令面通信流程向UE分发了多播密钥。
- [0242] 可选地，S312，UE通过RAN和MB-UPF配置/创建多播传输通道。应理解，该多播传输通道配置/创建完成之后，UE可以从该MB-UPF接收业务数据。
- [0243] 通过上述过程，可以实现MBS会话配置和承载的建立。进一步地，网络侧还可以向UE发送多播密钥，以保护多播通信的安全。
- [0244] 下面介绍两种网络侧向UE发送多播密钥的传输流程。
- [0245] 在一种实现方式中，网络侧通过信令面通信流程(control-plane procedure)向UE发送多播密钥。例如，MBSF在S302的MBS会话创建请求消息中携带多播密钥，MB-SMF接收到该多播密钥之后，将该多播密钥保存在MBS会话上下文。SMF在S310从MB-SMF获取MBS会话上下文之后，从该MBS会话上下文中获取多播密钥，然后SS311UE加入响应消息中将该多播密钥发送给UE。
- [0246] 在另一种实现方式中，网络侧通过用户面通信流程(user-plane procedure)向UE发送多播密钥。例如，S313，UE通过多播功能网元执行安全能力开放机制协商流程及用户服务注册流程，其中这里的多播功能网元包括MBSF或MBSTF。用户服务注册流程成功执行之后，在S314，UE通过MBSTF发送的MIKEY消息接收多播密钥。需要说明的是，如果UE和网络侧协商的安全能力开放机制为AKMA机制，则UE和MBSTF利用AKMA生成应用密钥，该应用密钥用于对多播服务密

钥进行安全保护，该多播服务密钥用于对MIKEY消息中传输的多播密钥(这里指的是多播传输密钥)进行安全保护。如果UE和网络侧协商的安全能力开放机制为GBA机制，则UE和MBSTF利用GBA生成应用密钥，该应用密钥用于对多播服务密钥进行安全保护，该多播服务密钥用于对MIKEY消息中传输的多播密钥(这里指的是多播传输密钥)进行安全保护。

- [0247] 下面结合S315-S318，简单介绍多播通信过程。
- [0248] S315，AF向MBSTF发送业务数据。对应地，MBSTF接收来自MBSTF的该业务数据。
- [0249] S316，MBSTF向MB-UPF发送安全保护的该业务数据。
- [0250] 示例性地，MBSTF接收来自AF的业务数据之后，通过多播密钥对该业务数据进行安全保护得到安全保护的数据，然后将该安全保护的数据发送给MB-UPF。
- [0251] S317，MB-UPF向UE发送安全保护的数据。对应地，UE接收来自MB-UPF的该安全保护的数据。
- [0252] 示例性地，MB-UPF接收来自MBSTF的安全保护的数据之后，通过多播会话(即UE和MB-UPF之间的多播传输通道)，将该安全保护的数据发送给UE。
- [0253] S318，UE通过多播密钥对通过多播会话接收的安全保护的数据解安全保护得到业务数据，并使用业务数据。
- [0254] 图4示出了本申请实施例提供的方法400的示例性流程图。方法400描述了一种UE和MBSTF之间执行安全能力开放机制的协商流程及用户服务注册流程。
- [0255] S401，UE向MBSTF发送HTTP请求消息，该HTTP请求消息包括KID。对应地，MBSTF接收来自UE的该HTTP请求消息。
- [0256] 示例性地，UE利用AKMA/GBA生成密钥标识符KID，然后在HTTP请求消息中携带该KID，该HTTP请求消息可以是应用请求(application request)消息。
- [0257] 该HTTP请求消息中还携带user-agent信元，该user-agent信元指示UE支持的安全能力开放机制，包括AKMA，GBA中的一个或多个。
- [0258] 可以理解的是，如果UE使用的是AKMA，则该KID为A-KID，user-agent信元中包括字符串“3gpp-akma”。如果UE使用的是GBA，则该KID为B-

KID。user-agent信元中包括字符串"3gpp-gba""3gpp-gba-uicc" "3gpp-gba-digest" 中的一个或多个。

[0259] S402, MBSTF向AAnF/BSF发送密钥获取请求消息。对应地, AAnF/BSF接收来自MBSTF的该密钥获取请求消息。

[0260] 示例性地, MBSTF接收来自UE的HTTP请求消息之后, 则如果MBSTF没有KID关联的激活上下文, 则MBSTF选择AAnF/BSF并向AAnF/BSF发送密钥请求(Key get request)消息, 该密钥请求消息中携带KID。

[0261] 可以理解的是, MBSTF根据user-agent信元选择使用AKMA或者GBA机制。示例性的, 如果密钥请求消息中携带的user-agent信元包括"3gpp-akma", MBSTF选择使用AKMA机制, 则MBSTF选择AAnF, 并向该AAnF发送该密钥请求消息; 如果密钥请求消息中携带的user-agent信元包括字符串"3gpp-gba" "3gpp-gba-uicc" "3gpp-gba-digest" 中的一个或多个, MBSTF选择使用GBA机制, 则MBSTF选择BSF, 并向该BSF发送该密钥请求消息。

[0262] S403, AAnF/BSF向MBSTF发送密钥获取响应消息。对应地, AAnF/BSF接收来自MBSTF的密钥获取响应消息。

[0263] 示例性地, AAnF/BSF根据KID查询或生成对应的密钥AF key, 然后通过密钥获取响应(Key get request)消息将该AF key发送给MBSTF。该密钥获取响应消息还包括UE的标识(user id)。可以理解的是, 当UE使用的是AKMA, 则AAnF在该密钥获取响应消息中携带的UE标识(user id)为GPSI; 当UE使用的是GBA时, 则BSF在该密钥获取响应消息中携带的UE标识(user id)为IMPI。

[0264] S404, MBSTF向UE发送HTTP响应消息。对应地, UE接收来自该MBSTF的HTTP响应消息。该HTTP响应消息可以是应用答复(application answer)消息。

[0265] 示例性地, 在安全能力开放机制协商成功的失败的情况下, MBSTF在该HTTP响应消息中携带用于指示协商失败的指示信息。UE接收来自MBSTF的HTTP响应消息后, 如果该HTTP响应消息中携带了用于指示协商失败的指示信息, 则UE确定安全能力开放机制协商失败; 如果该HTTP响应消息没有携带用于指示协商失败的指示信息, 且UE对FQDN校验成功, 则UE确定安全能力开放机制协商成功。

- [0266] S405, UE向MBSTF发送HTTP请求消息, 该HTTP请求消息包括多播业务标识。对应地, MBSTF接收来自UE的该HTTP请求消息。
- [0267] 示例性地, UE根据service announcement的参数, 向MBSTF发起服务请求。具体地, UE向MBSTF发送HTTP请求消息, 该HTTP请求消息包括多播业务标识, 例如MBS用户服务标识(MBS user service IDs)。该HTTP请求消息用于注册多播用户服务。
- [0268] S406, MBSTF向UE发送HTTP响应消息, 该HTTP响应消息包括状态码401。对应地, UE接收来自MBSTF的HTTP响应消息。
- [0269] 示例性地, 当需要对UE进行鉴权时, MBSTF向UE发送HTTP响应消息, 该HTTP响应消息中携带状态码401, 该状态码401指示UE未授权, 需要进行认证。
- [0270] S407, UE向MBSTF发送HTTP请求消息, 该HTTP请求消息包括多播业务标识、KID、psd。对应地, MBSTF接收来自MBSTF的HTTP请求消息。
- [0271] 示例性地, UE状态码401, 向MBSTF发送HTTP请求请求, 该HTTP请求消息中携带多播业务标识, 例如MBS服务标识(MBS service ID), 作为用户名的密钥标识KID, 以及基于应用密钥生成的认证参数, 如psd。
- [0272] S408, MBSTF向UE发送HTTP响应信息没改HTTP响应消息包括状态码。对应地, UE接收来自MBSTF的该HTTP响应信息。
- [0273] 示例性地, MBSTF根据认证参数, 对UE进行鉴权, 并根据鉴权结果向UE发送HTTP响应消息, 具体地, 该HTTP响应消息可以是HTTP认证信息(HTTP Authentication Info), 该HTTP响应消息中包括状态码(status code)。
- [0274] 可以理解的是, 在方法400中, S401-S404可以看做UE和MBSTF之间的安全能力开放参数的协商流程, S405-S408可以看做用户服务注册流程。用户服务注册流程可以在安全能力开放参数协商流程之后执行, 也可以交叉执行。例如, S401-S404可以在S405和S406之后执行, 本申请不作限定。
- [0275] 可以理解的是, S407中的多播业务标识和PSD也可以通过401消息随KID一并发给MBSTF, 此时可以不执行S407; 对应地, 408中的状态码可以在404的HTTP响应消息中返回给UE, 此时可以不执行S408。

- [0276] S401的HTTP请求消息和S407的HTTP请求消息可以是两个单独的消息，也可以合并为一条消息，本申请不作限定。
- [0277] 图5A示出了本申请实施例提供的方法500的示例性流程图。下面结合图5A中的各个步骤对方法500作示例性说明。
- [0278] S501，网络设备确定第一指示信息，该第一指示信息指示至少一种多播密钥传输流程。
- [0279] 示例性地，该至少一种多播密钥传输流程中的每一种多播密钥传输流程均是网络侧支持的、用于向终端设备传输多播密钥的通信流程，该多播密钥为终端设备与多播用户面功能网元之间的多播会话的安全传输密钥。
- [0280] 其中，该至少一种多播密钥传输流程包括以下一种或多种：C流程、U1流程、U2流程。
- [0281] 可以理解的是，对于C流程，这里的网络侧可以指的是多播服务传输功能网元、多播服务功能网元、多播会话管理网元、会话管理网元等；对于U1流程，这里的网络侧可以指的是多播服务传输功能网元、多播服务功能网元、应用认证与密钥管理锚点功能(Authentication and Key Management for Applications anchor function, AAnf)网元等；对于U2流程，这里的网络侧可以指的是多播服务传输功能网元、多播服务功能网元、引导服务功能(bootstrapping server function, BSF)等。
- [0282] 该网络设备可以是多播服务功能网元、接入网设备、应用功能网元、会话管理网元中的任意一种。
- [0283] 在该网络设备为多播服务功能网元的情况下，该多播服务功能网元可以根据配置信息确定该第一指示信息，其中，这里的配置信息可以是预置在多播服务功能网元上的，也可以是该多播功能网元从网络管理设备(如操作维护和管理(operation administration and maintenance, OAM)系统)或其他网元获取的，本申请不作限定。
- [0284] 在该网络设备为接入网设备的情况下，该接入网设备可以根据预配置信息确定第一指示信息，也可以从多播服务功能网元接收该第一指示信息。其中，本申

请实施例中的接入网设备可以是用于与终端设备通信的任意一种具有无线收发功能的通信设备，如eNB，或gNB等。

- [0285] 在该网络设备为应用功能网元的情况下，该应用功能网元可以从多播服务功能网元接收该第一指示信息。
- [0286] 在该网络设备为会话管理网元的情况下，该会话管理网元可以在多播会话上下文中获取该第一指示信息，例如，多播服务功能网元在多播会话创建过程将该第一指示信息发送给多播会话管理网元，多播会话管理网元将该第一指示信息保存到该多播会话对应的多播会话上下文中。会话管理网元可以从该多播会话管理网元获取该多播会话上下文，并从该多播会话上下文获取该第一指示信息。
- [0287] S502，网络设备向终端设备发送第一指示信息。对应地，终端设备接收来自该网络设备的该第一指示信息。
- [0288] 示例性地，在该网络设备为多播服务功能网元的情况下，该多播服务功能网元通过第一消息向终端设备发送该第一指示信息。在一种实现方式中，该第一消息可以是服务宣告消息。终端设备从该第一消息中获取该第一指示信息。
- [0289] 在该网络设备为接入网设备的情况下，该接入网设备可以向终端设备发送第二消息，该第二消息包括该第一指示信息。在一种实现方式中，该第二消息可以是系统消息。终端设备从该第二消息中获取该第一指示信息。
- [0290] 在该网络设备为应用功能网元的情况下，该应用功能网元可以向终端设备发送第三消息，该第三消息包括该第一指示信息。终端设备从该第三消息中获取该第一指示信息。
- [0291] 在该网络设备为会话管理网元的情况下，该会话管理网元可以向终端设备发送第四消息，该第四消息包括该第一指示信息。在一种实现方式中，该第四消息可以是多播会话加入响应消息。例如，终端设备向该会话管理网元请求加入多播会话，会话管理网元根据终端设备的请求，向多播会话管理网元获取该多播会话的多播会话上下文，并从该多播会话上下文中获取该第一指示信息。然后该会话管理网元向终端设备发送多播会话加入响应消息，该多播会话加入响应消息包括该第一指示信息。终端设备从该第四消息中获取该第一指示信息。

- [0292] S503, 终端设备基于自身对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [0293] 示例性地, 终端设备获取第一指示信息之后, 确定自身对该第一指示信息指示的至少一种多播密钥传输流程的支持情况, 然后基于该支持情况从核心网获取业务数据。其中, 所谓终端设备对至少一种多播密钥传输流程的支持情况, 是指终端设备是否支持该至少一种多播密钥传输流程中的多播密钥传输流程, 或者是指终端设备支持该至少一种多播密钥传输流程中的哪种或哪些种多播密钥传输流程, 又或者是指终端设备所支持的多播密钥传输流程与该至少一种多播密钥传输流程是否有交集, 交集是什么; 示例性地, 支持情况可以是以下任一种: 终端设备支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程, 或者终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程。例如, 该至少一种为网络侧所支持的多播密钥传输流程包括C流程和U1流程, 在终端设备支持C1流程和/或U1流程的情况下, 就可以说该终端设备支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程; 在终端设备既不支持C流程, 又不支持U1流程的情况下, 可以说终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程。
- [0294] 下面结合不同情况进行示例性说明。
- [0295] 在第一种实现方式中, 终端设备确定自身支持该至少一种多播密钥传输流程中的目标多播密钥传输流程。在这种情况下, 如果终端设备还未加入多播会话, 则终端设备向会话管理网元请求加入多播会话。并且, 终端设备通过该目标多播密钥传输流程获取多播密钥。
- [0296] 例如, 终端设备确定自身支持该至少一种多播密钥传输流程中的信令面通信流程, 即该目标多播密钥传输流程为会话管理网元和终端设备之间的信令面通信流程, 则终端设备从来自会话管理网元的多播会话加入响应消息中获取多播密钥, 其中这里的会话管理网元为核心网网元;
- [0297] 又例如, 终端设备确定自身支持该至少一种多播密钥传输流程中的用户面通信流程, 即该目标多播密钥传输流程为多播服务网元和终端设备之间的用户面通

信流程，则终端设备从来自多播服务网元的多媒体因特网密钥管理消息中获取该多播密钥。

[0298] 终端设备获取多播密钥之后，基于该多播密钥从第一内容分发网元获取业务数据。例如，终端设备通过多播会话从多播用户面功能网元接收安全保护的数据，然后利用多播密钥对该安全保护的数据解安全保护，得到业务数据。其中这里的第一内容分发网元为核心网网元。该第一内容分发网元例如可以是多播用户面功能网元。

[0299] 可以理解的是，终端设备确定多播会话建立完成之后，可以向应用功能网元发送第三指示信息，该第三指示信息用于指示多播会话建立成功。应用功能网元可以根据该第三指示信息确定通过多播会话向终端设备发送业务数据，或者说，应用功能网元确定通过第一内容分发网元向终端设备发送业务数据，或者说，应用功能网元确定不再通过单播会话向终端设备发送业务数据，该单播会话例如是协议数据单元会话。在这种情况下，当应用功能网元需要向终端设备发送业务数据时，应用功能网元将该业务数据发送给多播服务网元，多播服务网元利用多播密钥对该业务数据进行安全保护后得到安全保护的数据，并将该安全保护的数据发送给第一内容分发网元，然后第一内容分发网元通过多播会话向终端设备发送该安全保护的数据，终端设备利用利用多播密钥对该安全保护的数据解安全保护，得到业务数据。

[0300] 在第二种实现方式中，终端设备确定自身不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程。在这种情况下，如果终端设备还未加入多播会话，则终端设备不再向会话管理网元请求加入多播会话；如果终端设备已加入多播会话，则终端设备向会话管理网元请求离开该多播会话。终端设备确定不通过多播会话获取业务数据。

[0301] 可选地，终端设备可以选择通过单播会话从第二内容分发网元接收业务数据。该单播会话可以是终端设备已建立的协议数据单元会话。其中，这里的第二内容分发网元为核心网网元，例如用户面功能网元。

[0302] 可以理解的是，在终端设备确定单播会话建立完成之后，终端设备可以向应用功能网元发送第二指示信息，该第二指示信息用于指示单播会话建立成功。应

用功能网元可以根据该第二指示信息确定通过单播会话向终端设备发送业务数据，或者说，应用功能网元确定通过用户面功能网元向终端设备发送业务数据。在这种情况下，当应用功能网元需要向终端设备发送业务数据时，应用功能网元将该业务数据发送给第二内容分发网元，然后第二内容分发网元通过单播会话将该业务数据发送给终端设备。

[0303] 基于图5A对应的方案，一方面，终端设备可以基于自身对网络侧支持的至少一种多播密钥传输流程的支持情况从核心网获取业务数据，其中，从核心网获取业务数据的会话路径是基于该支持情况确定的，从而避免了终端设备因无法获取网络侧下发的多播密钥而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验；另一方面，本申请实施例提供的方案由终端设备自行判断自身对网络侧所支持的至少一种多播密钥传输流程的支持情况，从而无需让网络侧来判断或决策采用哪种多播密钥传输流程向终端设备分发多播密钥，从而可以降低网络侧的开销。

[0304] 这里的方法500可以与后续方法600、方法700以及方法800对应。其中，方法500中的第一指示信息可对应于方法600-800中的指示信息#1。方法500中的终端设备可对应于方法600-800中的UE；方法500中的网络设备可对应于方法600中的MBSF，此时方法500中的S501可对应于方法600中的S603，方法500中的S502可对应于方法600中的S604；或者，方法500中的网络设备还可以对应于方法600中的AF，此时方法500中的S502可对应于方法600中的S606；或者方法500中的网络设备还可以对应于方法700中的MBSF，此时方法500中的S501可对应于方法700中的S702；或者方法500中的网络设备还可以对应于方法700中的SMF，此时方法500中的S502可对应于方法700中的S712；或者方法500中的网络设备还可以对应于方法800中的RAN，此时方法500中的S502可对应于方法800中的S802。方法500中的S503可对应于方法600中的S610-S627，或者对应于方法700中的S714-S730，或者对应于方法800中的S807-S824。

[0305] 可以理解的是，上述方法500对应第一种通信系统的方法流程，该第一种通信系统至少包括终端设备和网络设备，该终端设备可以执行如上述方法500中的终

端设备所执行的方法对应的流程，该网络设备可以执行如上述方法500中的网络设备所执行的方法对应的流程。

[0306] 图5B示出了本申请实施例提供的方法520的示意性流程图。下面结合图5B中的各个步骤对方法520作示例性说明。

[0307] S521，终端设备确定从网络侧获取多播密钥失败。

[0308] 示例性地，该多播密钥为终端设备与第一内容分发网元之间的多播会话的安全传输密钥。下面结合示例对终端设备确定获取多播密钥失败的各种情况作示例性说明。

[0309] 示例性地，终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败，其中该第一种多播密钥传输流程是网络侧用于向所述终端设备传输多播密钥的第一通信流程。在一种可能的实现方式中，该第一种多播密钥传输流程为C流程，在这种情况下，终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败，包括终端设备确定通过C流程从网络侧获取多播密钥失败。例如，该终端设备向会话管理网元请求加入多播会话；会话管理网元根据终端设备的请求，从多播会话管理网元获取该多播会话对应的多播会话上下文。进一步地，会话管理网元向终端设备发送响应消息。可以理解的是，如果该多播会话上下文包括多播密钥，即网络侧通过C流程向终端设备发送多播密钥，则会话管理网元在发送给终端设备的响应消息中携带多播密钥，否则该响应消息中不携带多播密钥。对应地，终端设备接收来自该会话管理网元的该响应消息之后，判断是否可以从该响应消息中获取到多播密钥。可以理解的是，如果该响应消息中携带了多播密钥，并且终端设备支持C流程，则终端设备可以从该响应消息中获取到多播密钥，在这种情况下，终端设备确定从网络侧获取多播密钥成功；如果响应消息中没有携带多播密钥，或者终端设备不支持C流程，则终端设备不能从该响应消息中获取到多播密钥，在这种情况下，终端设备确定从网络侧获取多播密钥失败。

[0310] 示例性地，在终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败的情况下，终端设备可以尝试通过第二种多播密钥传输流程从网络侧获

取多播密钥，其中，该第二种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第二通信流程。

- [0311] 在一种可能的实现方式中(记为“方式I”),该第二种多播密钥传输流程为U1流程或U2流程,在这种情况下,终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥传输流程失败后,终端设备向网络侧发起安全能力开放机制协商流程。如果该安全能力开放机制协商失败,则终端设备根据该协商失败的结果确定从网络侧获取多播密钥失败;如果该安全能力开放机制协商成功,则终端设备可以继续执行用户服务注册流程,并通过U1从网络侧获取多播密钥,在这种情况下,终端设备确定从网络侧获取多播密钥成功。
- [0312] 在另一种可能的实现方式中(记为“方式II”),该第二种多播密钥传输流程为U1流程,在这种情况下,终端设备确定通过第一种多播密钥传输流程从网络侧获取多播密钥传输流程失败后,该终端设备基于应用认证与密钥管理机制向多播服务网元发起用户服务注册流程。如果用户服务注册流程失败,则终端设备根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败;如果用户服务注册流程成功,则终端设备可以通过U1流程获取多播密钥,在这种情况下,终端设备确定从网络侧获取多播密钥成功。
- [0313] 对应于上述方式II,在终端设备确定通过第二种多播密钥传输流程从网络侧获取多播密钥失败的情况下,终端设备可以尝试通过第三种多播密钥传输流程从网络侧获取多播密钥,其中,该第三种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第三通信流程。
- [0314] 在一种可能的实现方式中,该第三种多播密钥传输流程为U2流程,在这种情况下,终端设备确定通过第二种多播密钥传输流程从网络侧获取多播密钥传输流程失败后,该终端设备基于通用引导架构机制向多播服务网元发起用户服务注册流程。如果用户服务注册流程失败,则终端设备根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败;如果用户服务注册流程成功,则终端设备可以通过U2流程获取多播密钥,在这种情况下,终端设备确定从网络侧获取多播密钥成功。

- [0315] 可以理解的是，上述方式II中的第二种多播密钥传输流程和第三种多播密钥传输流程可以互换。也就是说，在另一种可能的实现方式中，第二种多播密钥传输流程为U2流程，第三种多播密钥传输流程为U3流程，具体实现方式与上述示例类似，这里不再重复说明。还可以理解的是，终端设备可以在分别确定通过第一种多播密钥传输流程、第二种多播密钥传输流程以及第三种多播密钥传输流程获取多播密钥失败之后，再确定从网络侧获取多播密钥失败。
- [0316] S522，该终端设备向会话管理网元请求离开已加入的多播会话。
- [0317] 示例性地，终端设备确定从网络侧获取多播密钥失败之后，向会话管理网元请求离开已加入的多播会话。例如，终端设备向会话管理网元发送多播会话离开请求消息，该多播会话离开请求消息包括终端设备已加入的多播会话的标识，该多播会话离开请求消息用于离开该多播会话。
- [0318] 可选地，S523，终端设备确定通过单播会话从用户面功能网元获取业务数据。
- [0319] 综上所述，终端设备确定从网络侧获取多播密钥失败之后，终端设备离开已加入的多播会话，并确定通过单播会话从用户面功能网元获取业务数据，也就是说，终端设备确定从网络侧获取多播密钥失败之后，确定不通过多播会话接收业务数据。
- [0320] 基于上述方法520，一方面，终端设备确定获取多播密钥失败后，离开已加入的多播会话，并在后续流程使用单播会话接收业务数据，从而可以避免由于终端设备无法获取网络侧下发的多播密钥，而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验；另一方面，本申请实施例提供的方案无需让网络侧来判断或决策采用哪种多播密钥传输流程向终端设备分发多播密钥，从而可以降低网络侧的开销。
- [0321] 这里的方法520可以与后续方法900对应。其中，方法520中的终端设备可对应于方法900中的UE，方法520中的会话管理网元可对应于方法900中的SMF，方法520中的S522可对应于方法900中的S927，方法520中的S523可对应于方法900中的S926。
- [0322] 可以理解的是，上述方法520对应第二种通信系统的方法流程，该第二种通信系统至少包括终端设备和会话管理网元，该终端设备可以执行如上述方法520中

的终端设备所执行的方法对应的流程，该会话管理网元可以执行如上述方法520中的会话管理网元所执行的方法对应的流程。

[0323] 图5C示出了本申请实施例提供的方法540的示意性流程图。下面结合图5C中的各个步骤对方法540作示例性说明。

[0324] S541，终端设备向会话管理网元发送请求消息，该请求消息用于请求加入该终端设备与多播用户面功能网元之间的多播会话。

[0325] S542，该会话管理网元确定该终端设备不支持至少一种为网络侧所支持的多播密钥传输流程中的所有多播密钥传输流程。

[0326] 示例性地，会话管理网元接收来自终端设备的请求消息之后，判断该终端设备是否支持至少一种为网络侧所支持的多播密钥传输流程中的所有多播密钥传输流程。例如，终端设备在S541的请求消息中携带用于指示至少一种为终端设备所支持多播密钥传输流程的指示信息，会话管理网元根据该指示信息判断该终端设备是否支持网络侧所支持的多播密钥传输流程中的至少一种多播密钥传输流程，或者说，会话管理网元根据该指示信息判断网络侧是否支持为终端设备所支持的多播密钥传输流程中的至少一种多播密钥传输流程，或者说，会话管理网元根据该指示信息判断终端设备对网络侧所支持的多播密钥传输流程的支持情况，或者说，会话管理网元根据该指示信息确定终端设备支持的多播密钥传输流程与网络侧支持的多播密钥传输流程是否匹配。

[0327] 可以理解的是，会话管理网元可以从该多播会话对应的多播会话上下文中确定网络侧支持的至少一种多播密钥传输流程，具体方式本申请不作限定。

[0328] S543，会话管理网元向该终端设备发送第三指示信息，该第三指示信息指示该会话管理网元拒绝该终端设备加入该多播会话或者指示该终端设备通过单播会话获取业务数据。

[0329] 示例性地，在会话管理网元确定该终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，会话管理网元向该终端设备发送第三指示信息，以拒绝该终端设备加入该多播会话，或者指示该终端设备通过单播会话获取业务数据。

[0330] 可选地，S544，该终端设备确定通过单播会话获取业务数据。

- [0331] 示例性地，该终端设备接收来自该会话管理网元的第三指示信息，根据该第三指示信息确定多播会话加入失败，或者，终端设备根据第三指示信息确定不通过多播会话获取业务数据。可选地，终端设备根据该第三指示信息，确定通过单播会话获取业务数据。
- [0332] 基于上述方法540，会话管理网元可以在确定终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，拒绝终端设备加入多播会话，使得终端设备后续可以通过单播会话接收业务数据，从而可以避免由于终端设备无法获取网络侧下发的多播密钥，而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验。
- [0333] 这里的方法540可以与后续方法1000对应。其中，方法540中的终端设备可对应于方法1000中的UE，方法540中的会话管理网元可对应于方法1000中的SMF，方法540中的S541可对应于方法1000中的S1009，方法500中的第三指示信息可对应于方法1000中的指示信息#7，方法500中的S544可对应于方法100中的S1025。
- [0334] 可以理解的是，上述方法540对应第三种通信系统的方法流程，该第三种通信系统至少包括终端设备和会话管理网元，该终端设备可以执行如上述方法540中的终端设备所执行的方法对应的流程，该会话管理网元可以执行如上述方法540中的会话管理网元所执行的方法对应的流程。
- [0335] 下面以5G系统为基础，详细介绍本申请实施例提供的通信方法。后续方法600至方法1000可应用于图1或图2所示的网络架构中。在一种实现方式中，方法600至方法1000中的MBSF可对应于方法500中的多播服务功能网元，方法600至方法1000中的MBSTF可对应于方法500中的多播服务网元，方法600至方法1000中的AF可对应于方法500中的应用功能网元，方法600至方法1000中的MB-SMF可对应于方法500中的多播会话管理网元，方法600至方法1000中的SMF可对应于方法500中的会话管理网元，方法600至方法1000中的UE可对应于方法500中的终端设备，方法600至方法1000中的指示信息#1可对应于方法500中的第一指示信息。
- [0336] 图6示出了本申请实施例提供的方法600的示例性流程图。下面结合各个步骤对方法600作示例性说明。

- [0337] S601, AF向MBSF发送MBS会话创建请求消息。对应地, MBSF接收来自AF的该MBS会话创建请求消息。
- [0338] S602, MBSF向AF发送MBS会话创建响应消息。对应地, AF接收来自MBSF的该MBS会话创建响应消息。
- [0339] 应理解, S601和S602与方法300中的S301和S306类似, 并且, 方法600中省略了方法300中的S302-S305对应的步骤, 为了简洁, 这里不再赘述。
- [0340] S603, MBSF确定指示信息#1。
- [0341] 示例性地, 该指示信息#1用于指示至少一种为网络侧所支持的多播密钥传输流程, 或者, 指示信息#1用于指示至少一种网络侧要求的多播密钥传输流程, 或者指示信息#1用于指示至少一种网络侧对应的多播密钥传输流程, 为了方便, 后续实施例均以第一种情况为例进行说明。该指示信息#1还可以是其他名称, 例如, 该指示信息#1还可以称作安全设置参数, 或者是安全参数, 或者是能力信息等, 本申请不作限定。
- [0342] 可以理解的是, 本申请实施例不限定指示信息#1的适用范围或者粒度; 示例性地, 指示信息#1可以适用于整个PLMN或者说可以为PLMN粒度, 即MBSF针对同一个PLMN下的所有UE采用/发送相同的指示信息#1; 示例性地, 指示信息#1可以适用于整个用户服务或者说可以为用户服务粒度, 即MBSF针对同一用户服务对应的所有UE采用/发送相同的指示信息#1; 示例性地, 指示信息#1可以适用于多播会话或者说可以为多播会话粒度, 即MBSF针对同一个多播会话关联的所有UE采用/发送相同的指示信息#1。
- [0343] 该至少一种为网络侧所支持的多播密钥传输流程包括以下一种或多种: C流程、U1流程、U2流程。
- [0344] 在一种实现方式中, MBSF根据配置信息确定该指示信息#1。其中, MBSF可以通过预置信息获取该配置信息, 或者MBSF通过OAM或者其他网元获取该核心网配置信息, 本申请不作限定。
- [0345] 可选地, MBSF可以从AF获取安全策略信息(例如从S602的MBS会话创建响应消息中获取安全策略信息), 该安全策略信息用于指示该多播会话是否需要安全保护。在安全策略信息指示该多播会话需要进行安全保护的情况下, MBSF

确定指示信息#1。在安全策略信息指示该多播会话不需要进行安全保护的情况下，MBSF可以不指定S603。

[0346] 下面结合不同示例，介绍几种通过指示信息#1来指示网络侧所支持的多播密钥传输流程。

[0347] 在一种实现方式(记为方案1)中，可以通过指示信息#1的取值，来指示网络侧所支持的多播密钥传输流程。示例性地，表1示出了指示信息#1的一种可能的取值方式。

[0348] 表1

指示信息#1 取值	含义
control-plane procedure	网络侧支持通过信令面通信流程(即 C 流程)传输多播密钥
user-plane procedure	网络侧支持通过用户面通信流程(即 U1 流程或 U2 流程)传输多播密钥
AKMA-based user-plane procedure	网络侧支持通过基于 AKMA 的用户面通信流程(即 U1 流程)传输多播密钥

GBA-based user-plane procedure	网络侧支持通过基于 GBA 的用户面通信流程(即 U2 流程)传输多播密钥
control-plane procedure and AKMA-based user-plane procedure	网络侧既支持通过信令面通信流程(即 C 流程)传输多播密钥，又支持通过基于 AKMA 的用户面通信流程(U1 流程)传输多播密钥
control-plane procedure and GBA-based user-plane procedure	网络侧既支持通过信令面通信流程(C 流程)传输多播密钥，又支持通过基于 GBA 的用户面通信流程(即 U2 流程)传输多播密钥
AKMA-based user-plane procedure and GBA-based user-plane procedure	网络侧既支持通过基于 AKMA 的用户面通信流程(即 U1 流程)传输多播密钥，又支持通过基于 GBA 的用户面通信流程(即 U2 流程)传输多播密钥
control-plane procedure, AKMA-based user-plane procedure and GBA-based user-plane procedure	网络侧既支持通过信令面通信流程(即 C 流程)传输多播密钥，又支持通过基于 AKMA 的用户面通信流程(即 U1 流程)传输多播密钥，还支持通过基于 GBA 的用户面通信流程(即 U2 流程)传输多播密钥

[0349] 可以理解的是，指示信息#1的取值可以是表1中任意一行。

[0350] 在另一种实现方式(记为方案2)中，指示信息#1中包括多个不同的字段，通过对不同字段的取值，来指示网络侧支持的多播密钥传输流程。示例性地，表2示出了一种指示信息#1中字段的设置及取值方式。

[0351] 表2

	字段	取值	含义
指 示 信 息 #1	control-plane procedure required	yes	网络侧支持通过信令面通信流程（即 C 流程）传输多播密钥
		no	网络侧不支持通过信令面通信流程(即 C 流程)传输多播密钥
	AKMA required	yes	网络侧支持通过基于 AKMA 的用户面通信流程（即 U1 流程）传输多播密钥
		no	网络侧不支持通过基于 AKMA 的用户面通信流程（即 U1 流程）传输多播密钥
	GBA required	yes	网络侧支持通过基于 GBA 的用户面通信流程（即 U2 流程）传输多播密钥
		no	网络侧不支持通过基于 GBA 的用户面通信流程（即 U2 流程）传输多播密钥

[0352] 可以理解的是，指示信息#1可以包括表2中三个字段中的一个或多个。

[0353] 在又一种实现方式(记为方案3)中，指示信息#1包括密钥分发元素(key distribution element)，可选地还包括安全能力开放参数(security capability exposure parameter)。其中，密钥分发元素用于指示网络侧所支持的多播密钥传输流程(包括信令面通信流程和用户面通信流程)，安全能力开放参数用于指示网络侧支持的安全能力开放机制(包括AKMA机制和GBA机制)。示例性地，表3示出了一种指示信息#1中元素的设置及取值方式。

[0354] 表3

	元素信息	取值	含义
指 示 信 息 #1	key distribution element	control-plane procedure	网络侧仅支持通过信令面通信流程（即 C 流程）传输多播密钥
		user-planc procedure	网络侧仅支持通过用户面通信流程（即 U1 流程或 U2 流程）传输多播密钥
		control-plane procedure and user-plane procedure	网络侧既支持通过信令面通信流程（即 C 流程），又支持通过用户面通信流程（即 U1 流程或 U2 流程）传输多播密钥
	security capability exposure parameter	AKMA	网络侧支持基于 AKMA 的用户面通信流程（即 U1 流程）传输多播密钥
		GBA	网络侧支持基于 GBA 的用户面通信流程（即 U1 流程）传输多播密钥
		AKMA and GBA	网络侧既支持基于 AKMA 的用户面通信流程（即 U1 流程）传输多播密钥，又支持基于 GBA 的用户面通信流程（即 U1 流程）传输多播密钥

- [0355] 可以理解的是，指示信息#1可以包括表3中的“key distribution element”，且“key distribution element”的取值可以是表3中与“key distribution element”对应的三个字段中的任意一个。如果“key distribution element”的取值为“user-plane procedure”或“control-plane procedure and user-plane procedure”，则指示信息#1还包括“security capability exposure parameter”，且“security capability exposure parameter”的取值可以是表3中与“security capability exposure parameter”对应的三个字段中的任意一个。
- [0356] 应理解，S603可以在S601之后执行，也可以在S602之后执行，本申请不作限定。
- [0357] 进一步地，MBSF向UE发送指示信息#1。下面结合以下方案A和方案B作示例性说明。
- [0358] 方案A：

[0359] S604, MBSF向UE发送服务宣告(Service Announcement)消息, 该服务宣告消息包括指示信息#1。对应地, UE接收来自MBSF的该服务宣告消息, 并从该服务宣告消息中获取指示信息#1。

[0360] 可以理解的是, 该指示信息#1可以是服务宣告消息中已有信元的一部分, 例如, 该指示信息#1可以作为服务宣告消息中的安全描述信元或服务保护描述信元的一部分。也就是说, MBSF可以将指示信息#1携带在服务宣告消息中已有信元发送给UE, 也可以将指示信息#1携带在独立于服务宣告消息中已有信元的新信元发送给UE, 本申请不作限定。示例性的服务宣告消息如下:

```
HTTP/2 200 OK
Server: xxx/1.6.3
Content-Type: application/xml
Content-Length: xx
<?xml version="1.0" encoding="UTF-8"?>
<securityDescription
  xmlns="urn:3GPP:metadata:2005:MBMS:securityDescription"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:3GPP:metadata:2005:MBMS:securityDescription security.xsd">
  <keyManagement
    offsetTime="5"
    randomTimePeriod="10"
    uiocKeyManagement="true"
    Control-planeKeyManagement="true"><!--表示网络侧支持通过C流程传输多播密钥-->
  ...
</securityDescription><!--安全描述信元-->
```

[0361] 上述示例是以MBSF通过服务宣告消息向UE发送指示信息#1为例进行说明的, 但可以理解的是, MBSF还可以通过其他消息或者流程向UE发送指示信息#1, 本申请不作限定。

[0362] 方案B:

[0363] S605, MBSF向AF发送指示信息#1, 对应地, AF接收来自MBSF的该指示信息#1。

[0364] S606, AF向UE发送指示信息#1。对应地, UE接收来自AF的该指示信息#1。

[0365] 可以理解的是, 上述示例是以MBSF将指示信息#1发送给AF, 然后由AF发送给UE为例进行说明的。但应理解, MBSF还可以将指示信息#1发送给其他网元, 然后由其他网元发送给UE。例如, MBSF可以将指示信息#1发送给该UDM, 然后UDM通过UE配置更新流程(UE Configuration Update procedure)向UE进行发送该指示信息#1。

- [0366] 可以理解的是，如果MBSF从AF获取的安全策略信息指示该MBS会话不需要进行安全保护的话，MBSF可以不确定指示信息#1，即不执行S603。在这种情况下，MBSF可以向UE指示该MBS会话不需要安全保护。
- [0367] S607，UE通过网络侧执行PDU会话建立流程。具体过程本申请不作限定。
- [0368] 可选地，S608，UE向AF发送指示信息#2，该指示信息#2用于指示UE和UPF之间的PDU会话建立成功。对应地，AF接收来自UE的该指示信息#2。
- [0369] 示例性地，UE确定PDU会话建立成功之后，向AF发送指示信息#2，以指示UE和UPF之间的PDU会话建立成功。
- [0370] 可选地，S609，AF确定通过PDU会话发送业务数据。
- [0371] 示例性地，AF接收来自UE的指示信息#2之后，根据该指示信息#2确定通过PDU会话向该UE发送业务数据，即AF确定通过UPF向UE下发业务数据，该UPF指的是该PDU会话中为该UE提供服务的UPF。
- [0372] 可以理解的是，S607-S609可以在S611之前执行，也可以在S611之后执行，本申请不作限定。
- [0373] S610，UE确定自身对网络侧所支持的至少一种多播密钥传输流程的支持情况。示例性地，UE接收到指示信息#1之后，根据指示信息#1确定网络侧所支持的至少一种多播密钥传输流程，然后UE确定自身对该至少一种多播密钥传输流程的支持情况，或者说，UE确定自身是否支持该至少一种多播密钥传输流程中的至少一种，或者说，UE判断自身支持的多播密钥传输流程与该至少一种多播密钥传输流程是否匹配，或者说，UE判断是否满足网络侧所要求的至少一种多播密钥传输流程中的一种或多种。
- [0374] 其中，UE对该至少一种多播密钥传输流程的支持情况，包括以下任一种：UE支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程，以及UE不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程。例如，该至少一种为网络侧支持的多播密钥传输流程包括C1流程和U1流程，在UE支持C1流程，或者UE支持U1流程的情况下，UE确定自身支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程；在UE既不支持信C1流程，又不支持

U1流程的情况下，UE确定自身不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程。

[0375] 如此，UE可以基于支持情况选择用于获取业务数据的会话。

[0376] 示例性地，在UE支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下，或者说，在UE满足该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下，UE执行图6中的情况A所对应的流程，以确定通过多播会话获取业务数据；在UE不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，或者说，在UE不满足该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE执行图6中的情况B所对应的流程，以确定通过PDU会话获取业务数据。下面分别对情况A和情况B进行示例性说明。

[0377] 情况A：

[0378] S611，UE向MB-SMF发送多播会话加入请求消息，该多播会话加入请求消息用于请求加入多播会话。对应地，MB-SMF接收来自UE的该多播会话加入请求消息。

[0379] 应理解，S611与方法300中的S309类似，这里不再赘述。

[0380] S612，SMF通过MB-SMF获取多播会话上下文。

[0381] S612与方法300中的S310类似，这里不再赘述。可以理解的是，如果MBSF选择信令面通信流程(control-plane procedure)向UE发送多播密钥，则MBSF在S601之后，可以将多播密钥发送给MB-SMF，MB-SMF接收到该多播密钥之后，将该多播密钥保存到MBS会话上下文。也就是说，如果MBSF选择了信令面通信流程向UE发送多播密钥，则SMF获取的该多播会话上下文中包括多播密钥。

[0382] S613，SMF向UE发送多播会话加入响应消息。对应地，UE接收来自SMF的该多播会话加入响应消息。

[0383] 示例性地，如果SMF在S612从多播会话上下文中获得多播密钥，则SMF在该多播多播会话加入响应消息中携带该多播密钥。

[0384] 如果UE在S610确定自身支持网络侧所支持的至少一种多播密钥传输流程中的C1流程的话，则终端设备通过C1流程获取多播密钥。具体地，UE接收来自

SMF的该多播会话加入响应消息，然后从该多播会话加入响应消息中获取多播密钥。

- [0385] 信令面通信流程可选地，S614，UE通过RAN和MB-UPF配置/创建/加入多播传输通道，该多播传输通道包括UE到RAN，以及RAN到MB-UPF之间的传输通道。具体过程本申请不作限定。可以理解的是，多播会话中的业务数据是通过该传输通道进行传输的。在RAN不支持多播业务的情况下，RAN和MB-UPF之间使用5GC单独的数据发送方式，即配置RAN到UPF，UPF到MB-UPF的传输通道；在RAN支持多播业务的情况下，RAN和MB-UPF之间使用5GC共享的数据发送方式，RAN和MB-UPF的传输通道在601-602会话创建过程中配置。
- [0386] 应理解，该多播传输通道配置完成之后，UE便可以通过该多播传输通道从MB-UPF接收业务数据。
- [0387] 如果UE在S610确定自身支持网络侧所支持的至少一种多播密钥传输流程中的U1流程或U2流程的话，则UE通过U1流程或U2流程获取多播密钥。具体地，在S615，UE通过MBSTF执行安全能力开放机制协商流程即用户服务注册流程，详细过程可参考方法400，这里不再赘述。然后，在S616，UE从MBSTF接收多播密钥。例如，UE从来自MBSTF的MIKEY消息中获取多播密钥。
- [0388] 可选地，S617，UE向AF发送指示信息#3，该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。
- [0389] 示例性地，UE确定多播会话建立成功之后，向AF发送指示信息#3，该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。
- [0390] 可选地，S618，AF确定通过多播会话发送业务数据。
- [0391] 示例性地，AF接收来自UE的指示信息#3之后，根据该指示信息#3确定通过多播会话向该UE发送业务数据，即AF确定通过MB-UPF向UE下发业务数据，其中该MB-UPF指的是该多播会话中为该UE提供服务的MB-UPF。
- [0392] 如果在S618之前，AF执行了S609，则S618也可以描述为：AF确定不再通过PDU会话向UE发送业务数据。
- [0393] 可选地，S619，UE确定通过多播会话接收业务数据。

- [0394] 示例性地，UE确定多播会话建立成功之后，确定通过多播会话接收业务数据。
- [0395] 通过上述方案，UE可以从网络侧获取多播密钥。下面结合S619–S622对多播通信的过程作示例性说明。
- [0396] S620，AF向MBSTF发送业务数据。对应地，MBSTF接收来自AF的该业务数据。
- [0397] 示例性地，当AF需要向UE发送业务数据时，AF基于S618，将业务数据发送给MBSTF。
- [0398] S621，MBSTF向MB-UPF发送安全保护的数据。对应地，MB-UPF接收来自MBSTF的该安全保护的数据。
- [0399] 示例性地，MBSTF接收来自AF的业务数据之后，通过多播密钥对该业务数据进行加密，得到安全保护的数据，然后MBSTF将该安全保护的数据发送给MB-UPF。
- [0400] S622，MB-UPF向UE发送安全保护的数据。对应地，UE接收来自MB-UPF的该安全保护的数据。
- [0401] S623，UE通过多播密钥对通过多播会话接收的安全保护的数据解安全保护，得到业务数据，并使用该业务数据。
- [0402] 情况B：
- [0403] 可选地，S624，UE选择通过PDU会话接收业务数据。
- [0404] 示例性地，在UE确定自身不支持为网络侧所支持的至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE不加入多播会话，并选择通过PDU会话接收业务数据，或者说，UE选择不通过多播会话接收业务数据。如果UE已加入多播会话，则UE触发多播会话离开流程，例如，UE向SMF发送多播会话离开请求消息，以请求离开已加入的多播会话。
- [0405] 可选地，如果UE没有执行S608，则UE可以在S624之后向AF发送指示信息#4，该指示信息#4用于指示UE将通过PDU会话获取业务数据，或者指示AF触发UPF通过PDU会话向UE传输业务数据。
- [0406] S625，AF向UPF发送业务数据。对应地，UPF接收来自AF的该业务数据。

- [0407] 示例性地，当AF需要向UE发送业务数据时，AF基于S609，将业务数据发送给UPF。
- [0408] S626，UPF向UE发送该业务数据。对应地，UE接收来自UPF的该业务数据。
- [0409] S627，UE使用通过PDU会话接收的业务数据。
- [0410] 综上所述，在上述情况A中，UE在S604或S606获取指示信息#1，并在S610确定支持该指示信息#1指示的至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下，才在S611请求加入多播会话，即UE确定通过多播会话从MB-UPF获取业务数据。可选地，在这种情况下，UE可以在S617向AF发送指示信息#3，以便AF能够及时确定通过多播会话向UE发送业务数据。
- [0411] 在上述情况B中，UE在S604或S606获取指示信息#1，并在S610确定不支持该指示信息#1指示的至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE不请求加入多播会话，即UE确定通过PDU会话从UPF获取业务数据。可选地，在这种情况下，如果UE此前没有向AF发送指示信息#2(如S608)，则UE向AF发送指示信息，以便AF能够及时确定通过PDU会话向UE发送业务数据。
- [0412] 图7示出了本申请实施例提供的方法700的示例性流程图。下面结合各个步骤对方法700做示例性说明。
- [0413] S701，AF向MBSF发送MBS会话创建请求消息。对应地，MBSF接收来自AF的MBS会话创建请求消息。
- [0414] 应理解，S701与方法300的S301类似，为了简洁，这里不再赘述。
- [0415] S702，MBSF确定指示信息#1。具体实现方式可参见方法600的S603，这里不再赘述。
- [0416] S703，MBSF向MB-SMF发送MBS会话创建请求消息。对应地，MB-SMF接收来自MBSF的会话创建请求消息。
- [0417] 可以理解的是，如果MBSF仅支持信令面通信流程，则MBSF在该MBS会话创建请求消息中携带多播密钥，在这种情况下MBSF可以不执行S703；如果MBSF不支持信令面通信流程，但支持用户面通信流程，则MBSF在该MBS会话创建请求消息中携带指示信息#1；如果MBSF既支持信令面通信流程，又支持用户面通

信流程，则MBSF可以在该MBS会话创建请求消息中携带多播密钥以及指示信息#1。

[0418] 对应的，MB-SMF接收来自MBSF的该MBS会话创建请求消息之后，将该MBS会话创建请求消息中携带的信息(多播密钥和/或指示信息#1)保存到多播会话上下文。

[0419] 用户面通信流程S704，MB-SMF向MBSF发送MBS会话创建响应消息。对应地，MBSF接收来自MB-SMF的该MBS会话创建响应消息。

[0420] S705，MBSF向AF发送MBS会话创建响应消息。对应地，AF接收来自MBSF的该MBS会话创建响应消息。

[0421] S706，MBSF向UE发送服务宣告消息。对应地，UE接收来自MBSF的该服务宣告消息。

[0422] 应理解，S704-S706与方法300中的S303、S306、S307类似，为了简洁，这里不再赘述。

[0423] S707，UE通过网络侧执行PDU会话建立流程。具体过程本申请不作限定。

[0424] 可选地，S708，UE向AF发送指示信息#2，该指示信息#2用于指示UE和UPF之间的PDU会话建立成功。对应地，AF接收来自UE的该指示信息#2。具体过程与方法600中的S608类似，这里不再赘述。

[0425] 可选地，S709，AF确定通过PDU会话发送业务数据。具体过程与方法600中的S609类似，这里不再赘述。

[0426] S710，UE向SMF发送多播会话加入请求消息。对应地，SMF接收来自UE的该多播会话加入请求消息。

[0427] S711，SMF获取多播会话上下文。

[0428] S710与S711与方法600中的S611、S612类似，这里不再赘述。可以理解的是，SMF在S711获取的多播会话上下文中包括MBSF在S703发送给MB-SMF的信息，即多播密钥和/或指示信息#1。

[0429] S712，SMF向UE发送多播会话加入响应消息。对应地，UE接收来自SMF的该多播会话加入响应消息。

- [0430] 示例性地, 该多播会话加入响应消息包括SMF从多播会话上下文中获取的多播密钥和/或指示信息#1。
- [0431] 可选地, S713, UE通过RAN和MB-UPF配置/创建多播传输通道。具体描述可参考方法600中的S614, 这里不再赘述。
- [0432] S714, UE判断是否能够获取多播密钥。
- [0433] 示例性地, UE接收来自SMF的多播会话加入响应消息之后, 判断是否能够从该多播会话加入响应消息中获取多播密钥。
- [0434] 在该多播会话加入响应消息中携带了多播密钥(即网络侧支持信令面通信流程), 且UE支持信令面通信流程的情况下, UE可以从该多播会话加入响应消息中获取多播密钥, 在这种情况下, UE执行图7中的情况C所对应的流程; 在该多播会话加入响应消息中没有携带多播密钥(即网络侧不支持信令面通信流程), 或者UE不支持信令面通信流程的情况下, UE无法从该多播会话加入响应消息中获取多播密钥, 在这种情况下, UE执行图7中的情况D对应的流程。下面分别对情况A和情况B进行示例性说明。
- [0435] 情况C:
- [0436] S715, UE获取多播密钥。即UE从该多播会话加入响应消息中获取多播密钥。
- [0437] 可以理解的是, 在这种情况下, 如果多播会话加入响应消息中携带了指示信息#1, UE可以忽略该指示信息#1。
- [0438] 可选地, S716, UE向AF发送指示信息#3, 该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。
- [0439] 可选地, S717, AF确定通过多播会话发送业务数据。
- [0440] 可选地, S718, UE确定通过多播会话接收业务数据。
- [0441] S719, UE和AF之间基于多播会话传输业务数据。
- [0442] 应理解, S716-S718与方法600中的S617-S619类似, S719可对应于方法600中的S620-S623, 为了简洁, 这里不再赘述。
- [0443] 情况D:
- [0444] S720, UE确定自身对网络侧所支持的至少一种多播密钥传输流程的支持情况。

- [0445] 示例性地，UE根据指示信息#1确定网络侧所支持的至少一种多播密钥传输流程，然后UE确定自身对该至少一种多播密钥传输流程的支持情况，或者说，UE确定自身是否支持该至少一种多播密钥传输流程中的一种或多种，或者说，UE判断自身支持的多播密钥传输流程与该至少一种多播密钥传输流程是否匹配。
- [0446] 在UE支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下，UE执行图7中的情况E所对应的流程；在UE不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE执行图7中的情况F所对应的流程。下面分别对情况E和情况F进行示例性说明。
- [0447] 情况E：
- [0448] S721，UE发起用户服务注册流程。具体过程可参考方法400中的S405-S408，这里不再赘述。
- [0449] S722，MBSTF向UE发送多播密钥。
- [0450] S723，UE向AF发送指示信息#3，该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。
- [0451] 可选地，S724，AF确定通过多播会话发送业务数据。
- [0452] 可选地，S725，UE确定通过多播会话接收业务数据。
- [0453] S726，UE和AF之间基于多播会话传输业务数据。
- [0454] 应理解，S722-S725与方法600中的S616-S619类似，S726可对应于方法600中的S620-S623，为了简洁，这里不再赘述。
- [0455] 情况F：
- [0456] 可选地，S727，UE选择通过PDU会话接收业务数据。具体过程与方法600中的S624类似，这里不再赘述。
- [0457] S728，UE向SMF发送多播会话离开请求消息，该多播会话离开请求消息用于请求离开UE已加入的多播会话。对应地，SMF接收来自UE的该多播会话离开请求消息。然后在S729，执行多播会话离开流程，具体过程本申请不作限定。
- [0458] S730，UE和AF之间基于PDU会话传输业务数据。
- [0459] 应理解，S730可对应于方法600中的S625-S627，为了简洁，这里不再赘述。

- [0460] 综上所述,在上述情况C中,如果UE能够在S712的多播会话加入响应消息中获取到多播密钥,则UE可以基于该多播密钥通过多播会话从MB-UPF获取业务数据。可选地,在这种情况下,UE可以在S716向AF发送指示信息#3,以便AF能够及时确定通过多播会话向UE发送业务数据。
- [0461] 在上述情况D中,在UE从S712的多播会话加入响应消息中没有获取到多播密钥,但获取到了指示信息#1的情况下,UE在S720确定自身对指示信息#1指示的至少一种多播密钥传输流程的支持情况。在UE确定自身支持该至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下(对应情况E),UE确定通过多播会话从MB-UPF获取业务数据。可选地,在这种情况下,UE可以在S723向AF发送指示信息#3,以便AF能够及时确定通过多播会话向UE发送业务数据。在UE确定自身不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下(对应情况F),UE在S728请求离开已加入的多播会话,即UE确定通过PDU会话从UPF获取业务数据。可选地,在这种情况下,如果UE此前没有向AF发送指示信息#2(如S708),则UE向AF发送指示信息,以便AF能够及时确定通过PDU会话向UE发送业务数据。
- [0462] 图8示出了本申请实施例提供的方法800的示例性流程图。下面结合各个步骤对方法800做示例性说明。
- [0463] S801, RAN获取指示信息#1。
- [0464] 示例性地,可以由OAM将指示信息#1配置到该RAN,也可以是由其他网络侧网元生成指示信息#1之后,发送给该RAN的。例如, MBSF确定指示信息#1(如方法600的S603)之后,将该指示信息#1发送给该RAN。其中该RAN支持MBS。
- [0465] 应理解,该指示信息#1的含义和形式可参考方法600中S603部分的描述,这里不再赘述。
- [0466] S802, RAN向UE发送系统消息,该系统消息包括指示信息#1。对应地, UE接收来自RAN的该系统消息。
- [0467] 示例性地, RAN可以将指示信息#1携带在系统消息中发送给UE, UE接收到系统消息后,从系统消息获取指示信息#1。

- [0468] 示例性地，该指示信息#1可以作为系统信息中已有信元的一部分。其中，系统信息的格式如下：系统消息包括主信息块(master information block, MIB)、系统信息块1(system information block 1, SIB 1)和系统信息(system information, SI)，其中MIB包括有限个最重要、最常用的传输参数，SIB 1包括其他SIB的调度信息以及其他小区接入的相关信息，SI承载的是SIB的调度信息。SI还包括SIB 2、SIB 3、SIB 4和SIB 5，其中SIB 2包括小区无线配置信息，SIB 3包括小区重选信息，SIB 4包括同频邻区列表、黑名单，SIB5包括频间邻区列表。
- [0469] 可选地，S803，MBSF向UE发送服务宣告；对应地，UE接收来自MBSF的服务宣告。具体过程可参考方法300中的S307类似，这里不再赘述。
- [0470] S804，UE通过网络侧执行PDU会话建立流程。
- [0471] 可选地，S805，UE向AF发送指示信息#2，该指示信息#2用于指示UE和UPF之间的PDU会话建立成功。对应地，AF接收来自UE的该指示信息#2。
- [0472] 可选地，S806，AF确定通过PDU会话发送业务数据。
- [0473] S804-S806与方法600中的S607-S609类似，这里不再赘述。
- [0474] S807，UE确定自身对网络侧所支持的至少一种多播密钥传输流程的支持情况。
- [0475] 在UE支持该至少一种多播密钥传输流程中的任意多播密钥传输流程的情况下，UE执行图8中的情况A所对应的流程；在UE不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE执行图8中的情况B所对应的流程。下面分别对情况A和情况B进行示例性说明。
- [0476] 针对S807，以及情况A和情况B所对应的流程可参考方法600中的S610-S627，这里不再赘述。
- [0477] 基于上述方法600-800，一方面，UE可以根据自身对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据，从而避免了UE由于因无法获取网络侧下发的多播密钥，导致而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况，可以提高用户体验；另一方面，本申请实施例提供的方案由UE自行判断自身对网络侧支持的至少一种多播密钥传输流

程的支持情况，从而无需让网络侧来判断或决策采用哪种多播密钥传输流程向UE分发多播密钥，从而可以降低网络侧的开销。

[0478] 图9A示出了本申请实施例提供的方法900的示例性流程图。下面结合各个步骤对方法900做示例性说明。

[0479] 应理解，S901-S904与方法300中的S301、S306、S307、S308类似，S905-S906与方法600中的S608-S609类似，S907-S910与方法300中的S309-S312类似，为了简洁，上述步骤不再赘述。

[0480] S911，UE判断是否能够获取多播密钥。

[0481] 示例性地，UE接收来自SMF的多播会话加入响应消息之后，判断是否能够从该多播会话加入响应消息中获取多播密钥。

[0482] 在该多播会话加入响应消息中携带了多播密钥(即网络侧支持信令面通信流程)，且UE支持信令面通信流程的情况下，UE可以从该多播会话加入响应消息中获取多播密钥，在这种情况下，UE执行图9A中的情况M所对应的流程；在该多播会话加入响应消息中没有携带多播密钥(即网络侧不支持信令面通信流程)，或者UE不支持信令面通信流程的情况下，UE无法从该多播会话加入响应消息中获取多播密钥，在这种情况下，UE执行图9A中的情况N对应的流程。下面分别对情况M和情况N进行示例性说明。

[0483] 情况M：

[0484] S912，UE获取多播密钥。具体地，UE从多播会话响应消息中获取多播密钥。

[0485] 可选地，S913，UE向AF发送指示信息#3，该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。

[0486] 可选地，S914，AF确定通过多播会话发送业务数据。

[0487] 可选地，S915，UE确定通过多播会话接收业务数据。

[0488] S916，UE和AF之间基于多播会话传输业务数据。

[0489] 应理解，S913-S915与方法600中的S617-S619类似，S916可对应于方法600中的S620-S623，为了简洁，这里不再赘述。

[0490] 情况N：

- [0491] 在一种实现方式中，UE确定不能从S909的多播会话加入响应消息中获取多播密钥后，发起安全能力开放机制协商流程，然后根据安全能力开放机制协商结果获取业务数据。下面结合S917–S929进行示例性说明。
- [0492] S917，UE向MBSTF发送HTTP请求消息，该HTTP请求消息中携带了指示UE支持的安全开放机制的信息，该HTTP请求消息用于协商安全能力开放机制。该S917可参考方法400中的S401，这里不再赘述。
- [0493] S918，MBSTF向UE发送HTTP响应消息。该S918可参考方法400中的S402，这里不再赘述。
- [0494] S919，UE确定安全能力开放机制是否协商成功。
- [0495] 示例性地，UE接收来自MBSTF的HTTP响应消息。如果该HTTP响应消息中携带了用于指示协商失败的指示信息，则UE确定安全能力开放机制协商失败；如果该HTTP响应消息没有携带用于指示协商失败的指示信息，且UE对FQDN校验成功，则UE确定安全能力开放机制协商成功。
- [0496] 可选地，在UE与MBSTF建立安全通道失败的情况下，则MBSTF可以向其他一些核心网网元发送通知消息，该通知消息中携带UE的标识(user ID)和原因值。其中，该核心网网元可以是NWDAF、MBSF、PCF、SMF、UPF中的任意一个。该UE的标识可以是SUPI或GPSI等，该原因值可以是UE与网络多播安全能力不匹配或UE建立多播安全失败等。应理解，该通知消息可以用于会话管理/计费管理/策略管理等。例如，在该核心网网元是NWDAF的情况下，NWDAF接收到该通知消息之后，记录失败原因，为后续升级网络设备提供参考。
- [0497] 在协商成功的情况下，UE执行图9A中的情况P对应的流程；在协商不成功的情况下，UE执行图9A中的情况Q对应的流程。下面分别对情况P和情况Q作示例性说明。
- [0498] 情况p:
- [0499] S920，UE发起用户服务注册流程。具体过程可参考方法400中的S405–S408，这里不再赘述。
- [0500] S921，MBSTF向UE发送多播密钥。

- [0501] S922, UE向AF发送指示信息#3, 该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。
- [0502] 可选地, S923, AF确定通过多播会话发送业务数据。
- [0503] 可选地, S924, UE确定通过多播会话接收业务数据。
- [0504] S925, UE和AF之间基于多播会话传输业务数据。
- [0505] 应理解, S921-S924与方法600中的S616-S619类似, S925可对应于方法600中的S620-S623, 为了简洁, 这里不再赘述。
- [0506] 情况Q:
- [0507] 可选地, S926, UE选择通过PDU会话接收业务数据。具体过程与方法600中的S624类似, 这里不再赘述。
- [0508] S927, UE向SMF发送多播会话离开请求消息, 该多播会话离开请求消息用于请求离开UE已加入的多播会话。对应地, SMF接收来自UE的该多播会话离开请求消息。然后在S928, 执行多播会话离开流程, 具体过程本申请不作限定。
- [0509] S929, UE和AF之间基于PDU会话传输业务数据。
- [0510] 应理解, S929可对应于方法600中的S625-S627, 为了简洁, 这里不再赘述。
- [0511] 在另一种实现方式中, UE确定不能从S909的多播会话加入响应消息中获取多播密钥后, 尝试通过用户面通信流程获取多播密钥。例如, UE尝试通过U1流程获取多播密钥, 如果多播密钥获取成功, 则UE可以执行如S922-S925所示的通信流程; 如果多播密钥获取失败, 则UE可以尝试通过基于GBA的用户面通信流程获取多播密钥, 如果多播密钥获取成功, 则UE可以执行如S922-S925所示的通信流程, 如果多播密钥获取失败, 则UE可以执行如情况Q所示的通信流程。
- [0512] 下面结合图9B和图9C介绍方法900对应两种逻辑流程图。
- [0513] 在图9B示出的第一种逻辑流程图中, UE接收多播会话加入响应消息(如S909)之后, 判断是否能够通过C流程获取多播密钥, 即判断是否能够从该多播会话加入响应消息中获取多播密钥(如S911)。在UE能够通过C流程中获取多播密钥的情况下, UE基于该多播密钥从MB-UPF获取业务数据(如S912-S916); 在UE不能通过C流程获取多播密钥的情况下, UE判断自身是否支持用户面多播密钥传输流程, 即UE判断自身是否支持U1流程和/或U2流程。在UE确定自身支持用户

面多播密钥传输流程的情况下(即UE支持U1流程和/或U2流程的情况下), UE发起安全能力开放机制协商流程(如S917-S918)。然后UE判断安全能力开放机制是否协商成功(如S919), 在确定协商成功的情况下, UE发起用户服务注册流程(如S920)。如果UE和网络侧协商确定的安全能力开放机制为AKMA机制, 则UE通过U1流程获取多播密钥(如S921如果UE和网络侧协商确定的安全能力开放机制为GBA机制, 则UE通过U2流程获取多播密钥; 然后UE基于该多播密钥从MB-UPF获取业务数据(如S925); 在UE确定自身不支持用户面多播密钥传输流程, 或者在确定安全能力开放机制协商失败的情况下, UE发起多播会话离开流程(如S927)以离开已加入的多播会话, 然后选择通过PDU会话从UPF获取业务数据。

[0514] 在图9C示出的第二种逻辑流程图中, UE接收多播会话加入响应消息(如S909)之后, 判断是否能够通过C流程获取多播密钥, 即判断是否能够从该多播会话加入响应消息中获取多播密钥(如S911)。在UE能够用过C流程获取多播密钥的情况下, UE基于该多播密钥从MB-UPF获取业务数据(如S912-S916); 在UE不能通过C流程获取多播密钥的情况下, UE确定是否能够通过U1流程获取多播密钥, 如果能够获取多播密钥的话, UE基于该多播密钥从MB-UPF获取业务数据(如S925), 如果不能获取多播密钥的话, UE进一步确定是否能够通过U2流程获取多播密钥, 如果能够获取多播密钥的话, UE基于该多播密钥从MB-UPF获取业务数据(如S925), 如果不能获取多播密钥的话, UE发起多播会话离开流程(如S927)以离开已加入的多播会话, 然后选择通过PDU会话从UPF获取业务数据。

[0515] 基于上述方法900, 一方面, UE可以根据从网络侧获取多播密钥的情况从核心网获取业务数据, 从而降低了UE因无法获取网络侧下发的多播密钥, 而无法获取业务数据(或无法对使用多播密钥进行安全保护的的数据进行解安全保护)的可能性, 可以提高用户体验; 另一方面, 本申请实施例提供的方案无需让网络侧来判断或决策采用哪种多播密钥传输流程向UE分发多播密钥, 从而可以降低网络侧的开销。

[0516] 图10示出了本申请实施例提供的方法1000的示例性流程图。下面结合各个步骤对方法1000做示例性说明。

- [0517] S1001, AF向MBSF发送MBS会话创建请求消息。对应地, MBSF接收来自AF的该MBS会话创建请求消息。
- [0518] S1002, MBSF向AF发送MBS会话创建响应消息。对应地, AF接收来自MBSF的该MBS会话创建响应消息。
- [0519] 应理解, S1001和S1002与方法300中的S301和S306类似, 并且, 方法1000中省略了方法300中的S302-S305对应的步骤, 为了简洁, 这里不再赘述。
- [0520] S1003, MBSF确定指示信息#1。S1003与方法600中的S603类似, 这里不再赘述。
- [0521] S1004, MBSF向MB-SMF发送通知消息, 该通知消息包括指示信息#1。对应地, MB-SMF接收来自MBSF的该通知消息, 并从该通知消息中获取指示信息#1。
- [0522] S1005, MBSF向UE发送服务宣告消息。对应地, UE接收来自MBSF的该服务宣告消息。
- [0523] S1006, UE通过网络侧执行PDU会话建立流程
- [0524] 可选地, S1007, UE向AF发送指示信息#2, 该指示信息#2用于指示UE和UPF之间的PDU会话建立成功。对应地, AF接收来自UE的该指示信息#2。
- [0525] 可选地, S1008, AF确定通过PDU会话发送业务数据。
- [0526] 上述S1005-S1008与方法700中的S706-S709类似, 这里不再赘述。
- [0527] S1009, UE向SMF发送多播会话加入请求消息, 该多播会话加入请求消息中包括指示信息#5, 该指示信息#5用于指示该UE支持的至少一种多播密钥传输流程。
- [0528] S1010, SMF通过MB-SMF获取多播会话上下文, 该多播会话上下文中包括指示信息#1。
- [0529] S1011, SMF确定UE对网络侧所支持的多播密钥传输流程的支持情况。
- [0530] 示例性地, SMF根据指示信息#1和指示信息#5, SMF确定UE对网络侧所支持的多播密钥传输流程的支持情况, 或者说, SMF确定UE是否支持网络侧支持的多播密钥传输流程中的至少一种, 或者说, SMF确定UE支持的多播密钥传输流

程与网络侧支持的多播密钥传输流程是否匹配，或者说，SMF确定网络侧是否支持UE支持的多播密钥传输流程中的至少一种。

[0531] 在UE支持该网络侧支持的至少一种多播密钥传输流程中的一种或多种多播密钥传输流程的情况下，UE执行图10中的情况Y所对应的流程；在UE不支持网络侧支持的至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下，UE执行图10中的情况Z所对应的流程。下面分别对情况Y和情况Z进行示例性说明。

[0532] 情况Y：

[0533] S1012，SMF向UE发送多播会话加入响应消息，该多播会话加入响应消息包括多播密钥。对应地，UE接收来自SMF的该多播会话加入响应消息。

[0534] 示例性地，在UE支持网络侧支持的多播密钥传输流程中的信令面通信流程的情况下，即UE和网络侧均支持C流程的情况下，SMF将在多播会话上下文中获取的多播密钥通过该多播会话加入响应消息发送给UE，UE接收该多播会话加入响应消息，并从该多播会话加入响应消息中获取多播密钥。

[0535] S1013与方法600中的S614类似，这里不再赘述。

[0536] S1014，SMF向UE发送多播会话加入响应消息，该多播会话加入响应消息包括指示信息#6。对应地，UE接收来自SMF的该多播会话加入响应消息。

[0537] 示例性地，在UE支持网络侧支持的多播密钥传输流程中的用户面通信流程的情况下，即UE和网络侧均支持用户面通信流程的情况下，SMF在该多播会话响应消息中携带指示信息#6，该指示信息#6用于指示UE通过用户面通信流程获取多播密钥。

[0538] UE根据该指示信息#6，在S1015发起安全能力开放机制协商流程以及用户服务注册流程，详细过程可参考方法400，这里不再赘述。然后，在S616，UE从MBSTF接收多播密钥。例如，UE从来自MBSTF的MIKEY消息中获取多播密钥。

[0539] 可选地，S1017，UE向AF发送指示信息#3，该指示信息#3指示UE和MB-UPF之间的多播会话建立成功。

[0540] 可选地，S1018，AF确定通过多播会话发送业务数据。

- [0541] 可选地，S1019，UE确定通过多播会话接收业务数据。
- [0542] S1020–S1023，UE和AF之间基于多播会话传输业务数据。
- [0543] 应理解，S1017–S1023与方法600中的S617–S623，为了简洁，这里不再赘述。
- [0544] 情况Z：
- [0545] S1024，SMF向UE发送多播会话加入响应消息，该多播会话加入响应消息包括指示信息#6。对应地，UE接收来自SMF的该多播会话加入响应消息。
- [0546] 示例性地，在UE不支持为网络侧所支持的任意一种多播密钥传输流程中的所有多播密钥传输流程的情况下，SMF在该多播会话响应消息中携带指示信息#7，该指示信息#7拒绝UE加入多播会话，或者该指示信息#7用于指示UE不支持为网络侧所支持的至少一种多播密钥传输流程中的所有多播密钥传输流程，或者该指示信息#7用于指示UE支持的多播密钥传输流程和网络侧支持的多播密钥传输流程不匹配，或者该指示信息#7用于指示UE通过PDU会话接收业务数据。
- [0547] 示例性的，SMF通过AMF向UE发送多播会话加入响应消息。具体消息举例如下：

8	7	6	5	4	3	2	1	
扩展协议标识符								octet 1
安全报头类型								octet 2
消息认证码								octet 3
								octet 6
顺序值								octet 7
拒绝原因值								octet 8
								octet n

- [0548] 可选地，在另一种可能的实现方式中，SMF也可以在UE加入多播会话之后，向UE发送指示信息#8，该指示信息#8用于指示UE离开已加入的多播会话，或者，该指示信息#8用于指示UE不支持为网络侧所支持的至少一种多播密钥传输流程中的所有多播密钥传输流程，或者该指示信息#8用于指示UE支持的多播密钥传输流程和网络侧支持的多播密钥传输流程不匹配，或者该指示信息#7用于指示UE通过PDU会话接收业务数据。UE根据该指示信息#8，向SMF请求离开该多播会话。

- [0549] S1025, UE选择通过PDU会话接收业务数据。
- [0550] 示例性地, UE根据指示信息#7选择通过PDU会话接收业务数据, 或者说UE根据指示信息#7选择不通过多播会话接收业务数据, 或者说, UE根据指示信息#7离开已加入的多播会话。在这种情况下, UE不向AF发送用于指示多播会话建立成功或通过多播会话传输业务数据的指示信息#3, 并在后续流程通过PDU会话接收业务数据。也就是说, 在确定多播会话加入响应消息中没有携带用于拒绝UE接入多播会话的指示信息#7的情况下, UE才向AF发送指示信息#3。
- [0551] 可选地, 如果在步骤S1025之前UE没有执行S1007, 则UE可以向AF发送指示信息#9, 该指示信息#9用于指示UE将通过PDU会话传输业务数据, 或者指示AF触发UPF通过PDU会话向UE传输业务数据。AF根据该指示信息#9确定通过PDU会话向UE发送业务数据, 进而触发UPF通过PDU会话向UE发送业务数据, 具体参见步骤S1026-S1027。
- [0552] 可选地, 如果在步骤S1025之前UE没有执行S1007, 则UE也可以向AF发送指示信息#2(指示PDU会话建立成功), AF根据收到PDU会话建立成功的指示信息(即指示信息#2)而没有收到多播会话建立成功的指示信息, 也可以确定通过PDU会话向UE发送业务数据, 进而触发UPF通过PDU会话向UE发送业务数据, 具体参见步骤S1026-S1027。
- [0553] S1026-S1028与方法600中的S625-S627类似, 这里不再赘述。
- [0554] 基于上述方法1000, SMF可以在确定UE不支持为网络侧所支持的至少一种多播密钥传输流程中的所有多播密钥传输流程的情况下, 拒绝UE加入多播会话, 或者指示UE离开已加入的多播会话, 使得UE后续可以通过PDU会话接收业务数据, 从而可以避免由于UE无法获取网络侧下发的多播密钥, 而无法获取业务数据(或无法对使用多播密钥进行安全保护的業務数据进行解安全保护)的情况, 可以提高用户体验。
- [0555] 相应于上述各方法实施例给出的方法, 本申请实施例还提供了相应的装置, 该装置包括用于执行上述各个方法实施例相应的模块。该模块可以是软件, 也可以是硬件, 或者是软件和硬件结合。可以理解的是, 上述各方法实施例所描述

的技术特征同样适用于以下装置实施例，因此，未详细描述的内容可以参见上文方法实施例，为了简洁，这里不再赘述。

- [0556] 图11是本申请实施例提供的通信装置10的示意性框图。该装置10包括收发模块11和处理模块12。收发模块11可以实现相应的通信功能，处理模块12用于进行数据处理，或者说该收发模块11用于执行接收和发送相关的操作，该处理模块12用于执行除了接收和发送以外的其他操作。收发模块11还可以称为通信接口或通信单元。
- [0557] 可选地，该装置10还可以包括存储模块13，该存储模块13可以用于存储指令和/或数据，处理模块12可以读取存储模块中的指令和/或数据，以使得装置实现前述各个方法实施例中设备或网元的动作。
- [0558] 在第一种设计中，该装置10可对应于上文方法实施例中的终端设备(如方法500、520、540中的终端设备，或者是方法600至方法1000中的UE)，或者是终端设备的组成部件(如芯片)。
- [0559] 该装置10可实现对应于上文方法实施例中的终端设备执行的步骤或者流程，其中，收发模块11可用于执行上文方法实施例中终端设备的收发相关的操作(如方法500中的S502)，处理模块12可用于执行上文方法实施例中终端设备的处理相关的操作(如方法500中的S503)。
- [0560] 在一种可能的实现方式，收发模块11，用于获取第一指示信息，该第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向该终端设备传输多播密钥的通信流程，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；该处理模块12，用于基于该终端设备对该至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [0561] 可选地，该处理模块12，具体用于确定支持该至少一种多播密钥传输流程中的目标多播密钥传输流程；以及，通过该目标多播密钥传输流程获取该多播密钥；基于该多播密钥从该第一内容分发网元获取该业务数据。
- [0562] 可选地，该处理模块12，具体用于使用该多播密钥对通过该多播会话从该内容分发网元接收的安全保护的数据解安全保护，得到该业务数据。

- [0563] 可选地，该目标多播密钥传输流程为会话管理网元和该装置之间的信令面通信流程，该收发模块11，具体用于从来自该会话管理网元的多播会话加入响应消息获取该多播密钥；或者，该目标多播密钥传输流程为多播服务网元和该装置之间基于应用认证与密钥管理的用户面通信流程，该处理模块12，具体用于基于通过认证与密钥管理机制生成的应用密钥，该收发模块11，具体用于从来自该多播服务网元的多媒体因特网密钥管理消息获取该多播密钥；或者，该目标多播密钥传输流程为多播服务网元和该装置之间基于通用引导架构的用户面通信流程，该处理模块12，具体用于基于通过通用引导架构机制生成的应用密钥，该收发模块11，具体用于从来自该多播服务网元的多媒体因特网密钥管理消息获取该多播密钥。
- [0564] 可选地，该处理模块12，具体用于确定不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程；该收发模块11，具体用于通过单播会话从第二内容分发网元接收该业务数据。
- [0565] 可选地，该第二内容分发网元为用户面功能网元。
- [0566] 可选地，该通信装置已加入该多播会话，该收发模块11，还用于向会话管理网元请求离开该多播会话。
- [0567] 可选地，该处理模块12，具体用于基于该终端设备对该至少一种多播密钥传输流程的支持情况选择用于从核心网获取业务数据的会话。
- [0568] 可选地，该第一内容分发网元为多播用户面功能网元，该处理模块12，具体用于确定支持该至少一种多播密钥传输流程中的目标多播密钥传输流程；以及，选择该装置与该第一内容分发网元之间的多播会话作为用于获取该业务数据的会话。
- [0569] 可选地，该处理模块12，具体用于确定该终端设备不支持该至少一种多播密钥传输流程中的所有多播密钥传输流程；以及选择该通信装置与第二内容分发网元之间的单播会话作为用于获取该业务数据的会话。
- [0570] 可选地，该处理模块12，具体用于从来自多播服务功能网元的第一消息中获取该指示信息。
- [0571] 可选地，该第一消息为服务宣告消息。

- [0572] 可选地，该处理模块12，具体用于从来自接入网设备的第二消息中获取该指示信息。
- [0573] 可选地，该第二消息为系统消息。
- [0574] 可选地，该处理模块12，具体用于从来自应用功能网元的第三消息中获取该指示信息。
- [0575] 可选地，该处理模块12，具体用于从来自会话管理网元的第四消息中获取该指示信息。
- [0576] 可选地，该第四消息为多播会话加入响应消息。
- [0577] 可选地，该至少一种多播密钥传输流程，包括以下一项或多项：会话管理网元与该通信装置之间的信令面通信流程，多播服务网元与该通信装置之间基于应用认证与密钥管理的用户面通信流程，以及多播服务网元与该通信装置之间基于通用引导架构的用户面通信流程。
- [0578] 可选地，该处理模块12，还用于确定该单播会话建立完成；该收发模块11，还用于向应用功能网元发送第二指示信息，该第二指示信息指示该单播会话建立成功。
- [0579] 可选地，该处理模块12，还用于确定该多播会话建立完成；该收发模块11，还用于向应用功能网元发送第三指示信息，该第三指示信息指示该多播会话建立成功。
- [0580] 在另一种可能的实现方式，收发模块11，用于向会话管理网元发送请求消息，该请求消息用于请求加入该通信装置与第一内容分发网元之间的多播会话；以及，接收来自该会话管理网元的第三指示信息，该第三指示信息指示该会话管理功能拒绝该终端设备加入该多播会话或者指示该终端设备通过单播会话获取业务数据；处理模块12，用于根据该第三指示信息确定多播会话建立失败。
- [0581] 可选地，该第一内容分发网元为多播用户面功能网元。
- [0582] 在第二种设计中，该装置10可对应于上文方法实施例中的网络设备(如方法500中的会话管理网元，或者是方法520和方法540中的会话管理网元，或者是方法600—方法700中的SMF，或MBSF，或者是方法800中的RAN，或者是方法900和方法1000中的SMF)，或者是网络设备的组成部件(如芯片)。

- [0583] 该装置10可实现对应于上文方法实施例中的网络设备执行的步骤或者流程，其中，收发模块11可用于执行上文方法实施例中网络设备的收发相关的操作(如方法500中的S502)，处理模块12可用于执行上文方法实施例中网络设备的处理相关的操作(如方法500中的S501)。
- [0584] 一种可能的实现方式，处理模块12，用于确定第一指示信息，该第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向终端设备传输多播密钥的通信流程，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；收发模块11，用于向该终端设备发送该第一指示信息。
- [0585] 可选地，该通信装置为多播服务网元，该收发模块11，具体用于向该终端设备发送第一消息，该第一消息包含该指示信息。
- [0586] 可选地，该第一消息为服务宣告消息。
- [0587] 可选地，该通信装置为接入网设备，该收发模块11，具体用于向该终端设备发送第二消息，该第二消息包含该指示信息。
- [0588] 可选地，该第二消息为系统消息。
- [0589] 可选地，该通信装置为应用功能网元，该收发模块11，具体用于向该终端设备发送第三消息，该第三消息包含该指示信息。
- [0590] 可选地，该通信装置为会话管理网元，该收发模块11，具体用于向该终端设备发送第四消息，该第四消息包含该指示信息。
- [0591] 可选地，该第四消息为多播会话加入响应消息。
- [0592] 可选地，该至少一种多播密钥传输流程，包括以下一种或多种：会话管理网元与该终端设备之间的信令面通信流程，多播服务网元和该终端设备之间基于应用认证与密钥管理的用户面通信流程，以及多播服务网元和该终端设备之间基于通用引导架构的用户面通信流程。
- [0593] 另一种可能的实现方式，该通信装置可以是前述会话管理网元，或者是会话管理网元的组成部分。其中，收发模块11，用于向会话管理网元发送请求消息，该请求消息用于请求加入该终端设备与第一内容分发网元之间的多播会话；以及，接收来自该会话管理网元的第三指示信息，该第三指示信息指示该会话管

理功能拒绝该终端设备加入该多播会话或者指示该终端设备通过单播会话获取业务数据；处理模块12，用于根据该第三指示信息确定多播会话建立失败。

[0594] 结合第四方面，在第四方面的某些实现方式中，该处理模块12，还用于根据该第三指示信息选择通过该终端设备与第二内容分发网元之间的单播会话获取业务数据。

[0595] 结合第四方面，在第四方面的某些实现方式中，该第一内容分发网元为多播用户面功能网元，该第二内容分发网元为用户面功能网元。

[0596] 结合第四方面，在第四方面的某些实现方式中，该收发模块11，具体用于接收来自该会话管理网元的该请求消息对应的响应消息，该响应消息包括该第三指示信息。

[0597] 结合第四方面，在第四方面的某些实现方式中，该收发模块11，还用于向应用功能网元发送第四指示信息，该第四指示信息指示通过单播会话向该终端设备发送业务数据。

[0598] 又一种可能的实现方式，该通信装置可以是前述会话管理网元，或者是会话管理网元的组成部分。其中，处理模块12，用于确定从网络侧获取多播密钥失败，该多播密钥为该终端设备与第一内容分发网元之间的多播会话的安全传输密钥；收发模块11，用于向会话管理网元请求离开该终端设备已加入的多播会话。

[0599] 可选地，该处理模块12，具体用于确定通过第一种多播密钥传输流程从网络侧获取多播密钥失败，该第一种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第一通信流程。

[0600] 可选地，该收发模块11，具体用于向会话管理网元请求加入该多播会话；以及，接收来自该会话管理网元的响应消息；该处理模块12，具体用于确定从该响应消息中获取该多播密钥失败。

[0601] 可选地，该处理模块12，具体用于确定通过第二种多播密钥传输流程从网络侧获取多播密钥失败，该第二种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第二通信流程。

- [0602] 可选地，该收发模块11，具体用于向该网络侧发起安全能力开放机制协商流程；该处理模块12，具体用于确定该安全能力开放机制协商失败；以及，根据该安全能力开放机制协商失败的结果确定从网络侧获取多播密钥失败。
- [0603] 可选地，该第二种多播密钥传输流程为多播服务网元 and 该通信装置之间基于应用认证与密钥管理的用户面通信流程，该处理模块12，具体用于基于应用认证与密钥管理机制向多播服务网元发起用户服务注册流程；确定该用户服务注册流程失败；根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败。
- [0604] 可选地，该处理模块12，具体用于确定通过第三种多播密钥传输流程从网络侧获取多播密钥失败，该第三种多播密钥传输流程是网络侧用于向该终端设备传输多播密钥的第三通信流程。
- [0605] 可选地，该处理模块12，具体用于基于通用引导架构机制向多播服务网元发起用户服务注册流程；确定该用户服务注册流程失败；根据该用户服务注册流程失败的结果确定从网络侧获取多播密钥失败。
- [0606] 可选地，该处理模块12，还用于选择通过单播会话从第二内容分发网元接收业务数据。
- [0607] 可选地，该第二内容分发网元为用户面功能网元。
- [0608] 可选地，该收发模块11，还用于向应用功能网元发送第四指示信息，该第四指示信息指示通过单播会话向该终端设备发送业务数据。
- [0609] 可选地，该第一内容分发网元为多播用户面功能网元。
- [0610] 应理解，各模块执行上述相应步骤的具体过程在上述各方法实施例中已经详细说明，为了简洁，在此不再赘述。
- [0611] 还应理解，这里的装置10以功能模块的形式体现。这里的术语“模块”可以指应用特有集成电路(application specific integrated circuit, ASIC)、电子电路、用于执行一个或多个软件或固件程序的处理器(例如共享处理器、专有处理器或组处理器等)和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。在一个可选例子中，本领域技术人员可以理解，装置10可以具体为上述实施例中的终端设备(如方法500、520、540中的终端设备，或者是方法600至方法1000中

的UE)，可以用于执行上述各方法实施例中与终端设备对应的各个流程和/或步骤；或者，装置10可以具体为上述实施例中的网络设备(如方法500中的会话管理网元，或者是方法520和方法540中的会话管理网元，或者是方法600–方法700中的SMF，或MBSF，或者是方法800中的RAN，或者是方法900和方法1000中的SMF)，可以用于执行上述各方法实施例中与网络设备对应的各个流程和/或步骤，为避免重复，在此不再赘述。

[0612] 上述各个方案的装置10具有实现上述方法中的设备(如网络设备或终端设备)所执行的相应步骤的功能。该功能可以通过硬件实现，也可以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；例如收发模块可以由收发机替代(例如，收发模块中的发送单元可以由发送机替代，收发模块中的接收单元可以由接收机替代)，其它单元，如处理模块等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

[0613] 此外，上述收发模块11还可以是收发电路(例如可以包括接收电路和发送电路)，处理模块可以是处理电路。

[0614] 图12是本申请实施例提供另一种通信装置20的示意图。该装置20包括处理器21，处理器21用于执行存储器22存储的计算机程序或指令，或读取存储器22存储的数据/信令，以执行上文各方法实施例中的方法。可选地，处理器21为一个或多个。

[0615] 可选地，如图12所示，该装置20还包括存储器22，存储器22用于存储计算机程序或指令和/或数据。该存储器22可以与处理器21集成在一起，或者也可以分离设置。可选地，存储器22为一个或多个。

[0616] 可选地，如图12所示，该装置20还包括收发器23，收发器23用于信号的接收和/或发送。例如，处理器21用于控制收发器23进行信号的接收和/或发送。

[0617] 作为一种方案，该装置20用于实现上文各个方法实施例中由移动管理网元执行的操作。

[0618] 例如，处理器21用于执行存储器22存储的计算机程序或指令，以实现上文各个方法实施例中终端设备(如方法500、520、540中的终端设备，或者是方法600至方法1000中的UE)的相关操作，例如，处理器21执行存储器22存储的计算机程序

或执行，可以实现500、方法520、方法540中的终端设备执行的方法，或者用于指示方法600至方法中UE执行的方法。

- [0619] 作为另一种方案，该装置20用于实现上文各个方法实施例中由网络设备(如方法500中的会话管理网元，或者是方法520和方法540中的会话管理网元，或者是方法600-方法700中的SMF，或MBSF，或者是方法800中的RAN，或者是方法900和方法1000中的SMF)执行的操作。
- [0620] 例如，处理器21用于执行存储器22存储的计算机程序或指令，以实现上文各个方法实施例中网络设备的相关操作。例如，处理器21执行存储器22存储的计算机程序或执行，可以实现方法500中的网络设备执行的方法，或者可以实现方法520和方法540中的会话管理网元执行的方法。
- [0621] 应理解，本申请实施例中提及的处理器可以是中央处理单元(central processing unit, CPU)，还可以是其他通用处理器、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、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。
- [0622] 还应理解，本申请实施例中提及的存储器可以是易失性存储器和/或非易失性存储器。其中，非易失性存储器可以是只读存储器(read-only memory, ROM)、可编程只读存储器(programmable ROM, PROM)、可擦除可编程只读存储器(erasable PROM, EPROM)、电可擦除可编程只读存储器(electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory, RAM)。例如，RAM可以用作外部高速缓存。作为示例而非限定，RAM包括如下多种形式：静态随机存取存储器(static RAM, SRAM)、动态随机存取存储器(dynamic RAM, DRAM)、同步动态随机存取存储器(synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(synchlink

DRAM, SLD RAM)和直接内存总线随机存取存储器(direct rambus RAM, DR RAM)。

- [0623] 需要说明的是,当处理器为通用处理器、DSP、ASIC、FPGA或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件时,存储器(存储模块)可以集成在处理器中。
- [0624] 还需要说明的是,本文描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。
- [0625] 图13是本申请实施例提供一种芯片系统30的示意图。该芯片系统30(或者也可以称为处理系统)包括逻辑电路31以及输入/输出接口(input/output interface)32。
- [0626] 其中,逻辑电路31可以为芯片系统30中的处理电路。逻辑电路31可以耦合连接存储单元,调用存储单元中的指令,使得芯片系统30可以实现本申请各实施例的方法和功能。输入/输出接口32,可以为芯片系统30中的输入输出电路,将芯片系统30处理好的信息输出,或将待处理的数据或信令信息输入芯片系统30进行处理。
- [0627] 作为另一种方案,该芯片系统30用于实现上文各个方法实施例中由网络设备(如方法500中的会话管理网元,或者是方法520和方法540中的会话管理网元,或者是方法600—方法700中的SMF,或MBSF,或者是方法800中的RAN,或者是方法900和方法1000中的SMF)执行的操作。
- [0628] 作为另一种方案,该芯片系统30用于实现上文各个方法实施例中由终端设备(如方法500、520、540中的终端设备,或者是方法600至方法1000中的UE)执行的操作。
- [0629] 本申请实施例还提供一种计算机可读存储介质,其上存储有用于实现上述各方法实施例中由设备执行的方法的计算机指令。
- [0630] 例如,该计算机程序被计算机执行时,使得该计算机可以实现上述方法各实施例中由移动管理网元执行的方法。
- [0631] 又如,该计算机程序被计算机执行时,使得该计算机可以实现上述方法各实施例中由终端设备执行的方法。

- [0632] 本申请实施例还提供一种计算机程序产品，包含指令，该指令被计算机执行时以实现上述各方法实施例中由设备(如移动管理网元，又如终端设备设备)执行的方法。
- [0633] 本申请实施例还提供一种通信的系统，包括前述的移动管理网元和会话管理网元。可选地，该系统还包括与上述远端终端设备和/或中继终端设备通信的设备。
- [0634] 上述提供的任一种装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例，此处不再赘述。
- [0635] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，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。此外，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，机械或其它的形式。
- [0636] 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。例如，所述计算机可以是个人计算机，服务器，或者网络设备等。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(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含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, DVD)、或者半导体介质(例如固态硬盘(solid state disk, SSD)等。例如, 前述的可用介质包括但不限于: U盘、移动硬盘、只读存储器(read-only memory, ROM)、随机存取存储器(random access memory, RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0637] 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, 任何熟悉本技术领域的技术人员在本申请揭露的技术范围内, 可轻易想到变化或替换, 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

- [权利要求 1] 一种通信方法，其特征在于，包括：
- 终端设备获取第一指示信息，所述第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向所述终端设备传输多播密钥的通信流程，所述多播密钥为所述终端设备与第一内容分发网元之间的多播会话的安全传输密钥；
- 所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从核心网获取业务数据，包括：
- 所述终端设备确定所述终端设备支持所述至少一种多播密钥传输流程中的目标多播密钥传输流程；
- 所述终端设备通过所述目标多播密钥传输流程获取所述多播密钥；
- 所述终端设备基于所述多播密钥从所述第一内容分发网元获取所述业务数据。
- [权利要求 3] 根据权利要求2所述的方法，其特征在于，所述终端设备基于所述多播密钥从所述第一内容分发网元获取所述业务数据，包括：
- 所述终端设备使用所述多播密钥对通过所述多播会话从所述第一内容分发网元接收的安全保护的数据解安全保护，得到所述业务数据。
- [权利要求 4] 根据权利要求1所述的方法，其特征在于，所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从网络侧获取业务数据，包括：
- 所述终端设备确定所述终端设备不支持所述至少一种多播密钥传输流程中的所有多播密钥传输流程；

- 所述终端设备通过单播会话从第二内容分发网元接收所述业务数据。
- [权利要求 5] 根据权利要求4所述的方法，其特征在于，所述终端设备已加入所述多播会话，所述方法还包括：
- 所述终端设备向会话管理网元请求离开所述多播会话。
- [权利要求 6] 根据权利要求1至5中任一项所述的方法，其特征在于，所述终端设备获取第一指示信息，包括：
- 所述终端设备从来自多播服务功能网元的第一消息中获取所述第一指示信息。
- [权利要求 7] 根据权利要求6所述的方法，其特征在于，所述第一消息为服务宣告消息。
- [权利要求 8] 根据权利要求1至7中任一项所述的方法，其特征在于，所述终端设备获取第一指示信息，包括：
- 所述终端设备从来自接入网设备的第二消息中获取所述第一指示信息。
- [权利要求 9] 根据权利要求8所述的方法，其特征在于，所述第二消息为系统消息。
- [权利要求 10] 根据权利要求1至5中任一项所述的方法，其特征在于，所述终端设备获取第一指示信息，包括：
- 所述终端设备从来自应用功能网元的第三消息中获取所述第一指示信息。
- [权利要求 11] 根据权利要求1至5中任一项所述的方法，其特征在于，所述终端设备获取第一指示信息，包括：
- 所述终端设备从来自会话管理网元的第四消息中获取所述第一指示信息。
- [权利要求 12] 根据权利要求11所述的方法，其特征在于，所述第四消息为多播会话加入响应消息。

- [权利要求 13] 根据权利要求1至12中任一项所述的方法，其特征在于，所述至少一种多播密钥传输流程，包括以下一项或多项：
会话管理网元与所述终端设备之间的信令面通信流程，
多播服务网元与所述终端设备之间基于应用认证与密钥管理的用户面通信流程，以及
所述多播服务网元与所述终端设备之间基于通用引导架构的用户面通信流程。
- [权利要求 14] 根据权利要求4或5所述的方法，其特征在于，所述单播会话为所述终端设备与所述用户面功能网元之间的数据连接会话，所述方法还包括：
所述终端设备确定所述单播会话建立完成；
所述终端设备向应用功能网元发送第二指示信息，所述第二指示信息指示所述单播会话建立成功。
- [权利要求 15] 根据权利要求2或3所述的方法，其特征在于，所述方法还包括：
所述终端设备确定所述多播会话建立完成；
所述终端设备向应用功能网元发送第三指示信息，所述第三指示信息指示所述多播会话建立成功。
- [权利要求 16] 一种通信方法，其特征在于，包括：
网络设备确定第一指示信息，所述第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向终端设备传输多播密钥的通信流程，所述多播密钥为所述终端设备与第一内容分发网元之间的多播会话的安全传输密钥；
所述网络设备向所述终端设备发送所述第一指示信息。
- [权利要求 17] 根据权利要求16所述的方法，其特征在于，所述网络设备为多播服务功能网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：
所述多播服务功能网元向所述终端设备发送第一消息，所述第一消息包含所述第一指示信息。

- [权利要求 18] 根据权利要求17所述的方法，其特征在于，所述第一消息为服务宣告消息。
- [权利要求 19] 根据权利要求16所述的方法，其特征在于，所述网络设备为接入网设备，所述网络设备向所述终端设备发送所述第一指示信息，包括：
所述接入网设备向所述终端设备发送第二消息，所述第二消息包含所述第一指示信息。
- [权利要求 20] 根据权利要求19所述的方法，其特征在于，所述第二消息为系统消息。
- [权利要求 21] 根据权利要求16所述的方法，其特征在于，所述网络设备为应用功能网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：
所述应用功能网元向所述终端设备发送第三消息，所述第三消息包含所述第一指示信息。
- [权利要求 22] 根据权利要求16所述的方法，其特征在于，所述网络设备为会话管理网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：
所述会话管理网元向所述终端设备发送第四消息，所述第四消息包含所述第一指示信息。
- [权利要求 23] 根据权利要求22所述的方法，其特征在于，所述第四消息为多播会话加入响应消息。
- [权利要求 24] 根据权利要求16至23中任一项所述的方法，其特征在于，所述至少一种多播密钥传输流程，包括以下一种或多种：
会话管理网元与所述终端设备之间的信令面通信流程，
多播服务网元和所述终端设备之间基于应用认证与密钥管理的用户面通信流程，以及
所述多播服务网元和所述终端设备之间基于通用引导架构的用户面通信流程。

- [权利要求 25] 一种通信方法，其特征在于，包括：
网络设备确定第一指示信息，并将所述第一指示信息发送给终端设备，所述第一指示信息指示至少一种多播密钥传输流程，其中，每一种多播密钥传输流程均是网络侧支持的、用于向所述终端设备传输多播密钥的通信流程，所述多播密钥为所述终端设备与第一内容分发网元之间的多播会话的安全传输密钥；
所述终端设备获取所述第一指示信息；
所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从核心网获取业务数据。
- [权利要求 26] 根据权利要求25所述的方法，其特征在于，所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从核心网获取业务数据，包括：
所述终端设备确定所述终端设备支持所述至少一种多播密钥传输流程中的目标多播密钥传输流程；
所述终端设备通过所述目标多播密钥传输流程获取所述多播密钥；
所述终端设备基于所述多播密钥从所述第一内容分发网元获取所述业务数据。
- [权利要求 27] 根据权利要求26所述的方法，其特征在于，所述终端设备基于所述多播密钥从所述第一内容分发网元获取所述业务数据，包括：
所述终端设备使用所述多播密钥对通过所述多播会话从所述第一内容分发网元接收的安全保护的数据解安全保护，得到所述业务数据。
- [权利要求 28] 根据权利要求25所述的方法，其特征在于，所述终端设备基于所述终端设备对所述至少一种多播密钥传输流程的支持情况从网络侧获取业务数据，包括：
所述终端设备确定所述终端设备不支持所述至少一种多播密钥传输流程中的所有多播密钥传输流程；

所述终端设备通过单播会话从第二内容分发网元接收所述业务数据。

[权利要求 29] 根据权利要求28所述的方法，其特征在于，所述终端设备已加入所述多播会话，所述方法还包括：

所述终端设备向会话管理网元请求离开所述多播会话。

[权利要求 30] 根据权利要求25至29中任一项所述的方法，其特征在于，所述网络设备为多播服务功能网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：

所述多播服务功能网元向所述终端设备发送第一消息，所述第一消息包含所述第一指示信息；

所述终端设备获取指示信息，包括：

所述终端设备从来自所述多播服务功能网元的所述第一消息中获取所述第一指示信息。

[权利要求 31] 根据权利要求30所述的方法，其特征在于，所述第一消息为服务宣告消息。

[权利要求 32] 根据权利要求25至29中任一项所述的方法，其特征在于，所述网络设备为接入网设备，所述网络设备向所述终端设备发送所述指示信息，包括：

所述接入网设备向所述终端设备发送第二消息，所述第二消息包含所述第一指示信息；

所述终端设备获取第一指示信息，包括：

所述终端设备从来自所述接入网设备的所述第二消息中获取所述第一指示信息。

[权利要求 33] 根据权利要求32所述的方法，其特征在于，所述第二消息为系统消息。

[权利要求 34] 根据权利要求25至29中任一项所述的方法，其特征在于，所述网络设备为应用功能网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：

所述应用功能网元向所述终端设备发送第三消息，所述第三消息包含所述第一指示信息；

所述终端设备获取第一指示信息，包括：

所述终端设备从来自所述应用功能网元的所述第三消息中获取所述第一指示信息。

[权利要求 35]

根据权利要求25至29中任一项所述的方法，其特征在于，所述网络设备为会话管理网元，所述网络设备向所述终端设备发送所述第一指示信息，包括：

所述会话管理网元向所述终端设备发送第四消息，所述第四消息包含所述第一指示信息；

所述终端设备获取第一指示信息，包括：

所述终端设备从来自所述会话管理网元的所述第四消息中获取所述第一指示信息。

[权利要求 36]

根据权利要求35所述的方法，其特征在于，所述第四消息为多播会话加入响应消息。

[权利要求 37]

根据权利要求25至36中任一项所述的方法，其特征在于，所述至少一种多播密钥传输流程，包括以下一项或多项：

会话管理网元与所述终端设备之间的信令面通信流程，

多播服务网元与所述终端设备之间基于应用认证与密钥管理的用户面通信流程，以及

所述多播服务网元与所述终端设备之间基于通用引导架构的用户面通信流程。

[权利要求 38]

根据权利要求28或29所述的方法，其特征在于，所述单播会话为所述终端设备与所述用户面功能网元之间的数据连接会话，所述方法还包括：

所述终端设备确定所述单播会话建立完成；

所述终端设备向应用功能网元发送第二指示信息，所述第二指示信息指示所述单播会话建立成功。

- [权利要求 39] 根据权利要求26或27所述的方法，其特征在于，所述方法还包括：
所述终端设备确定所述多播会话建立完成；
所述终端设备向应用功能网元发送第三指示信息，所述第三指示信息指示所述多播会话建立成功。
- [权利要求 40] 一种通信装置，其特征在于，所述装置包括：用于执行如权利要求1至15中任一项所述的方法的模块，或者用于执行如权利要求16至24中任一项所述的方法的模块。
- [权利要求 41] 一种通信装置，其特征在于，包括：
处理器，用于执行存储器中存储的计算机程序，以使得所述装置执行如权利要求1至15中任一项所述的方法，或者以使得所述装置执行如权利要求16至24中任一项所述的方法。
- [权利要求 42] 一种计算机程序产品，其特征在于，所述计算机程序产品包括用于执行如权利要求1至15中任一项所述的方法的指令，或者，所述计算机程序产品包括用于执行如权利要求16至24中任一项所述的方法的指令。
- [权利要求 43] 一种计算机可读存储介质，其特征在于，包括：所述计算机可读存储介质存储有计算机程序；所述计算机程序在计算机上运行时，使得所述计算机执行如权利要求1至15中任一项所述的方法，或者使得所述计算机执行如权利要求16至24中任一项所述的方法。
- [权利要求 44] 一种通信系统，其特征在于，包括终端设备和网络设备，
其中，所述终端设备用于执行如权利要求1至15中任一项所述的方法，所述网络设备用于执行如权利要求16至24中任一项所述的方法。