

密钥获取方法和通信装置

5 技术领域

本申请涉及通信领域，尤其涉及一种密钥获取方法和通信装置。

背景技术

随着移动通信的高速发展，新业务类型，如视频聊天、虚拟现实（virtual reality，VR）等数据业务的普遍使用提高了用户对带宽的需求。设备到设备（device-to-device，D2D）通信允许终端设备之间直接进行通信，可以在小区网络的控制下与小区用户共享频谱资源，有效的提高频谱资源的利用率。

当终端设备处于网络覆盖之外或与无线接入网络（radio access network，RAN）网元之间通信信号不好时，远端终端设备（Remote UE）可以通过中继终端设备（Relay UE）进行辅助通信，即远端终端设备与中继终端设备之间建立 PC5 连接，中继终端设备与移动网络建立连接，进而实现远端终端设备通过 PC5 连接和中继终端设备与移动网络建立连接，并获得服务。

在非直接通信连接建立过程中，为了保证通信的安全，远端终端设备与中继终端设备之间需要建立安全连接，即远端终端设备与中继终端设备之间传输的数据被加密保护和/或完整性保护。由于非直接通信连接是按需动态建立的，远端终端设备与中继终端设备之间无法预配置共享的安全信息（如密钥），进而无法基于预配置的共享安全信息建立远端终端设备与中继终端设备的之间的安全连接。

发明内容

本申请实施例提供一种密钥获取方法和通信装置，用于在远端终端设备与中继终端设备之间共享密钥。

为达到上述目的，本申请的实施例采用如下技术方案：

第一方面，提供了一种密钥获取方法，包括：远端终端设备向中继终端设备发送第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；远端终端设备根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥，远端认证服务功能网元为服务远端终端设备的认证服务功能网元，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥。

本申请实施例提供的密钥获取方法，远端终端设备向中继终端设备发送第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识。远端终端设备根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。其中的第一标识用于远端 AUSF 网元确定对应的第一共享密钥，或者用于 PKMF 网元确定对应的第二共享密钥，而第二共享密钥同样是由第一共享密钥和/或中继服务码生成，使得远端终端设备与远端 AUSF 网元或 PKMF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

在一种可能的实施方式中，第一标识为远端终端设备的订阅隐藏标识 SUCI。在空口传输过程中不会暴露远端终端设备的 SUPI。

在一种可能的实施方式中，还包括：远端终端设备获取第一标识。

在一种可能的实施方式中，远端终端设备获取第一标识，包括：远端终端设备发送中继服务码；远端终端设备接收与中继服务码对应的第一标识。可以从远端 AUSF 网元获取与中继服务码对应的第一标识。

在一种可能的实施方式中，还包括：远端终端设备根据第一共享密钥、中继服务码，生成临时标识；远端终端设备根据临时标识获取第一标识。该实施方式公开了生成第一标识的一种方式。

在一种可能的实施方式中，远端终端设备根据第一共享密钥、中继服务码生成临时标识，包括：远端终端设备根据第一共享密钥、中继服务码和第二新鲜性参数，生成临时标识。该实施方式公开了生成临时标识的一种方式。

在一种可能的实施方式中，远端终端设备获取第一标识，包括：远端终端设备根据第二新鲜性参数、路由指示和家乡网络标识，生成第一标识。该实施方式公开了生成第一标识的一种方式。

在一种可能的实施方式中，还包括：远端终端设备发送中继服务码；远端终端设备接收中继服务码对应的第二新鲜性参数。第二新鲜性参数可以来自远端 AUSF 网元，用于生成第一标识，第二新鲜性参数可以是远端 AUSF 网元生成的随机数或者远端 AUSF 网元本地维护的计数器的值。

在一种可能的实施方式中，第二新鲜性参数为远端终端设备本地维护的计数器的值。远端 AUSF 网元与远端终端设备分别本地维护各自的计数器时，采用相同的初始值和计数规则，以使这两个计数器的值保持一致。

在一种可能的实施方式中，第一标识包括路由指示和家乡网络标识。便于 PKMF 网元通过路由指示和家乡网络标识确定 UDM 网元或远端 AUSF 网元。

在一种可能的实施方式中，还包括：远端终端设备向中继终端设备发送第一验证信息，第一验证信息由第一临时密钥，以及，携带第一验证信息的全部或部分信元生成，第一临时密钥由第一共享密钥生成。第一验证信息用于发送给远端 AUSF 网元，远端 AUSF 网元接收第一验证信息后，按照与远端终端设备相同的方式生成第三验证信息，远端 AUSF 网元比较第一验证信息和第三验证信息以对远端终端设备进行验证，验证是否授权远端终端设备通过中继终端设备接入网络获取业务。

在一种可能的实施方式中，第一临时密钥由中继服务码、第三新鲜性参数、远端终端设备的第二标识以及第一标识中的至少一项，以及，第一共享密钥生成，其中，第三新鲜性参数为远端终端设备生成。该实施方式公开了生成第一临时密钥的一种方式。

在一种可能的实施方式中，还包括：远端终端设备向中继终端设备发送第二验证信息，第二验证信息由第一新鲜性参数、中继服务码和第一共享密钥生成。第二验证信息用于发送给 PKMF 网元，PKMF 网元接收第二验证信息后，按照与远端终端设备相同的方式生成第四验证信息，PKMF 网元比较第二验证信息和第四验证信息以对远端终端设备进行验证，验证是否授权远端终端设备通过中继终端设备接入网络获取业

务。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第一随机数，还包括：远端终端设备向中继终端设备发送第一随机数。第一随机数发送给远端 AUSF 网元或 PKMF 网元。

- 5 在一种可能的实施方式中，至少一个第一新鲜性参数包括第二随机数，还包括：远端终端设备从中继终端设备接收第二随机数。第二随机数可以来自远端 AUSF 网元或 PKMF 网元。

- 10 在一种可能的实施方式中，至少一个第一新鲜性参数为远端终端设备本地维护的计数器的值。远端 AUSF 网元或 PKMF 网元中的一个与终端设备在本地维护各自的计数器时，采用相同的初始值和计数规则，以使这两个计数器的值保持一致。

在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 K_{ausf} （或由该密钥生成的其他密钥）。

- 15 在一种可能的实施方式中，远端终端设备根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥，包括：远端终端设备根据第一共享密钥和中继服务码生成第二共享密钥，根据第二共享密钥以及至少一个第一新鲜性参数，生成根密钥，第二共享密钥为远端终端设备与临近业务密钥管理功能网元共享的密钥。远端终端设备和 PKMF 网元采用相同的方式生成根密钥。

- 20 第二方面，提供了一种密钥获取方法，包括：远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个，以及，中继服务码；第二标识为远端终端设备的永久身份标识，第一标识为远端终端设备的与中继服务码对应的标识；远端认证服务功能网元获取第一标识或第二标识对应的第一共享密钥；第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；远端认证服务功能网元根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥；远端认证服务功能网元发送根密钥。

- 25 本申请实施例提供的密钥获取方法，远端 AUSF 网元获取远端终端设备的第一标识或第二标识中的一个，以及，中继服务码；第二标识为远端终端设备的永久身份标识，第一标识为远端终端设备的与中继服务码对应的标识；远端 AUSF 网元获取第一标识或第二标识对应的第一共享密钥；第一共享密钥为远端终端设备与远端 AUSF 网元共享的密钥；远端 AUSF 网元根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥；远端 AUSF 发送根密钥。其中的第一标识用于远端 AUSF 网元确定对应的第一共享密钥，使得远端终端设备和远端 AUSF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

- 30 在一种可能的实施方式中，远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个，包括：远端认证服务功能网元接收远端终端设备的第一标识或第二标识中的一个。远端终端设备的第一标识或第二标识中的一个可以来自远端终端设备或 PKMF 网元。

在一种可能的实施方式中，远端认证服务功能网元获取远端终端设备的第一标识

或第二标识中的一个,包括:远端认证服务功能网元根据第一共享密钥、中继服务码,生成临时标识;远端认证服务功能网元根据临时标识生成第一标识。该实施方式公开了生成第一标识的一种方式。生成第一标识之后,可以发送给远端终端设备。

5 在一种可能的实施方式中,远端认证服务功能网元根据第一共享密钥、中继服务码,生成临时标识,包括:远端终端设备根据第一共享密钥、中继服务码和第二新鲜性参数,生成临时标识。该实施方式公开了生成临时标识的一种方式。

10 在一种可能的实施方式中,远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个,包括:远端认证服务功能网元根据第二新鲜性参数、路由指示和远端终端设备的家乡网络标识,生成第一标识。该实施方式公开了生成第一标识的一种方式。生成第一标识之后,可以发送给远端终端设备。

在一种可能的实施方式中,第二新鲜性参数为远端认证服务功能网元本地维护的计数器的值。远端 AUSF 网元与远端终端设备分别本地维护各自的计数器时,采用相同的初始值和计数规则,以使这两个计数器的值保持一致。

15 在一种可能的实施方式中,还包括:远端认证服务功能网元接收中继服务码;远端认证服务功能网元发送第二新鲜性参数。第二新鲜性参数可以发送给远端终端设备,用于生成第一标识,第二新鲜性参数可以是远端 AUSF 网元生成的随机数或者远端 AUSF 网元本地维护的计数器的值。

20 在一种可能的实施方式中,还包括:远端认证服务功能网元接收中继服务码;远端认证服务功能网元发送第一标识。中继服务码来自远端终端设备,第一标识用于发送给远端终端设备。

在一种可能的实施方式中,第一标识包括路由指示和家乡网络标识。便于 PKMF 网元通过路由指示和家乡网络标识确定 UDM 网元或远端 AUSF 网元。

25 在一种可能的实施方式中,还包括:远端认证服务功能网元接收第一验证信息;远端认证服务功能网元根据第一共享密钥,生成第一临时密钥;并根据第一临时密钥,以及,携带第一验证信息的消息的全部或部分信元,得到第三验证信息;远端认证服务功能网元比较第一验证信息和第三验证信息以对远端终端设备进行验证。即验证是否授权远端终端设备通过中继终端设备接入网络获取业务。

30 在一种可能的实施方式中,远端认证服务功能网元根据第一共享密钥,生成第一临时密钥,包括:远端认证服务功能网元根据中继服务码、第三新鲜性参数、第二标识以及远端终端设备的第一标识中的至少一项,以及,第一共享密钥,生成第一临时密钥,第三新鲜性参数为远端终端设备生成。该实施方式公开了生成第一临时密钥的一种方式。

在一种可能的实施方式中,至少一个第一新鲜性参数包括第一随机数,还包括:远端认证服务功能网元接收第一随机数。第一随机数来自远端终端设备。

35 在一种可能的实施方式中,至少一个第一新鲜性参数包括第二随机数,还包括:远端认证服务功能网元发送第二随机数。第二随机数发送给远端终端设备。

在一种可能的实施方式中,至少一个第一新鲜性参数为远端认证服务功能网元本地维护的计数器的值。远端 AUSF 网元与远端终端设备分别本地维护各自的计数器时,采用相同的初始值和计数规则,以使这两个计数器的值保持一致。

在一种可能的实施方式中，还包括：远端认证服务功能网元向统一数据管理网元发送第一标识。用于其他网元（例如 PKMF 网元）从 UDM 网元获取远端 AUSF 网元实例标识和/或远端终端设备的 SUPI。远端 AUSF 网元实例标识用于确定服务远端终端设备的远端 AUSF 网元。

- 5 在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 K_{ausf} （或由该密钥生成的其他密钥）。

第三方面，提供了一种密钥获取方法，包括：临近业务密钥管理功能网元接收远端终端设备的第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；临近业务密钥管理功能网元根据第
10 一标识获取远端终端设备与中继终端设备通信的根密钥，根密钥由第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数生成，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；临近业务密钥管理功能网元发送根密钥。

本申请实施例提供的密钥获取方法，PKMF 网元接收远端终端设备的第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远
15 端终端设备的匿名标识；PKMF 网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥，根密钥由第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数生成，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；PKMF 网元发送根密钥。其中的第一标识用于 PKMF 网元确定对应的第二共享密钥，使得远端终端设备和 PKMF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信
20 的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

在一种可能的实施方式中，临近业务密钥管理功能网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥，包括：临近业务密钥管理功能网元向统一数据管理功能网元发送第一标识；临近业务密钥管理功能网元从统一数据管理功能网元接收远端认证服务功能网元的标识信息；临近业务密钥管理功能网元根据标识信息，向
25 对应的远端认证服务功能网元发送第一标识；临近业务密钥管理功能网元从远端认证服务功能网元接收根密钥。该实施方式公开了 PKMF 网元获取根密钥的一种方式。

在一种可能的实施方式中，临近业务密钥管理功能网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥，包括：临近业务密钥管理功能网元向统一数据管理功能网元发送第一标识；临近业务密钥管理功能网元从统一数据管理功能网元接
30 收远端认证服务功能网元的标识信息以及远端终端设备的永久身份标识；临近业务密钥管理功能网元根据标识信息，向对应的远端认证服务功能网元发送远端终端设备的永久身份标识；临近业务密钥管理功能网元从远端认证服务功能网元接收根密钥。该实施方式公开了 PKMF 网元获取根密钥的一种方式。

在一种可能的实施方式中，临近业务密钥管理功能网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥，包括：临近业务密钥管理功能网元从远端认证服务功能网元接收至少一个第二共享密钥，第二共享密钥为远端终端设备与临近业务
35 密钥管理功能网元共享的密钥，第二共享密钥由第一共享密钥和中继服务码生成；临近业务密钥管理功能网元根据第一标识对应的第二共享密钥，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。该实施方式公开了 PKMF

网元获取根密钥的一种方式。

在一种可能的实施方式中，还包括：临近业务密钥管理功能网元接收第二验证信息；临近业务密钥管理功能网元根据第一新鲜性参数和第二共享密钥，生成第四验证信息；临近业务密钥管理功能网元比较第二验证信息和第四验证密信息以对远端终端设备进行验证。即验证是否授权远端终端设备通过中继终端设备接入网络获取业务。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第一随机数，还包括：临近业务密钥管理功能网元接收第一随机数。第一随机数来自远端终端设备。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第二随机数，还包括：临近业务密钥管理功能网元发送第二随机数。第二随机数发送给远端终端设备。

10 在一种可能的实施方式中，至少一个第一新鲜性参数为临近业务密钥管理功能网元本地维护的计数器的值。PKMF网元与远端终端设备分别本地维护各自的计数器时，采用相同的初始值和计数规则，以使这两个计数器的值保持一致。

在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf（或由该密钥生成的其他密钥）。

15 第四方面，提供了一种通信装置，包括收发模块和处理模块；收发模块，用于向中继终端设备发送第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；处理模块，用于根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥，远端认证服务功能网元为服务远端终端设备的认证服务功能网元，
20 第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥。

在一种可能的实施方式中，第一标识为远端终端设备的 SUCI。

在一种可能的实施方式中，处理模块和收发模块还用于获取第一标识。

在一种可能的实施方式中，收发模块还用于发送中继服务码；接收与中继服务码对应的第一标识。

25 在一种可能的实施方式中，处理模块还用于根据第一共享密钥、中继服务码，生成临时标识；根据临时标识获取第一标识。

在一种可能的实施方式中，处理模块还用于根据第一共享密钥、中继服务码和第二新鲜性参数，生成临时标识。

30 在一种可能的实施方式中，处理模块还用于根据第二新鲜性参数、路由指示和家乡网络标识，生成第一标识。

在一种可能的实施方式中，收发模块还用于发送中继服务码；接收中继服务码对应的第二新鲜性参数。

在一种可能的实施方式中，第二新鲜性参数为远端终端设备本地维护的计数器的值。

35 在一种可能的实施方式中，第一标识包括路由指示和家乡网络标识。

在一种可能的实施方式中，收发模块还用于向中继终端设备发送第一验证信息，第一验证信息由第一临时密钥，以及，携带第一验证信息的消息的全部或部分信元生成，第一临时密钥由第一共享密钥生成。

在一种可能的实施方式中，第一临时密钥由中继服务码、第三新鲜性参数、远端

终端设备的第二标识以及第一标识中的至少一项, 以及, 第一共享密钥生成, 其中, 第三新鲜性参数为远端终端设备生成。该实施方式公开了生成第一临时密钥的一种方式。

5 在一种可能的实施方式中, 收发模块还用于向中继终端设备发送第二验证信息, 第二验证信息由第一新鲜性参数、中继服务码和第一共享密钥生成。

在一种可能的实施方式中, 至少一个第一新鲜性参数包括第一随机数, 收发模块还用于向中继终端设备发送第一随机数。第一随机数发送给远端 AUSF 网元或 PKMF 网元。

10 在一种可能的实施方式中, 至少一个第一新鲜性参数包括第二随机数, 收发模块还用于从中继终端设备接收第二随机数。第二随机数可以来自远端 AUSF 网元或 PKMF 网元。

在一种可能的实施方式中, 至少一个第一新鲜性参数为远端终端设备本地维护的计数器的值。

15 在一种可能的实施方式中, 第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf。

在一种可能的实施方式中, 处理模块还用于根据第一共享密钥和中继服务码生成第二共享密钥, 根据第二共享密钥以及至少一个第一新鲜性参数, 生成根密钥, 第二共享密钥为远端终端设备与临近业务密钥管理功能网元共享的密钥。

20 第五方面, 提供了一种通信装置, 包括收发模块和处理模块; 处理模块用于获取远端终端设备的第一标识或第二标识中的一个, 以及, 中继服务码; 第二标识为远端终端设备的永久身份标识, 第一标识为远端终端设备的与中继服务码对应的标识; 处理模块还用于获取第一标识或第二标识对应的第一共享密钥; 第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥; 远端认证服务功能网元根据第一共享密钥、中继服务码, 以及, 至少一个第一新鲜性参数, 生成远端终端设备与中继终端设备通信的根密钥; 收发模块用于发送根密钥。

25 在一种可能的实施方式中, 收发模块还用于接收远端终端设备的第一标识或第二标识中的一个。

在一种可能的实施方式中, 处理模块还用于根据第一共享密钥、中继服务码, 生成临时标识; 远端认证服务功能网元根据临时标识生成第一标识。

30 在一种可能的实施方式中, 处理模块还用于根据第一共享密钥、中继服务码和第二新鲜性参数, 生成临时标识。

在一种可能的实施方式中, 处理模块还用于根据第二新鲜性参数、路由指示和远端终端设备的家乡网络标识, 生成第一标识。

35 在一种可能的实施方式中, 第二新鲜性参数为远端认证服务功能网元本地维护的计数器的值。

在一种可能的实施方式中, 收发模块还用于接收中继服务码; 发送第二新鲜性参数。

在一种可能的实施方式中, 收发模块还用于接收中继服务码; 发送第一标识。

在一种可能的实施方式中, 第一标识包括路由指示和家乡网络标识。

在一种可能的实施方式中，收发模块还用于接收第一验证信息；处理模块还用于根据第一共享密钥，生成第一临时密钥；并根据第一临时密钥，以及，携带第一验证信息的消息的全部或部分信元，得到第三验证信息；比较第一验证信息和第三验证信息以对远端终端设备进行验证。

- 5 在一种可能的实施方式中，处理模块还用于根据中继服务码、第三新鲜性参数、第二标识以及远端终端设备的第一标识中的至少一项，以及，第一共享密钥，生成第一临时密钥，第三新鲜性参数为远端终端设备生成。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第一随机数，收发模块还用于接收第一随机数。

- 10 在一种可能的实施方式中，至少一个第一新鲜性参数包括第二随机数，收发模块还用于发送第二随机数。

在一种可能的实施方式中，至少一个第一新鲜性参数为远端认证服务功能网元本地维护的计数器的值。

在一种可能的实施方式中，收发模块还用于向统一数据管理网元发送第一标识。

- 15 在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf。

- 第六方面，提供了一种通信装置，包括收发模块和处理模块；收发模块用于接收远端终端设备的第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；处理模块用于根据第一标识获取远端终端设备与中继终端设备通信的根密钥，根密钥由第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数生成，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；收发模块还用于发送根密钥。
- 20

- 在一种可能的实施方式中，收发模块还用于向统一数据管理功能网元发送第一标识；从统一数据管理功能网元接收远端认证服务功能网元的标识信息；根据标识信息，向对应的远端认证服务功能网元发送第一标识；从远端认证服务功能网元接收根密钥。
- 25

在一种可能的实施方式中，收发模块还用于向统一数据管理功能网元发送第一标识；从统一数据管理功能网元接收远端认证服务功能网元的标识信息以及远端终端设备的永久身份标识；根据标识信息，向对应的远端认证服务功能网元发送远端终端设备的永久身份标识；从远端认证服务功能网元接收根密钥。

- 30 在一种可能的实施方式中，收发模块还用于从远端认证服务功能网元接收至少一个第二共享密钥，第二共享密钥为远端终端设备与临近业务密钥管理功能网元共享的密钥，第二共享密钥由第一共享密钥和中继服务码生成；处理模块还用于根据第一标识对应的第二共享密钥，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

- 35 在一种可能的实施方式中，还包括：收发模块还用于接收第二验证信息；处理模块还用于根据第一新鲜性参数和第二共享密钥，生成第四验证信息；比较第二验证信息和第四验证密信息以对远端终端设备进行验证。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第一随机数，收发模块还用于接收第一随机数。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第二随机数，收发模块还用于发送第二随机数。

在一种可能的实施方式中，至少一个第一新鲜性参数为临近业务密钥管理功能网元本地维护的计数器的值。

- 5 在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 K_{ausf}。

第七方面，提供了一种通信装置，包括处理器，处理器与存储器相连，存储器用于存储计算机程序，处理器用于执行存储器中存储的计算机程序，以使得通信装置执行如第一方面及其任一项实施方式的方法。

- 10 第八方面，提供了一种通信装置，包括处理器，处理器与存储器相连，存储器用于存储计算机程序，处理器用于执行存储器中存储的计算机程序，以使得通信装置执行如第二方面及其任一项实施方式所述的方法。

- 15 第九方面，提供了一种通信装置，包括处理器，处理器与存储器相连，存储器用于存储计算机程序，处理器用于执行存储器中存储的计算机程序，以使得通信装置执行如第三方面及其任一项实施方式所述的方法。

第十方面，提供了一种计算机可读存储介质，计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行如第一方面及其任一项实施方式所述的方法。

- 20 第十一方面，提供了一种计算机可读存储介质，计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行如第二方面及其任一项实施方式所述的方法。

第十二方面，提供了一种计算机可读存储介质，计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行如第三方面及其任一项实施方式所述的方法。

- 25 第十三方面，提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器执行如第一方面及任一项实施方式所述的方法。

第十四方面，提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器，执行如第二方面及其任一项实施方式所述的方法。

- 30 第十五方面，提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器，执行如第三方面及其任一项实施方式所述的方法。

第十六方面，提供了一种通信系统，包括如第四方面及其任一项所述的通信装置、如第五方面及其任一项所述的通信装置，以及，如第六方面及其任一项所述的通信装置；或者，包括如第七方面所述的通信装置、如第八方面及其任一项所述的通信装置，以及，如第九方面及其任一项所述的通信装置。

- 35 第四方面到第十六方面的技术效果参照第一方面至第三方面的内容，在此不再重复。

附图说明

图 1 为本申请实施例提供的一种通信系统的架构示意图；

图 2 为本申请实施例提供的一种密钥获取方法的流程示意图一；

- 图 3 为本申请实施例提供的一种密钥获取方法的流程示意图二；
图 4 为本申请实施例提供的一种密钥获取方法的流程示意图三；
图 5 为本申请实施例提供的一种密钥获取方法的流程示意图四；
图 6 为本申请实施例提供的一种密钥获取方法的流程示意图五；
5 图 7 为本申请实施例提供的一种密钥获取方法的流程示意图六；
图 8 为本申请实施例提供的一种密钥获取方法的流程示意图七；
图 9 为本申请实施例提供的一种密钥获取方法的流程示意图八；
图 10 为本申请实施例提供的一种密钥获取方法的流程示意图九；
图 11 为本申请实施例提供的一种密钥获取方法的流程示意图十；
10 图 12 为本申请实施例提供的一种通信装置的结构示意图一；
图 13 为本申请实施例提供的一种通信装置的结构示意图二；
图 14 为本申请实施例提供的一种通信装置的结构示意图三；
图 15 为本申请实施例提供的一种通信装置的结构示意图四；
图 16 为本申请实施例提供的一种通信装置的结构示意图五；
15 图 17 为本申请实施例提供的一种通信装置的结构示意图六。

具体实施方式

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。

本申请实施例中，“/”表示该符号前后两者是“或”的关系。

本申请实施例既可以应用于时分双工（time division duplexing, TDD）的场景，也可以适用于频分双工（frequency division duplexing, FDD）的场景，不予限制。

本申请实施例依托无线通信网络中 5G 网络的场景进行说明，应当指出的是，本
25 申请实施例中的方案还可以应用于其他无线通信网络中，相应的名称也可以用其他无线通信网络中的对应功能的名称进行替代。

图 1 提供了一种 5G 通信系统架构，包括接入网和核心网。接入网用于实现无线接入有关的功能，接入网包括 3GPP 接入网和 non-3GPP 的接入网。该通信系统包括：
30 终端设备 101、（无线）接入网（（radio） access network, (R)AN）网元 102、用户面功能（user plane function, UPF）网元 103、数据网络（data network, DN）104、接入和移动性管理功能（access and mobility management function, AMF）网元 105、会话管理功能（session management function, SMF）网元 106、策略控制网元（policy control function, PCF）网元 107、统一数据管理网元（unified data management, UDM）网元 108、应用功能（application function, AF）网元 109、鉴权服务器功能（authentication
35 server function, AUSF）网元 110 以及网络切片选择功能（network slice selection function, NSSF）网元 111、网络开放功能（network exposure function, NEF）网元 112、网络功能库（network function repository function, NRF）网元 113、网络切片特定认证和授权功能（network slice specific authentication and authorization function, NSSAAF）114 和服务通信代理（service communication proxy, SCP）115。

需要说明的是，图 1 中的各个网元之间的接口名字只是一个示例，具体实现中接口名字可能为其他名字，不予限制。例如，终端设备 101 与 AMF 网元 105 之间的接口可以为 N1 接口，(R)AN 网元 102 与 AMF 网元 105 之间的接口可以为 N2 接口，(R)AN 网元 102 与 UPF 网元 103 之间的接口可以为 N3 接口，UPF 网元 103 与 SMF 网元 106 之间的接口可以为 N4 接口，UPF 网元 103 与 DN 104 之间的接口可以为 N6 接口。AMF 网元 105 向网络提供的服务接口 Namf，SMF 网元 106 向网络提供的服务接口 Nsmf，PCF 网元 107 向网络提供的服务接口 Npcf，UDM 网元 108 向网络提供的服务接口 Nudm，AF 网元向网络提供的服务接口 Naf，AUSF 网元 110 向网络提供的服务接口 Nausf，NSSF 网元 111 向网络提供的服务接口 Nnssf，NEF 网元 112 向网络提供的服务接口 Nnef，NRF 网元 113 向网络提供的服务接口 Nnrf，NSSAAF 网元 114 向网络提供的服务接口 Nnssaaf。

终端设备 101 与 (R)AN 网元 102 之间采用某种空口技术相互通信。终端设备 101 可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其他处理设备；还可以包括用户单元 (subscriber unit)、蜂窝电话 (cellular phone)、智能电话 (smart phone)、无线数据卡、个人数字助理 (personal digital assistant, PDA) 电脑、平板型电脑、无线调制解调器 (modem)、手持设备 (handheld)、膝上型电脑 (laptop computer)、无绳电话 (cordless phone) 或者无线本地环路 (wireless local loop, WLL) 台、机器类型通信 (machine type communication, MTC) 终端、用户设备 (user equipment, UE)、移动台 (mobile station, MS)、终端设备 (terminal device) 或者中继用户设备等。其中，中继用户设备可以是 5G 家庭网关 (residential gateway, RG)。为方便描述，上面提到的设备可以统称为终端设备。

本申请实施例中远端终端设备 (远端 UE) 可以通过中继终端设备 (中继 UE) 接入到 3GPP 网络，并与网络设备和应用服务器进行非直接通信。

(R)AN 网元 102 为终端设备 101 提供无线接入的设备，包括 RAN 网元和 AN 网元，其中，RAN 网元主要是 3GPP 网络无线网络设备，AN 网元可以是 non-3GPP 定义的接入网设备。本申请以 RAN 网元为例，但不意在限定于此。

其中，RAN 网元主要负责空口侧的无线资源管理、服务质量 (quality of service, QoS) 管理、数据压缩和加密等功能。其可以包括各种形式的基站，例如：宏基站、微基站 (也称为小站)、中继站、接入点等。在采用不同的无线接入技术的系统中，具备基站功能的设备的名称可能会有所不同，例如，在第五代 (5th generation, 5G) 通信系统中，称为 RAN 网元或者 gNB (5G NodeB)；在长期演进 (long term evolution, LTE) 系统中，称为演进的节点 B (evolved NodeB, eNB 或者 eNodeB)；在第三代 (3rd generation, 3G) 通信系统中，称为节点 B (Node B) 等。

AN 网元允许终端设备和 3GPP 核心网之间采用非 3GPP 技术互连互通，其中，非 3GPP 技术包括例如：无线保真 (Wireless Fidelity, Wi-Fi)、全球微波互联接入 (worldwide interoperability for microwave access, WiMAX)、码分多址 (code division multiple access, CDMA) 网络等。

UPF 网元 103 主要负责对用户报文进行处理，如转发、计费等。可以从数据网络接收用户数据，通过 RAN 网元传输给终端设备；UPF 网元还可以通过 RAN 网元从终

端设备接收用户数据，转发到 DN。UPF 网元中为终端设备提供服务的传输资源和调度功能由 SMF 网元管理控制。

DN 104 指的是为用户提供数据传输服务的网络，如 IP 多媒体业务 (IP multi-media service, IMS)、互联网 (Internet) 等。终端设备 101 通过建立终端设备、RAN 网元 102、UPF 网元 103 以及 DN 104 之间的协议数据单元 (protocol data unit, PDU) 会话来访问 DN 104。其中用户面的路径为：终端设备到 (R)AN 网元，到 UPF 网元，再到 DN。

AMF 网元 105 主要负责移动网络中的移动性管理，如用户位置更新、用户注册网络、用户切换等。

SMF 网元 106 主要负责移动网络中的会话管理，如会话建立、修改、释放。例如，具体功能包括：为用户分配 IP 地址、选择提供报文转发功能的 UPF 网元等。

PCF 网元 107 提供统一的策略框架来控制网络行为，提供策略规则给控制层网络功能，例如 QoS 策略、切片选择策略等。同时负责获取与策略决策相关的用户签约信息。

UDM 网元 108 用于生成认证信任状，用户标识处理 (如存储和管理用户永久身份等)，接入授权控制和签约数据管理等。

AF 网元 109 也可以称为服务器，负责与 3GPP 核心网交互来提供服务，例如影响数据路由决策，策略控制功能或者向网络侧提供第三方的一些服务等。

AUSF 网元 110 用于对用户进行鉴权和授权。

NSSF 网元 111 用于对切片功能进行集中管理。

NEF 网元 112 负责内外部网络隔离，用于支持能力和事件的开放，包括开放监控 (Monitoring) 能力、策略/计费能力和分析报告能力等。

NRF 网元 113 负责维护可用的网络功能实例的文本和网络功能支持的服务，用于其他网络功能网元进行服务发现或网络功能网元发现。

NSSAAF 网元 114 用于支持网络切片特定的认证和授权流程，可以和 AAA (authentication, authorization and accounting, 认证授权和计费) 服务器或 AAA 代理通信。

SCP 网元 115 用于支持非直接通信、代理发现以及向目标网络功能网元或下一跳 SCP 发送路由消息等。

在临近业务 (Proximity-based Services, ProSe) 的课题研究中，为了支持临近业务通信，还引入了 5G 直接发现名称管理功能 (direct discovery name management Function, DDNMF) 网元，用于分配和处理 ProSe 应用标识和 ProSe 应用码映射。

如图 2 所示，在 5G 通信系统中的非直接通信中，基于层 3 (对于 IP 类型的 PDU 会话，中继终端设备基于 IP 地址转发数据) 的非直接通信连接建立流程包括：

S201、远端终端设备和中继终端设备分别注册到网络，并从网络侧获取授权信息。

对于远端终端设备，获取的授权信息包括：

指示信息，用于指示是否授权通过中继终端设备接入 5GC。

用于临近业务中继发现 (ProSe Relay Discovery) 的参数，这些参数用于使能与中继终端设备建立连接，包括例如中继服务码 (relay service code)、PDU 会话参数 (例

如数据网络名称 (data network name, DNN)、单网络切片选择辅助信息 (single network slice selection assistance information, S-NSSAI)、接入类型偏好、PDU 会话类型、会话和业务连续性模式)。

5 基于中继服务码的用于临近业务中继发现 (ProSe Relay Discovery) 的安全相关内容。

对于中继终端设备, 获取的授权信息包括:

作为中继终端设备的授权策略, 包括授权为远端终端设备提供中继业务的公共陆地移动网络 (public land mobile network, PLMN)。

10 用于临近业务中继发现 (ProSe Relay Discovery) 的参数, 包括: 指示信息, 用于指示授权作为 UE 与网络之间的中继 (UE-to-Network relay); 中继服务码、PDU 会话参数 (例如 DNN、S-NSSAI、接入类型偏好、PDU 会话类型、会话和业务连续性模式)。

基于中继服务码的用于临近业务中继发现 (ProSe Relay Discovery) 的安全相关内容。

S202、中继终端设备建立 PDU 会话。

15 该会话可以是专为远端终端设备服务的 PDU 会话; 对于 IP 类型的 PDU 会话, 网络侧 SMF 网元为 PDU 会话分配 IP 地址 (可以为 IPv4 地址或 IPv6 前缀等), 中继终端设备利用该 PDU 会话为远端终端设备传输数据。

该步骤是可选的。

S203、远端终端设备通过中继发现流程发现中继终端设备。

20 S204、远端终端设备与中继终端设备建立 PC5 通信链接。

如果中继终端设备已经建立的 PDU 会话不能满足远端终端设备的会话需求 (如 DNN、S-NSSAI 等), 中继终端设备为远端终端设备建立新的 PDU 会话, 该 PDU 会话用于远端终端设备与应用服务器之间的传输数据。或者若中继终端设备未建立用于传输远端终端设备的业务的 PDU 会话, 则会建立新的 PDU 会话, 该 PDU 会话用于远

25 端终端设备与应用服务器之间的传输数据。

S205、中继终端设备为远端终端设备分配用于 PC5 通信的 IP 地址。

S206、中继终端设备将远端终端设备的 ID 和 IP 信息 (IP info) 发送给 AMF 网元和 SMF 网元。

该 IP 信息是中继终端设备为远端终端设备分配的用于网络侧通信的地址。

30 该步骤可以通过 PDU 会话修改流程进行。例如, 若 SMF 网元为中继终端设备分配 IP 地址为 IPv4, 则 IP 信息表示为特定的端口号 (TCP/UDP port), 意味着中继终端设备利用该 IPv4 地址和该特定的端口号传输远端终端设备的数据。若 SMF 网元为中继终端设备分配的 IP 地址为 IPv6 前缀 (IPv6 prefix), 则 IP 信息表示为更长的 IPv6 前缀, 意味着中继终端设备利用更长的 IPv6 前缀传输远端终端设备的数据。

35 S207、中继终端设备根据 IP 地址转发远端终端设备的上下行数据。

例如, 远端终端设备在 PC5 通信链路上使用的 IP 地址为 IP3, 中继终端设备的 PDU 会话对应的 IP 地址为 IP1, 中继终端设备为远端终端设备分配的 IP 信息 (IP info) 为 IP1-1。则远端终端设备利用 IP3 向服务器传输数据, 服务器利用 IP1-1 向远端终端设备传输数据, 中继终端设备要绑定 IP3 和 IP1-1 的关联关系。

在下行方向，中继终端设备从 UPF 网元接收到 IP1-1 数据包，获知数据为远端终端的，再修改 IP 地址为 IP3，通过 PC5 链路发送给远端终端设备。

在上行方向，中继终端设备接收到 IP3 数据包后，再修改 IP 地址为 IP1-1，通过 PDU 会话发送给 UPF 网元，进而发送到服务器。

- 5 在上述非直接通信连接建立过程中，为了保证通信的安全，远端终端设备和中继终端设备之间需要建立安全连接，即远端终端设备和中继终端设备之间传输的数据被加密保护和/或完整性保护。由于非直接通信连接是按需动态建立的，远端终端设备和中继终端设备之间无法预配置共享的安全信息（例如密钥），进而基于预配置的共享安全信息建立远端终端设备和中继终端设备之间的安全连接。因此需要动态建立远端终端设备和中继终端设备之间的共享安全信息（例如密钥）。
- 10

本申请实施例提供了一种密钥获取方法，如图 3 所示，包括：

S301、远端终端设备接入 3GPP 网络并获取中继发现和密钥素材；中继终端设备接入 3GPP 网络并获取发现和密钥素材。

S302、远端终端设备通过 AMF 网元向 AUSF 网元发送密钥请求。

- 15 该密钥请求中包括临近业务远端接入指示、5G 全球唯一临时标识（globally unique temporary identity, GUTI）或用户隐藏标识（subscription concealed identifier, SUCI）。

S303、AUSF 网元向 UDM 网元发送认证请求。

该认证请求中包括临近业务远端接入指示、5G-GUTI 或 SUCI。

S304、UDM 网元向 AUSF 网元发送认证响应。

- 20 该认证响应中包括用户的永久身份标识（subscription permanent identifier, SUPI）。

S305、AUSF 网元使用最新的远端终端设备与 AUSF 网元之间共享的密钥（Kausf）生成根密钥（REAR Key）。

S306、AUSF 网元向远端终端设备发送密钥响应。

该密钥响应中包括根密钥和中继终端设备的标识。

- 25 S307、远端终端设备发现中继终端设备。

S308、远端终端设备向中继终端设备发送直接通信请求。

该直接通信请求中包括中继服务码、5G-GUTI 和消息验证码（message authentication code, MAC）。

S309、中继终端设备向 AUSF 网元发送密钥请求。

- 30 该密钥请求中包括中继服务码、5G-GUTI 和 MAC。

S310、AUSF 网元执行认证和授权检查。

S311、授权之后，AUSF 网元生成远端终端设备的密钥 K_{NR_ProSe} 。

- 35 $K_{NR_ProSe} = KDF$ （根密钥 REAR 密钥, 5G-GUTI, 中继服务码或服务标识, 新鲜性参数, 其他可能的参数）。其中，密钥推演函数（key derivation function, KDF）是一种生成密钥的算法。

S312、AUSF 网元向中继终端设备发送密钥响应。

该密钥响应中包括 K_{NR_ProSe} 和新鲜性参数。

S313、中继终端设备向远端终端设备发送直接安全模式命令。

该直接安全模式命令中包括生成 K_{NR_ProSe} 的新鲜性参数。

S314、远端终端设备根据直接安全模式命令生成密钥 K_{NR_ProSe} 。

S315、远端终端设备根据直接安全模式命令向中继终端设备发送直接安全模式命令完成消息。

该方案中，密钥推演过程中使用了中继终端设备的标识，但是由于存在一个或多个终端设备能够提供中继服务，在远端终端设备发现中继终端设备之前，网络无法获取提供中继服务的终端设备的标识，因此无法推演对应的密钥。此外，未定义推演密钥的 AUSF 网元如何确定，也未定义中继终端设备如何发现远端终端设备推演密钥的 AUSF 网元。若中继终端设备任意选择 AUSF 网元，如果该 AUSF 网元未存储远端终端设备获取的密钥，则无法验证远端终端设备生成的 MAC。

10 本申请实施例提供了一种密钥获取方法，如图 4 所示，包括：

S401、远端终端设备和中继终端设备分别获取发现密钥素材。

具体的，包括：

远端终端设备与临近业务（ProSe）功能网元交互以获取中继发现参数和临近业务密钥管理功能（ProSe key management function, PKMF）网元的地址。

15 远端终端设备从中继的 PKMF 网元获取发现密钥素材。

中继终端设备与临近业务（ProSe）功能网元交互以获取中继发现参数和 PKMF 网元的地址。

中继终端设备从 PKMF 获取网元发现密钥素材。

S402、远端终端设备向 PKMF 网元发送密钥请求。

20 该密钥请求中包括指示信息，用于请求中继通信密钥。可选的包括之前获取的密钥的密钥标识——临近业务中继用户密钥（ProSe relay user key, PRUK）ID。

相应地，PKMF 网元向远端终端设备发送响应消息，该响应消息中包括 PRUK 和对应的 PRUK Id。

S403、远端终端设备发现中继终端设备。

25 S404、远端终端设备向中继终端设备发送直接通信请求。

该直接通信请求中包括 PRUK ID 或国际移动用户识别码（international mobile subscriber identity, IMSI）中的一个、中继服务码。

S405、中继终端设备向 PKMF 网元发送密钥请求。

该密钥请求中包括 PRUK ID 或 IMSI 中的一个、中继服务码和第一随机数。

30 S406、PKMF 网元根据 PRUK ID 或 IMSI 识别终端设备，并执行授权检查。

授权检查通过后，PKMF 网元确定远端终端设备是否需要新的 PRUK。若需要，PKMF 网元与归属用户服务器（home subscriber server, HSS）网元交互以获取用户的通用引导信息（generic bootstrapping information, GPI）（通用引导架构（generic bootstrapping architecture, GBA）推送信息（Push Info）、GBA 推送信息）或认证向
35 量。

S407、PKMF 网元向中继终端设备发送密钥响应。

该密钥响应中包括密钥 K_d 、生成密钥 K_d 的随机数、GPI、远端终端设备标识。

S408、中继终端设备向远端终端设备发送直接安全模式命令。

该直接安全模式命令中包括生成密钥 K_d 的随机数、GPI。

相应地，远端终端设备向中继终端设备发送直接安全模式完成。

该方案是基于 4G 通信系统的，密钥的推演基于 GBA 机制，当前 5G 不支持 GBA 机制。远端终端设备在与中继终端设备通信时可能会使用用户的永久身份标识（即 IMSI），这可能会造成用户隐私被泄露。

5 为此，本申请实施例提供了另一种密钥获取方法，一方面，通过使用远端终端设备与 3GPP 网络之间建立共享的密钥，使得远端终端设备和中继终端设备建立通信的根密钥。另一方面，通过使用远端终端设备的临时标识或匿名标识 SUCI 来获取根密钥，保证了用户隐私的情况下，使得中继终端设备能够获得用于建立 PC5 接口安全的根密钥。

10 本申请实施例中，远端 AUSF 网元指服务远端终端设备的 AUSF 网元，远端 AUSF 网元存储有与远端终端设备共享的密钥。中继 AUSF 网元指服务中继终端设备的 AUSF 网元。远端 AMF 网元指服务远端终端设备的 AMF 网元，中继 AMF 网元指服务中继终端设备的 AMF 网元。远端 PCF 网元指服务远端终端设备的 PCF 网元，中继 PCF 网元指服务中继终端设备的 PCF 网元。远端 NRF 网元指服务远端终端设备的 NRF 网元。

15 远端 UDM 网元指服务远端终端设备的 UDM 网元。

本申请实施例中，如无特别说明，根据参数 A 生成某一标识、某一密钥或某一验证信息，指的是向某种算法（例如密钥推演函数（key derivation function, KDF）输入参数 A，计算得到某一标识、某一密钥或某一验证信息。

PKMF 网元为新的功能模块，可以独立部署或其他功能网元合设。PKMF 网元用于管理临近业务的安全信息，例如获取远端终端设备与中继终端设备之间的共享的密钥，执行授权检查等功能。

如图 5 所示，在终端侧该密钥获取方法包括：

S501、远端终端设备向中继终端设备发送远端终端设备的第一标识和中继服务码。

可选的，远端终端设备向中继终端设备发送第一验证信息。

25 可选的，远端终端设备向中继终端设备发送第二验证信息。

上述信息可以携带在同一消息（例如直接通信请求）或不同消息中，由中继终端设备最终转发给远端 AUSF 网元、中继 AUSF 网元或 PKMF 网元。

下面对涉及的几个信息进行说明：

中继服务码

30 用于标识一个连接服务，该连接服务为中继提供连接到应用的服务。同一个终端设备可以配置不同的中继服务码，用于接入到不同的应用或业务。

第一标识

第一标识可以为远端终端设备的与中继服务码对应的标识（例如 P-KID）（例如格式可以是 Username@realm），或者，第一标识可以为远端终端设备的匿名标识（例如 SUCI），从而在空口传递时不会暴露远端终端设备的永久身份标识（例如 SUPI）。第一标识可以与中继服务码一一对应，即针对不同的中继服务码远端终端设备可以使用不同的第一标识进行通信。

由于 AUSF 网元或 PKMF 网元可以服务多个终端设备，远端终端设备的第一标识用于 AUSF 网元或 PKMF 网元确定对应的远端终端设备，从而确定对应的第一共享密

钥, 或者, 确定远端终端设备的其他标识 (例如 SUPI), 第一共享密钥为远端终端设备与远端 AUSF 网元共享的密钥 (或由该密钥生成的其他密钥)。第一共享密钥可以是 Kausf, 该密钥 Kausf 由远端终端设备接入网络时与远端 AUSF 网元事先协商共享。或者, 第一共享密钥可以为根据 Kausf 进一步推演的用于临近业务通信的密钥。

- 5 对于第一标识为远端终端设备的与中继服务码对应的标识来说, 远端终端设备可以通过以下几种方式获取第一标识:

方式一、远端终端设备可以通过远端 AMF 网元向远端认证服务功能网元发送至少一个中继服务码; 远端 AUSF 网元生成与中继服务码对应的第一标识, 并通过远端 AMF 网元向远端终端设备发送第一标识; 相应地, 远端终端设备从远端认证服务功能
10 网元接收与中继服务码对应的第一标识。

方式二、远端终端设备根据第一共享密钥 (例如 Kausf)、中继服务码生成临时标识, 再根据临时标识获取第一标识。

远端终端设备根据第一共享密钥 (例如 Kausf)、中继服务码生成临时标识的方式包括:

- 15 在一种可能的实施方式中, 向某种算法 (例如密钥推演函数 (key derivation function, KDF) 输入第一共享密钥 (例如 Kausf) 和中继服务码, 计算得到一个临时标识。

可选的, 远端终端设备还可以根据第二新鲜性参数、远端终端设备的 SUPI 中的至少一个, 以及, 第一共享密钥 (例如 Kausf)、中继服务码生成临时标识。即计算上述临时标识的输入参数还可以包括第二新鲜性参数或其他参数 (例如远端终端设备的
20 SUPI 等)。

或者, 在另一种可能的实施方式中, 远端终端设备根据第一共享密钥生成临近业务根密钥, 再根据临近业务根密钥和中继服务码生成临时标识。

例如, 远端终端设备首先根据第一共享密钥 (例如 Kausf) 推演一个临近业务根密钥。可选的, 生成临近业务根密钥的算法的输入参数可以包含字符串 “ProSe”、远
25 端终端设备的 SUPI 等。然后, 远端终端设备使用临近业务根密钥和中继服务码作为 KDF 的输入生成临时标识。

可选的, 远端终端设备还可以根据第二新鲜性参数、远端终端设备的 SUPI 中的至少一个, 以及, 临近业务根密钥、中继服务码生成临时标识。即计算上述临时标识的输入参数还可以包括第二新鲜性参数或其他参数 (例如远端终端设备的 SUPI 等)。
30 即远端终端设备根据临时标识获取第一标识的方式包括:

在一种可能的实施方式中, 远端终端设备根据上述临时标识、路由指示和远端终端设备的家乡网络标识生成第一标识, 第一标识可以包括路由指示和家乡网络标识。例如, 可以对临时标识、路由指示和远端终端设备的家乡网络标识进行组合得到字符串作为临时标识, 以第一标识的格式为 Username@realm 为例, 第一标识
35 Username@realm 中的 Username 可以包括临时标识和路由指示, realm 可以包括远端终端设备的家乡网络标识。

或者, 在另一种可能的实施方式中, 远端终端设备将上述临时标识作为第一标识。

方式三、远端终端设备根据第二新鲜性参数、路由指示和远端终端设备的家乡网络标识生成第一标识, 第一标识可以包括路由指示和家乡网络标识。例如, 可以对第

二新鲜性参数、路由指示和远端终端设备的家乡网络标识进行组合得到字符串作为临时标识,以第一标识的格式为 Username@realm 为例,第一标识 Username@realm 中的 Username 可以包括第二新鲜性参数和路由指示, realm 可以包括远端终端设备的家乡网络标识。

- 5 方式四、远端终端设备根据第一共享密钥(例如 Kausf)和中继服务码生成第二共享密钥,第二共享密钥为远端终端设备与 PKMF 网元共享的密钥 Kp;远端终端设备再根据第二共享密钥 Kp 和第二新鲜性参数生成第一标识。

生成第一标识的过程中,使用中继服务码是为了生成基于中继服务码粒度的密钥,保证不同的中继服务码(业务)对应不同的临时标识,从而防止攻击者在空口根据相同的第一标识关联一个终端设备正在进行的两个不同的业务。

生成第一标识的过程中,使用第二新鲜性参数是为了保证不同的时刻针对同一个中继服务码,当没有发生新的主认证生成新的密钥(例如 Kausf)时,网络可以生成不同的临时标识,从而防止攻击者根据空口上的同一个第一标识关联一个终端设备在不同的时刻进行同一个业务。

15 **第二新鲜性参数**

第二新鲜性参数可以包括远端终端设备和远端 AUSF 网元分别本地维护的计数器的值,远端终端设备和远端 AUSF 网元在本地维护各自的计数器时,采用相同的初始值和计数规则,以使这两个计数器的值保持一致。此时,远端 AUSF 网元不必向远端终端设备发送第二新鲜性参数。

- 20 或者,远端终端设备可以向远端 AUSF 网元发送中继服务码;远端 AUSF 网元针对该中继服务码,根据第二新鲜性参数生成第一标识,并向远端终端设备发送第二新鲜性参数;相应地,远端终端设备从远端 AUSF 网元接收与中继服务码对应的第二新鲜性参数。第二新鲜性参数可以包括远端 AUSF 网元生成的随机值或者远端 AUSF 网元本地维护的计数器的值,具体生成方式不作限定。

25 **第一验证信息**

第一验证信息由第一临时密钥,以及,携带第一验证信息的信息(例如直接通信请求)的全部或部分信元生成。第一临时密钥由第一共享密钥(例如 Kausf)生成。具体的可以直接根据 Kausf 推演第一临时密钥,或根据 Kausf 推演一个中间密钥,基于中间密钥进一步推演第一临时密钥。

- 30 可选的,第一临时密钥由中继服务码、第三新鲜性参数、远端终端设备的第二标识(例如 SUPI)以及第一标识中的至少一项,以及,第一共享密钥(例如 Kausf)计算得到。其中,第三新鲜性参数为远端终端设备生成,例如可以为第三随机数。例如,输入中继服务码、第三新鲜性参数、远端终端设备的第二标识以及远端终端设备的第一标识中的至少一个,以及,第一共享密钥(例如 Kausf),通过某种算法计算得到
- 35 第一临时密钥 Kt。

第一验证信息用于发送给远端 AUSF 网元,远端 AUSF 网元接收第一验证信息后,按照与远端终端设备相同的方式生成第三验证信息,远端 AUSF 网元比较第一验证信息和第三验证信息以对远端终端设备进行验证,验证是否授权远端终端设备通过中终端设备接入网络获取业务。

第二验证信息

第二验证信息由第一新鲜性参数、中继服务码和第一共享密钥（例如 K_{ausf} ）生成。例如，远端终端设备根据中继服务码和第一共享密钥（例如 K_{ausf} ），生成第二共享密钥 K_p ，再根据第一新鲜性参数和第二共享密钥 K_p ，生成第二验证信息。

- 5 可选的，远端终端设备根据远端终端设备的第二标识（例如 $SUPI$ ）、临近业务（ $ProSe$ ）字符中的至少一个、中继服务码和第一共享密钥（例如 K_{ausf} ），生成第二共享密钥 K_p 。或者，远端终端设备根据第一共享密钥（例如 K_{ausf} ）和其他参数，生成第二共享密钥 K_p ，再根据第一新鲜性参数、中继服务码和第二共享密钥 K_p ，生成第二验证信息。

- 10 第二验证信息用于发送给 PKMF 网元，PKMF 网元接收第二验证信息后，按照与远端终端设备相同的方式生成第四验证信息，PKMF 网元比较第二验证信息和第四验证信息以对远端终端设备进行验证，验证是否授权远端终端设备通过中继终端设备接入网络获取业务。

- 15 S502、远端终端设备根据第一共享密钥（例如 K_{ausf} ）、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

例如，使用第一共享密钥（例如 K_{ausf} ）、中继服务码，以及，至少一个第一新鲜性参数，作为密钥推演函数 KDF 的输入，输出远端终端设备与中继终端设备通信的根密钥。

- 20 或者，使用第一共享密钥（例如 K_{ausf} ）作为 KDF 的输入，输出一个中间密钥。进一步地，使用该中间密钥、中继服务码，以及，至少一个第一新鲜性参数等作为 KDF 的输入，输出远端终端设备与中继终端设备通信的根密钥。

远端终端设备也可以根据第一共享密钥（例如 K_{ausf} ）和中继服务码生成第二共享密钥 K_p ，再根据第二共享密钥 K_p 以及至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

- 25 远端终端设备还可以根据第一共享密钥（例如 K_{ausf} ）生成第二共享密钥 K_p ，再根据中继服务码、第二共享密钥 K_p 以及至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

第一新鲜性参数

- 30 可选的，至少一个第一新鲜性参数可以包括远端 AUSF 网元或 PKMF 网元中的一个与终端设备分别本地维护的计数器的值，远端 AUSF 网元或 PKMF 网元中的一个与终端设备在本地维护各自的计数器时，采用相同的初始值和计数规则，以使这两个计数器的值保持一致。可选的，远端 AUSF 网元或 PKMF 网元中的一个与终端设备针对每一个中继服务器码分别维护计数器。

- 35 可选的，至少一个第一新鲜性参数包括第一随机数，可选的，远端终端设备还可以向中继终端设备发送第一随机数。第一随机数最终发往远端 AUSF 网元或 PKMF 网元，相应地，远端 AUSF 网元或 PKMF 网元接收第一随机数。

可选的，至少一个第一新鲜性参数包括第二随机数，远端终端设备还可以从中继终端设备接收第二随机数。第二随机数可以来自远端 AUSF 网元或 PKMF 网元，即远端 AUSF 网元或 PKMF 网元可以发送第二随机数。

本申请实施例提供的密钥获取方法，远端终端设备向中继终端设备发送第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识。远端终端设备根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。其中的第一标识用于远端 AUSF 网元确定对应的第一共享密钥，或者用于 PKMF 网元确定对应的第二共享密钥，而第二共享密钥同样是由第一共享密钥和/或中继服务码生成，使得远端终端设备与远端 AUSF 网元或 PKMF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

如图 6 所示，在网络侧该密钥获取方法由远端 AUSF 网元执行的步骤包括：

- 5 S601、远端 AUSF 网元获取远端终端设备的第一标识或第二标识中的一个，以及，中继服务码。

可选的，远端 AUSF 网元接收第一随机数。

可选的，远端 AUSF 网元还可以接收第一验证信息。关于第一验证信息参照前面描述，在此不再重复。

- 15 如前文所述的，第二标识可以为远端终端设备的永久身份标识（例如 SUPI），第一标识可以为远端终端设备的与中继服务码对应的标识（例如 P-KID）。

远端 AUSF 网元可以接收来自远端终端设备的中继服务码，中间通过例如远端 AMF 网元、中继终端设备、PKMF 网元等转发。关于中继服务码见前面描述，在此不再重复。

- 20 远端 AUSF 网元获取远端终端设备的第一标识或第二标识中的一个，包括以下几种方式：

在一种可能的实施方式中，远端 AUSF 网元接收远端终端设备的第一标识或第二标识中的一个。例如远端 AUSF 网元可以从 PKMF 网元接收远端终端设备的第一标识或第二标识中的一个。

- 25 在远端 AUSF 网元接收远端终端设备的第一标识的情况下，该方法还包括：远端 AUSF 网元可以采用步骤 S501 中与远端终端设备相同的方式（例如方式二、方式三），生成第一标识。

在另一种可能的实施方式中，远端 AUSF 网元可以采用步骤 S501 中与远端终端设备相同的方式（例如方式二、方式三），生成第一标识。

- 30 例如，远端 AUSF 网元可以根据第一共享密钥、中继服务码，生成临时标识；再根据临时标识生成第一标识。具体可以参照前面步骤 S501 的方式二中远端终端设备如何生成第一标识。

- 与远端终端设备类似的，远端 AUSF 网元根据第一共享密钥、中继服务码，生成临时标识，可以包括：远端终端设备根据第一共享密钥、中继服务码和第二新鲜性参数，生成临时标识。具体可以参照前面步骤 S501 的方式二中远端终端设备如何生成临时标识。

再例如，远端 AUSF 网元可以根据第二新鲜性参数、路由指示和远端终端设备的家乡网络标识，生成第一标识。具体可以参照前面步骤 S501 的方式三中远端终端设备如何生成第一标识。关于第二新鲜性参数见前面描述，在此不再重复。

另外，远端 AUSF 网元可以发送第二新鲜性参数，通过中继终端设备转发至远端终端设备，使远端终端设备接收第二新鲜性参数。

远端 AUSF 网元在生成第一标识之后，可以向中继终端设备发送与中继服务码对应的第一标识，由中继终端设备转发给远端终端设备，使得远端终端设备获取第一标识，即对应于步骤 S501 中远端终端设备获取第一标识的方式一。

远端 AUSF 网元还可以向 UDM 网元发送第一标识，用于其他网元（例如 PKMF 网元）从 UDM 网元获取远端 AUSF 网元实例标识和/或远端终端设备的 SUPI。远端 AUSF 网元实例标识用于确定服务远端终端设备的远端 AUSF 网元。

S602、远端 AUSF 网元获取第一标识或第二标识对应的第一共享密钥。
关于第一共享密钥见前面描述，在此不再重复。

远端 AUSF 网元可以通过本地查询第一标识或第二标识对应的第一共享密钥。

S603、远端 AUSF 网元根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

关于第一新鲜性参数的描述见前面描述，在此不再重复。需要说明的是，此处的第一新鲜性参数可以是远端终端设备和远端 AUSF 网元各自在本地维护的计数器的值。

远端 AUSF 网元可以采用与远端终端设备相同的方式来生成根密钥，具体参照步骤 S502 中的相关描述，在此不再重复。

远端 AUSF 网元接收到第一验证信息之后，在生成根密钥之前，与远端终端设备类似地，可以根据第一共享密钥生成第一临时密钥；并根据第一临时密钥，以及，携带第一验证信息的消息的全部或部分信元，得到第三验证信息；通过比较第一验证信息和第三验证信息以对远端终端设备进行验证，验证通过即可以生成根密钥。关于远端 AUSF 网元如何进行验证可以参照前面关于第一验证信息的描述，在此不再重复。

同样地，与远端终端设备类似地，远端 AUSF 网元可以根据中继服务码、第三新鲜性参数、第二标识以及远端终端设备的第一标识中的至少一项，以及，第一共享密钥，生成第一临时密钥。具体参照远端终端设备的相关描述，在此不再重复。

可选的，远端 AUSF 网元按照与远端终端设备相同的方式生成第二共享密钥 Kp。例如，根据中继服务码和第一共享密钥（例如 Kausf），生成第二共享密钥 Kp，并向 PKMF 网元发送第二共享密钥 Kp。具体参照前文远端终端设备生成第二共享密钥 Kp 的方式。

S604、远端 AUSF 网元发送根密钥。

远端 AUSF 网元可以向 PKMF 网元发送根密钥，通过 PKMF 网元向中继终端设备发送根密钥。

可选的，远端 AUSF 网元还可以发送生成根密钥的至少一个第一新鲜性参数。例如，至少一个第一新鲜性参数包括第二随机数，远端 AUSF 网元可以发送第二随机数，经过中继远端设备转发给远端终端设备。

本申请实施例提供的密钥获取方法，远端 AUSF 网元获取远端终端设备的第一标识或第二标识中的一个，以及，中继服务码；第二标识为远端终端设备的永久身份标识，第一标识为远端终端设备的与中继服务码对应的标识；远端 AUSF 网元获取第一标识或第二标识对应的第一共享密钥；第一共享密钥为远端终端设备与远端 AUSF 网

元共享的密钥；远端 AUSF 网元根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥；远端 AUSF 发送根密钥。其中的第一标识用于远端 AUSF 网元确定对应的第一共享密钥，使得远端终端设备和远端 AUSF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

如图 7 所示，在网络侧该密钥获取方法由 PKMF 网元执行的步骤包括：

S701、PKMF 网元接收远端终端设备的第一标识和中继服务码。

可选的，PKMF 网元接收第一随机数。

可选的，PKMF 网元接收第二验证信息。关于第二验证信息见前面描述，在此不再重复。

第一标识可以为远端终端设备的与中继服务码对应的标识（例如 P-KID），或者，第一标识可以为远端终端设备的匿名标识（例如 SUCI）。

在一种可能的实施方式中，PKMF 网元可以通过中继终端设备从远端终端设备接收第一标识和中继服务码。

S702、PKMF 网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥。

在一种可能的实施方式中，PKMF 网元向 UDM 网元发送第一标识；相应地从 UDM 网元接收远端 AUSF 的标识信息（例如远端 AUSF 网元实例标识）；PKMF 网元根据标识信息，向对应的远端 AUSF 网元发送第一标识；相应地，从远端 AUSF 网元接收根密钥。

在另一种可能的实施方式中，PKMF 网元向 UDM 网元发送第一标识；相应地，从 UDM 网元接收远端 AUSF 网元的标识信息以及远端终端设备的永久身份标识（例如 SUPI）；PKMF 网元根据标识信息，向对应的远端 AUSF 网元发送远端终端设备的永久身份标识；相应地，从远端 AUSF 网元接收根密钥。

上述两种实施方式对应于步骤 S601 中远端 AUSF 网元获取远端终端设备的第一标识或第二标识中的一个。

在又一种可能的实施方式中，PKMF 网元从远端 AUSF 网元接收至少一个第二共享密钥；PKMF 网元根据第一标识对应的第二共享密钥，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。可选的，PKMF 网元根据中继服务码、第一标识对应的第二共享密钥，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

PKMF 网元接收到第二验证信息之后，在生成根密钥之前，与远端终端设备类似地，可以根据第一新鲜性参数和第二共享密钥，生成第四验证信息；通过比较第一验证信息和第三验证信息以对远端终端设备进行验证，验证通过即可以生成根密钥。PKMF 网元如何进行验证可以参照前面关于第二验证信息的描述，在此不再重复。

关于第一新鲜性参数的描述见前面描述，在此不再重复。需要说明的是，此处的第一新鲜性参数可以是远端终端设备和 PKMF 网元各自在本地维护的计数器的值。

S703、PKMF 网元发送根密钥。

可选的，PKMF 网元还可以发送生成根密钥的至少一个第一新鲜性参数。例如，至少一个第一新鲜性参数包括第二随机数，PKMF 网元可以发送第二随机数，经过中

继远端设备转发给远端终端设备。

本申请实施例提供的密钥获取方法，PKMF 网元接收远端终端设备的第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；PKMF 网元根据第一标识获取远端终端设备与中继终端设备通信的根密钥，根密钥由第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数生成，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；PKMF 网元发送根密钥。其中的第一标识用于 PKMF 网元确定对应的第二共享密钥，使得远端终端设备和 PKMF 网元能够采用相同的方式生成远端终端设备与中继终端设备通信的根密钥，实现了在远端终端设备与中继终端设备之间共享密钥。

本申请实施例提供另一种密钥获取方法，远端终端设备主动向远端 AUSF 网元请求中继服务码对应的第一标识，使得远端 AUSF 网元能够根据中继服务码生成对应的第一标识，该第一标识用于发现远端 UDM 网元，并将生成的第一标识存储在远端 UDM 网元中。在非直接通信过程中，远端终端设备向中继终端设备发起直接通信请求，直接通信请求中包括第一标识。中继终端设备通过信令面向网络侧发起包含第一标识的密钥请求，PKMF 网元通过远端 UDM 网元确定第一标识对应的远端 AUSF 网元，从远端 AUSF 网元获取远端终端设备与中继终端设备通信的根密钥。

如图 8 所示，该密钥获取方法包括：

S801、远端终端设备接入网络，从远端 PCF 网元或其他相关网元获取用于通过中继终端设备通信的信息。

上述信息包括：用于指示是否授权该终端设备通过中继接入 5GC（即该终端设备作为远端终端设备）的指示信息；中继服务码等。

S802、中继终端设备接入网络，从中继 PCF 网元或其他相关网元获取作为中继终端设备提供通信的信息。

上述信息包括：用于指示是否授权该终端设备作为中继的指示信息；中继服务码等。

需要说明的是，步骤 S801 和 S802 的执行顺序不限。

S803、远端终端设备通过远端 AMF 网元向远端 AUSF 网元发送密钥请求。

该密钥请求中包括至少一个中继服务码。

可选的，远端 AMF 网元执行授权检查，检查是否授权远端终端设备作为中继终端设备的远端终端设备或者检查是否授权远端终端设备通过中继终端设备获取中继服务码对应的服务。

S804、远端 AUSF 网元生成远端终端设备的与各个中继服务码对应的第一标识（例如 P-KID）。

生成第一标识的过程参照步骤 S601。

S805、远端 AUSF 网元向远端 UDM 网元发送远端终端设备的第一标识。

远端 UDM 网元将远端终端设备的第一标识作为远端终端设备的上下文存储在本地，可选的，如果远端 UDM 网元将远端终端设备的上下文存储在统一数据存储库（unified data repository, UDR）网元中，则远端终端设备的第一标识也被存储在 UDR 网元的终端设备上下文中。

S806、远端 AUSF 网元通过远端 AMF 网元向远端终端设备发送密钥请求响应。

该密钥请求响应中包括：与中继服务码对应的第一标识，或者，用于生成第一标识的第二新鲜性参数。

相应地，远端终端设备通过远端 AMF 网元从远端 AUSF 网元接收与中继服务码
5 对应的第一标识，或者，用于生成第一标识的第二新鲜性参数。

如果在生成第一标识的过程中使用了第二新鲜性参数，则密钥请求响应中可以包括与中继服务码对应的第一标识，或者，用于生成第一标识的第二新鲜性参数。如果在生成第一标识的过程中未使用第二新鲜性参数，则密钥请求响应中包括与中继服务码对应的第一标识。

10 可选的，如果在接收的密钥请求中包括多个中继服务码，即请求的第一标识也有多个，则密钥请求响应中还可以包括与多个第一标识（或第二新鲜性参数）分别对应的多个中继服务码，即密钥请求响应中第一标识（或第二新鲜性参数）和中继服务码一一对应；或者，密钥请求响应中包括多个第一标识（或第二新鲜性参数），而不与中继服务码相对应，由远端终端设备从中自由选择并进行对应。

15 S807、远端终端设备获取第一标识。

如果在步骤 S806 中接收到第一标识，则远端终端设备直接进行存储。

如果在步骤 S806 中接收到第二新鲜性参数，则远端终端设备采用与远端 AUSF 网元相同的方式生成第一标识，例如按照步骤 S501 中方式二或方式三的方式生成第一标识。需要说明的是，远端终端设备生成第一标识的过程在步骤 S809 之前执行即可。

20 S808、远端终端设备执行发现流程以发现中继终端设备。

S809、远端终端设备向中继终端设备发送直接通信请求。

该直接通信请求中包括远端终端设备的第一标识（例如 P-KID）、中继服务码。如果有多个中继服务码，则远端终端设备可以通过中继服务码确定对应的第一标识。

可选的，该直接通信请求中还可以包括第一随机数（Nonce 1）。

25 可选的，该直接通信请求中还可以包括第一验证信息。

关于如何生成第一验证信息参照步骤 S501。

S810、中继终端设备向中继 AMF 网元发送密钥请求。

该密钥请求中包括第一标识（例如 P-KID）、中继服务码。

可选的，该密钥请求中还可以包括第一随机数。

30 可选的，该密钥请求中还可以包括第一验证信息（例如 MAC-I）。

S811、中继 AMF 网元选择中继 AUSF 网元，并向中继 AUSF 网元发送临近业务密钥请求。

该临近业务密钥请求中包括第一标识（例如 P-KID）、中继服务码、中继终端设备的标识（relay UE ID）（例如 SUPI）。

35 可选的，该临近业务密钥请求中还可以包括第一随机数。

可选的，该临近业务密钥请求中还可以包括第一验证信息（例如 MAC-I）。

可选的，中继 AMF 网元执行授权检查，即检查是否授权中继终端设备作为中继终端设备或者检查是否授权中继终端设备向远端终端设备提供中继服务码对应的连接服务。

S812、中继 AUSF 网元选择 PKMF 网元,并向 PKMF 网元发送临近业务密钥请求。

临近业务密钥请求中携带的信息与步骤 S811 的临近业务密钥请求中携带的信息相同。

- 5 S813、PKMF 网元根据临近业务密钥请求中的第一标识(例如 P-KID)选择远端 UDM 网元,并向远端 UDM 网元发送网元发现请求。

该网元发现请求中包括第一标识(例如 P-KID)。

远端 UDM 网元根据第一标识(例如 P-KID)获取远端 AUSF 网元实例标识,并发送给 PKMF 网元。AUSF 网络实例标识可以为全量域名(fully qualified domain name, FQDN)或 AUSF 的地址等能唯一识别远端 AUSF 的标识,这里不做限制。

- 10 可选的,PKMF 网元还可以获取远端终端设备的第二标识(例如 SUPI)。

S814、PKMF 网元对远端终端设备和中继终端设备进行授权。

若步骤 S813 中 PKMF 网元获取了远端终端设备的第二标识,PKMF 网元根据远端终端设备的第二标识(例如 SUPI)和中继服务码判断是否授权远端终端设备通过中继终端设备获取中继服务码对应的服务。

- 15 PKMF 网元根据中继终端设备的标识(relay UE ID,例如 SUPI)和中继服务码判断是否授权中继终端设备作为中继提供中继服务码对应的服务。授权通过则继续执行后续流程,否则发起拒绝流程。

需要说明的是,上述 PKMF 的授权过程是可选的,并且可以发生在步骤 S815 之后。

- 20 S815、PKMF 网元向远端 AUSF 网元发送临近业务密钥请求。

该临近业务密钥请求中包括远端终端设备的第二标识(例如 SUPI)或第一标识、中继服务码。

可选的,该临近业务密钥请求中还可以包括第一随机数。

可选的,该临近业务密钥请求中还可以包括第一验证信息(例如 MAC-I)。

- 25 S816、远端 AUSF 网元根据第一共享密钥、中继服务码,以及,至少一个第一新鲜性参数,生成远端终端设备与中继终端设备通信的根密钥。

- 30 此处的至少一个第一新鲜性参数可以包括第一随机数(Nonce 1),或者,可以包括远端 AUSF 网元生成的第二随机数(Nonce 2),或者,包括第一随机数和第二随机数,或者,可以包括远端 AUSF 网元本地维护的计数器的值,远端 AUSF 网元本地维护的计数器与远端终端设备本地维护的计数器采用相同的初始值和计数规则,以使这两个计数器的值保持一致。具体的第一新鲜性参数的实现方式不限制。

生成根密钥的过程参照步骤 S603。

- 35 需要说明的是,如果临近业务密钥请求中包括第一验证信息,远端 AUSF 网元按照与终端设备相同的方式生成第三验证信息,通过对比第一验证信息和第三验证信息来进行验证。验证通过后再生成根密钥。

S817、远端 AUSF 网元向 PKMF 网元发送临近业务密钥响应。

该临近业务密钥响应中可以包括根密钥,可选的,还可以包括第二随机数。

S818、PKMF 网元向中继 AUSF 网元发送临近业务密钥响应。

该临近业务密钥响应中可以包括根密钥,可选的,还可以包括第二随机数。

S819、中继 AUSF 网元通过中继 AMF 网元向中继终端设备发送临近业务密钥响应。

该临近业务密钥响应中可以包括根密钥，可选的，还可以包括第二随机数。

S820、中继终端设备向远端终端设备发送安全模式命令。

5 可选的，该安全模式命令中包括第二随机数。

可选的，中继终端设备产生第四随机数，并在安全模式命令消息中包括该第四随机数。

远端终端设备采用与远端 AUSF 网元相同的方法生成根密钥。

10 可选的，中继终端设备可以根据接收到的根密钥生成中继终端设备与远端终端设备之间的会话密钥。进一步可选的，中继终端设备可以根据该会话密钥生成信令面和/或用户面的加密密钥和/或完整性保护密钥。

或者，可选的，中继终端设备可以根据接收到的根密钥生成信令面和/或用户面的加密密钥和/或完整性保护密钥。

15 可选的，安全模式命令消息中包括消息验证码，消息验证码为根据信令面的完整性保护密钥生成。

S821、远端终端设备向中继终端设备发送安全模式命令完整消息。

20 上述密钥获取方法中，远端终端设备获取与中继服务码对应的第一标识，通过该第一标识，使得中继终端设备能够通过信令面从网络侧获取远端终端设备与中继终端设备通信的根密钥。可选的，PKMF 网元在获取根密钥之前先对远端终端设备和中继终端设备执行授权检查，保证只有授权的终端设备获取根密钥。其中，根密钥是根据第一共享密钥 Kausf 和中继服务码等参数生成。

25 本申请实施例提供另一种密钥获取方法，远端终端设备主动向远端 AUSF 网元请求中继服务码对应的第一标识，使得远端 AUSF 网元能够根据中继服务码生成对应的第一标识以及第二共享密钥，并发送给 PKMF 网元。在非直接通信过程中，远端终端设备向中继终端设备发起直接通信请求，直接通信请求中包括第一标识。中继终端设备通过信令面向网络侧发起包含第一标识的密钥请求，PKMF 网元根据第一标识获取对应的第二共享密钥 Kp，并生成远端终端设备与中继终端设备通信的根密钥。与图 8 的区别在于，远端 AUSF 网元将远端终端设备的第一标识和第二共享密钥 Kp 提前推送给 PKMF 网元。或者远端 AUSF 网元将第二共享密钥 Kp 提前推送给 PKMF 网元，
30 由 PKMF 生成远端终端设备的第一标识。

如图 9 所示，该密钥获取方法包括：

S901、远端终端设备接入网络，从远端 PCF 网元或其他相关网元获取用于通过中继终端设备通信的信息。

该步骤与步骤 S801 相同，在此不再重复。

35 S902、中继终端设备接入网络，从中继 PCF 网元或其他相关网元获取作为中继终端设备提供通信的信息。

该步骤与步骤 S802 相同，在此不再重复。

S903、远端终端设备通过远端 AMF 网元向远端 AUSF 网元发送密钥请求。

该步骤与步骤 S803 相同，在此不再重复。

S904、远端 AUSF 网元生成第二共享密钥 Kp。

生成第二共享密钥 Kp 的过程参照步骤 S603。

可选的，远端 AUSF 网元生成终端设备的与各个中继服务码对应的第一标识（例如 P-KID）。生成第一标识的过程参照步骤 S601。

- 5 S905、远端 AUSF 网元选择 PKMF 网元，并向 PKMF 网元发送临近业务信息提供消息。

远端 AUSF 网元选择 PKMF 网元的方式包括但不限于以下几种可能的方式：

- 方式一、远端 AUSF 网元根据中继服务码确定 PKMF 网元，例如远端 AUSF 网元向远端 NRF 网元或远端 PCF 网元发送中继服务码，以获取该中继服务码对应的 PKMF 网元。或者中继服务码中包括路由信息，远端 AUSF 网元根据路由信息选择 PKMF 网元。
- 10

方式二、远端终端设备在密钥请求中包括 PKMF 网元的发现信息（在步骤 S901 中从远端 PCF 网元或其他相关网元得到该信息），并由远端 AMF 网元转发给远端 AUSF 网元。

- 方式三、远端 AMF 网元在密钥请求中包括 PKMF 网元的发现信息（在步骤 S901 中从远端 PCF 网元或其他相关网元得到该信息）。
- 15

上述 PKMF 网元的发现信息用于 AUSF 网元确定 PKMF 网元，PKMF 网元的发现信息可以为路由信息或 PKMF 网元的地址信息或 PKMF 网元的标识等。

- 临近业务信息提供消息中包括远端终端设备的第二标识（例如 SUPI）、第二共享密钥 Kp，可选的，还可以包括中继服务码、远端终端设备的第一标识。
- 20

PKMF 网元存储接收到的远端终端设备的第二标识（例如 SUPI）、远端终端设备的第一标识（若接收到）、第二共享密钥 Kp，可选的，还可以存储中继服务码。

可选的，PKMF 网元可以在判断授权远端终端设备获取中继服务码之后才存储上述信息。

- 可选的，若临近业务信息提供消息中不包含第一标识，则由 PKMF 网元生成第一标识。这种情况下，可选的，PKMF 网元向远端 AUSF 网元发送生成的第一标识或第二新鲜性参数。
- 25

S906、远端 AUSF 网元通过远端 AMF 网元向远端终端设备发送密钥请求响应。

该步骤与步骤 S806 相同。

- S907、远端终端设备获取第一标识。
- 30

该步骤与步骤 S807 相同。需要说明的是，远端终端设备生成第一标识的过程在步骤 S909 之前执行即可。

S908、远端终端设备执行发现流程以发现中继终端设备。

该步骤与步骤 S808 相同。

- S909、远端终端设备向中继终端设备发送直接通信请求。
- 35

该步骤与步骤 S809 的区别在于远端终端设备可以生成第二验证信息而不是第一验证信息，生成第二验证信息的过程参照步骤 S501。并且直接通信请求中可选的包括第二验证信息，而不是包括第一验证信息。其他内容相同。

S910、中继终端设备向中继 AMF 网元发送密钥请求。

该步骤与步骤 S810 的区别在于密钥请求中可选的包括第二验证信息,而不是包括第一验证信息。其他内容相同。

S911、中继 AMF 网元选择中继 AUSF 网元,并向中继 AUSF 网元发送临近业务密钥请求。

- 5 该步骤与步骤 S811 的区别在于临近业务密钥请求中可选的包括第二验证信息,而不是包括第一验证信息。其他内容相同。

S912、中继 AUSF 网元选择 PKMF 网元,并向 PKMF 网元发送临近业务密钥请求。

- 10 该步骤与步骤 S812 的区别在于中继 AUSF 网元选择 PKMF 网元的方式与步骤 S905 中远端 AUSF 网元选择 PKMF 网元的方式相同;另外,临近业务密钥请求中可选的包括第二验证信息,而不是包括第一验证信息。其他内容相同。

S913、PKMF 网元对远端终端设备和中继终端设备进行授权。

该步骤与步骤 S814 相同。该步骤是可选的。

S914、PKMF 网元根据第二共享密钥 Kp,以及,至少一个第一新鲜性参数,生成远端终端设备与中继终端设备通信的根密钥。

- 15 此处的第一新鲜性参数可以包括第一随机数 (Nonce 1),或者,可以包括 PKMF 生成的第二随机数 (Nonce 2),或者,包括第一随机数和第二随机数,或者,可以包括远端终端设备和 PKMF 网元分别本地维护的计数器的值,远端终端设备和 PKMF 网元在本地维护各自的计数器时,采用相同的初始值和计数规则,以使这两个计数器的值保持一致。

- 20 生成根密钥的过程参照步骤 S702。

需要说明的是,如果该临近业务密钥请求中包括第二验证信息,PKMF 网元按照与终端设备相同的方式生成第四验证信息,通过对比第二验证信息和第四验证信息来进行验证。验证通过后再生成根密钥。

需要说明的是,上述验证过程与步骤 S913 的执行顺序不限。

- 25 S915、PKMF 网元向中继 AUSF 网元发送临近业务密钥响应。

该步骤与步骤 S818 相同。

S916、中继 AUSF 网元通过中继 AMF 网元向中继终端设备发送临近业务密钥响应。

该步骤与步骤 S819 相同。

- 30 S917、中继终端设备向远端终端设备发送安全模式命令。

该步骤与步骤 S820 相同。

S918、远端终端设备向中继终端设备发送安全模式命令完整消息。

该步骤与步骤 S821 相同。

- 35 上述密钥获取方法中,远端终端设备获取与中继服务码对应的第一标识,通过该第一标识,使得中继终端设备能够通过信令面从网络侧获取远端终端设备与中继终端设备通信的根密钥。进一步的,PKMF 网元在获取根密钥之前先对远端终端设备和中继终端设备执行授权检查,保证只有授权的终端设备获取根密钥。其中,根密钥是根据第一共享密钥 Kausf 和中继服务码等参数生成。

本申请实施例提供另一种密钥获取方法,远端终端设备通过远端 AMF 网元主动

向 PKMF 网元请求中继服务码对应的第一标识,再由 PKMF 网元向远端 AUSF 网元请求第一标识,使得远端 AUSF 网元能够根据中继服务码生成对应的第一标识以及第二共享密钥,并发送给 PKMF 网元。在非直接通信过程中,远端终端设备向中继终端设备发起直接通信请求,直接通信请求中包括第一标识。中继终端设备通过信令面向网络侧发起包含第一标识的密钥请求,PKMF 网元根据第一标识获取对应的第二共享密钥,并生成远端终端设备与中继终端设备通信的根密钥。与图 9 的区别在于,远端 AMF 网元直接与 PKMF 网元通信。

如图 10 所示,该密钥获取方法包括:

10 S1001、远端终端设备接入网络,从远端 PCF 网元或其他相关网元获取用于通过中继终端设备通信的信息。

该步骤与步骤 S801 相同,在此不再重复。

S1002、中继终端设备接入网络,从中继 PCF 网元或其他相关网元获取作为中继终端设备提供通信的信息。

该步骤与步骤 S802 相同,在此不再重复。

15 S1003、远端终端设备向远端 AMF 网元发送密钥请求。

该密钥请求中包括至少一个中继服务码。

可选的,远端 AMF 网元执行授权检查,即检查是否授权远端终端设备作为中继终端设备的远端终端设备或者检查是否授权远端终端设备通过中继终端设备获取中继服务码对应的服务。

20 S1004、远端 AMF 网元选择 PKMF 网元,并向 PKMF 网元发送密钥请求。

远端 AMF 网元选择 PKMF 网元的方式与步骤 S905 中远端 AUSF 网元选择 PKMF 网元的方式相同。

该密钥请求中包括中继服务码、远端 AUSF 网元实例标识、远端终端设备的第二标识(例如 SUPI)。

25 若步骤 S1003 的密钥请求中包括多个中继服务码,且对应不同的 PKMF 网元,则远端 AMF 网元分别向每个 PKMF 网元发送密钥请求。

S1005、PKMF 网元向远端 AUSF 网元发送临近业务安全信息请求。

该请求中包括远端终端设备的第二标识(例如 SUPI)、中继服务码。

30 可选的,在发送消息前,PKMF 网元根据远端终端设备的第二标识(例如 SUPI)和中继服务码判断是否授权远端终端设备通过中继终端设备获取中继服务码对应的服务。

S1006、远端 AUSF 网元生成终端设备的与各个中继服务码对应的第一标识(例如 P-KID),以及,生成第二共享密钥 K_p 。

该步骤与步骤 S904 相同。

35 S1007、远端 AUSF 网元向 PKMF 网元发送临近业务安全信息响应。

临近业务安全信息响应中包括第二共享密钥 K_p ,可选的,还可以包括中继服务码、远端终端设备的第二标识(例如 SUPI)和远端终端设备的第一标识。

S1008、PKMF 网元通过远端 AMF 网元向远端终端设备发送密钥请求响应。

关于密钥请求响应包括的信息可以参照步骤 S806,在此不再重复。

S1009、远端终端设备获取第一标识。

该步骤与步骤 S807 相同。需要说明的是，远端终端设备生成第一标识的过程在步骤 S1011 之前执行即可。

S1010、远端终端设备执行发现流程以发现中继终端设备。

5 该步骤与步骤 S808 相同。

S1011、远端终端设备向中继终端设备发送直接通信请求。

该步骤与步骤 S909 相同。

S1012、中继终端设备向中继 AMF 网元发送密钥请求。

该步骤与步骤 S910 相同。

10 S1013、中继 AMF 网元选择 PKMF 网元，并向 PKMF 网元发送临近业务密钥请求。

中继 AMF 网元选择 PKMF 网元的方式与步骤 S1004 中远端 AMF 网元选择 PKMF 网元的方式相同。

临近业务密钥请求中携带的信息与步骤 S912 的临近业务密钥请求中携带的信息相同。

15 可选的，中继 AMF 网元执行授权检查，即检查是否授权中继终端设备作为远端中继设备的中继终端设备或者检查是否授权中继终端设备向远端终端设备提供中继服务码对应的连接服务。

S1014、可选的，PKMF 网元对远端终端设备和中继终端设备进行授权。

该步骤与步骤 S814 相同。

20 S1015、PKMF 网元根据第二共享密钥 K_p ，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

该步骤与步骤 S914 相同。

S1016、PKMF 网元通过中继 AMF 网元向中继终端设备发送临近业务密钥响应。

临近业务密钥响应携带的信息与步骤 S818 中临近业务密钥响应携带信息相同。

25 S1017、中继终端设备向远端终端设备发送安全模式命令。

该步骤与步骤 S820 相同。

S1018、远端终端设备向中继终端设备发送安全模式命令完整消息。

该步骤与步骤 S821 相同。

30 上述密钥获取方法中，远端终端设备获取与中继服务码对应的第一标识，通过该第一标识，使得中继终端设备能够通过信令面从网络侧获取远端终端设备与中继终端设备通信的根密钥。进一步的，PKMF 网元在获取根密钥之前先对远端终端设备和中继终端设备执行授权检查，保证只有授权的终端设备获取根密钥。其中，根密钥是根据第一共享密钥 K_{ausf} 和中继服务码等参数生成。

35 本申请实施例提供另一种密钥获取方法，在非直接通信过程中，远端终端设备向中继终端设备发起直接通信请求，直接通信请求中包括远端终端设备的 SUCI。中继终端设备通过信令面向网络侧发起包含 SUCI 的密钥请求，PKMF 网元通过远端 UDM 网元确定 SUCI 对应的远端 AUSF 网元，从远端 AUSF 网元获取远端终端设备与中继终端设备通信的根密钥。与图 8 的区别在于，PKMF 网元通过远端终端设备的 SUCI 确定远端 AUSF 网元。

如图 11 所示, 该密钥获取方法包括:

S1101、远端终端设备接入网络, 从远端 PCF 网元或其他相关网元获取用于通过中继终端设备通信的信息。

该步骤与步骤 S801 相同, 在此不再重复。

5 S1102、中继终端设备接入网络, 从中继 PCF 网元或其他相关网元获取作为中继终端设备提供通信的信息。

该步骤与步骤 S802 相同, 在此不再重复。

S1103、远端终端设备执行发现流程以发现中继终端设备。

该步骤与步骤 S808 相同。

10 S1104、远端终端设备向中继终端设备发送直接通信请求。

该步骤与步骤 S809 的区别在于, 直接通信请求中的第一标识可以为远端终端设备的 SUCI。

S1105、中继终端设备向中继 AMF 网元发送密钥请求。

15 该步骤与步骤 S810 的区别在于, 密钥请求中的第一标识可以为远端终端设备的 SUCI。

S1106、中继 AMF 网元选择中继 AUSF 网元, 并向中继 AUSF 网元发送临近业务密钥请求。

该步骤与步骤 S811 的区别在于, 临近业务密钥请求中的第一标识可以为远端终端设备的 SUCI。

20 S1107、中继 AUSF 网元选择 PKMF 网元, 并向 PKMF 网元发送临近业务密钥请求。

该步骤与步骤 S812 的区别在于, 临近业务密钥请求中的第一标识可以为远端终端设备的 SUCI。

25 S1108、PKMF 网元根据临近业务密钥请求中的第一标识 (例如 SUCI) 选择远端 UDM 网元, 并向远端 UDM 网元发送终端设备标识 (UE ID) 请求。

该终端设备标识请求中包括第一标识 (例如 SUCI)。

远端 UDM 网元根据第一标识 (例如 SUCI) 获取远端终端设备的第二标识 (例如 SUPI), 以及服务远端终端设备的远端 AUSF 网元实例标识, 并发送给 PKMF 网元。

S1109、PKMF 网元对远端终端设备和中继终端设备进行授权。

30 该步骤与步骤 S814 相同。

S1110、PKMF 网元向远端 AUSF 网元发送临近业务密钥请求。

该步骤与步骤 S815 相同。

S1111、远端 AUSF 网元根据第一共享密钥、中继服务码, 以及, 至少一个第一新鲜性参数, 生成远端终端设备与中继终端设备通信的根密钥。

35 该步骤与步骤 S816 相同。

S1112、远端 AUSF 网元向 PKMF 网元发送临近业务密钥响应。

该步骤与步骤 S817 相同。

S1113、PKMF 网元向中继 AUSF 网元发送临近业务密钥响应。

该步骤与步骤 S818 相同。

S1114、中继 AUSF 网元通过中继 AMF 网元向中继终端设备发送临近业务密钥响应。

该步骤与步骤 S819 相同。

S1115、中继终端设备向远端终端设备发送安全模式命令。

5 该步骤与步骤 S820 相同。

S1116、远端终端设备向中继终端设备发送安全模式命令完整消息。

该步骤与步骤 S821 相同。

需要说明的是，步骤 S811 和 S812 是可选的，远端 AMF 网元可以直接选择 PKMF 网元并向 PKMF 网元发送临近业务密钥请求，临近业务密钥请求中携带的内容与步骤
10 S811 的临近业务密钥请求中携带的信息相同。

上述密钥获取方法，远端终端设备生成 SUCI，使得中继终端设备能够使用 SUCI 从 PKMF 网元获取远端终端设备与中继终端设备通信的根密钥。具体的，PKMF 网元根据 SUCI 能够确定远端 AUSF 网元，从远端 AUSF 网元获取远端终端设备与中继终端设备通信的根密钥。

15 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，该通信装置用于实现上述各种方法。该通信装置可以为上述方法实施例中的远端终端设备，或者包含上述远端终端设备的装置，或者为远端终端设备内的芯片或功能模块。或者，该通信装置可以为上述方法实施例中的远端 AUSF 网元，或者包含上述远端 AUSF 网元的装置，或者为远端 AUSF 网元
20 内的芯片或功能模块。或者，该通信装置可以为上述方法实施例中的 PKMF 网元，或者包含上述 PKMF 网元的装置，或者为 PKMF 网元内的芯片或功能模块。

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
25 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。

本申请实施例可以根据上述方法实施例对通信装置进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理
30 模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，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。

比如，以通信装置为上述方法实施例中的远端终端设备为例。图 12 示出了一种通信装置 120 的结构示意图。该通信装置 120 可以为图 1 中的远端终端设备。该通信装置
35 120 包括处理模块 1201 和收发模块 1202。处理模块 1201 也可以称为处理单元，用以实现上述方法实施例中远端终端设备的处理功能。例如执行图 5 中的步骤 S502，图 8-图 11 中远端终端设备的处理功能。收发模块 1202，也可以称为收发单元，用以实现上述方法实施例中远端终端设备的收发功能。例如执行图 5 中的步骤 S501，图 8-图 11 中远端终端设备的收发功能。收发模块 1202 可以称为收发电路、收发机、收发器

或者通信接口。

示例性的,收发模块 1202,用于向中继终端设备发送第一标识和中继服务码,第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识;处理模块 1201,用于根据第一共享密钥、中继服务码,以及,至少一个第一新鲜性参数,生成远端终端设备与中继终端设备通信的根密钥,远端认证服务功能网元为服务远端终端设备的认证服务功能网元,第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥。

在一种可能的实施方式中,第一标识为远端终端设备的 SUCI。

在一种可能的实施方式中,处理模块 1201 和收发模块 1202 还用于获取第一标识。

10 在一种可能的实施方式中,收发模块 1202 还用于发送中继服务码;接收与中继服务码对应的第一标识。

在一种可能的实施方式中,处理模块 1201 还用于根据第一共享密钥、中继服务码,生成临时标识;根据临时标识获取第一标识。

15 在一种可能的实施方式中,处理模块 1201 还用于根据第一共享密钥、中继服务码和第二新鲜性参数,生成临时标识。

在一种可能的实施方式中,处理模块 1201 还用于根据第二新鲜性参数、路由指示和家乡网络标识,生成第一标识。

在一种可能的实施方式中,收发模块 1202 还用于发送中继服务码;接收中继服务码对应的第二新鲜性参数。

20 在一种可能的实施方式中,第二新鲜性参数为远端终端设备本地维护的计数器的值。

在一种可能的实施方式中,第一标识包括路由指示和家乡网络标识。

25 在一种可能的实施方式中,收发模块 1202 还用于向中继终端设备发送第一验证信息,第一验证信息由第一临时密钥,以及,携带第一验证信息的全部或部分信息生成,第一临时密钥由第一共享密钥生成。

在一种可能的实施方式中,第一临时密钥由中继服务码、第三新鲜性参数、远端终端设备的第二标识以及第一标识中的至少一项,以及,第一共享密钥生成,其中,第三新鲜性参数为远端终端设备生成。该实施方式公开了生成第一临时密钥的一种方式。

30 在一种可能的实施方式中,收发模块 1202 还用于向中继终端设备发送第二验证信息,第二验证信息由第一新鲜性参数、中继服务码和第一共享密钥生成。

在一种可能的实施方式中,至少一个第一新鲜性参数包括第一随机数,收发模块 1202 还用于向中继终端设备发送第一随机数。第一随机数发送给远端 AUSF 网元或 PKMF 网元。

35 在一种可能的实施方式中,至少一个第一新鲜性参数包括第二随机数,收发模块 1202 还用于从中继终端设备接收第二随机数。第二随机数可以来自远端 AUSF 网元或 PKMF 网元。

在一种可能的实施方式中,至少一个第一新鲜性参数为远端终端设备本地维护的计数器的值。

在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf。

在一种可能的实施方式中，处理模块 1201 还用于根据第一共享密钥和中继服务码生成第二共享密钥，根据第二共享密钥以及至少一个第一新鲜性参数，生成根密钥，
5 第二共享密钥为远端终端设备与临近业务密钥管理功能网元共享的密钥。

比如，以通信装置为上述方法实施例中的远端 AUSF 网元为例。图 13 示出了一种通信装置 130 的结构示意图。该通信装置 130 可以为图 1 中的 AUSF 网元。该通信装置 130 包括处理模块 1301 和收发模块 1302。处理模块 1301 也可以称为处理单元，用以实现上述方法实施例中远端 AUSF 网元的处理功能，图 8-图 11 中远端 AUSF 网元的处理功能。例如执行图 6 中的步骤 S601-S603。收发模块 1302，也可以称为收发单元，用以实现上述方法实施例中远端 AUSF 网元的收发功能。例如执行图 6 中的步骤 S601、S604，图 8-图 11 中远端 AUSF 网元的收发功能。收发模块 1302 可以称为收发电路、收发机、收发器或者通信接口。
10

示例性的，处理模块 1301 用于获取远端终端设备的第一标识或第二标识中的一个，
15 以及，中继服务码；第二标识为远端终端设备的永久身份标识，第一标识为远端终端设备的与中继服务码对应的标识；处理模块 1301 还用于获取第一标识或第二标识对应的第一共享密钥；第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；远端认证服务功能网元根据第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥；收发模块 1302 用于发送根密
20 钥。

在一种可能的实施方式中，收发模块 1302 还用于接收远端终端设备的第一标识或第二标识中的一个。

在一种可能的实施方式中，处理模块 1301 还用于根据第一共享密钥、中继服务码，生成临时标识；远端认证服务功能网元根据临时标识生成第一标识。

25 在一种可能的实施方式中，处理模块 1301 还用于根据第一共享密钥、中继服务码和第二新鲜性参数，生成临时标识。

在一种可能的实施方式中，处理模块 1301 还用于根据第二新鲜性参数、路由指示和远端终端设备的家乡网络标识，生成第一标识。

在一种可能的实施方式中，第二新鲜性参数为远端认证服务功能网元本地维护的
30 计数器的值。

在一种可能的实施方式中，收发模块 1302 还用于接收中继服务码；发送第二新鲜性参数。

在一种可能的实施方式中，收发模块 1302 还用于接收中继服务码；发送第一标识。

在一种可能的实施方式中，第一标识包括路由指示和家乡网络标识。

35 在一种可能的实施方式中，收发模块 1302 还用于接收第一验证信息；处理模块 1301 还用于根据第一共享密钥，生成第一临时密钥；并根据第一临时密钥，以及，携带第一验证信息的全部或部分信元，得到第三验证信息；比较第一验证信息和第三验证信息以对远端终端设备进行验证。

在一种可能的实施方式中，处理模块 1301 还用于根据中继服务码、第三新鲜性参

数、第二标识以及远端终端设备的第一标识中的至少一项，以及，第一共享密钥，生成第一临时密钥，第三新鲜性参数为远端终端设备生成。

在一种可能的实施方式中，至少一个第一新鲜性参数包括第一随机数，收发模块 1302 还用于接收第一随机数。

5 在一种可能的实施方式中，至少一个第一新鲜性参数包括第二随机数，收发模块 1302 还用于发送第二随机数。

在一种可能的实施方式中，至少一个第一新鲜性参数为远端认证服务功能网元本地维护的计数器的值。

10 在一种可能的实施方式中，收发模块 1302 还用于向统一数据管理网元发送第一标识。

在一种可能的实施方式中，第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf。

15 比如，以通信装置为上述方法实施例中的 PKMF 网元为例。图 14 示出了一种通信装置 140 的结构示意图。该通信装置 140 包括处理模块 1401 和收发模块 1402。处理模块 1401 也可以称为处理单元，用以实现上述方法实施例中 PKMF 网元的处理功能。例如执行图 7 中的步骤 S702，图 8-图 11 中 PKMF 网元的处理功能。收发模块 1402，也可以称为收发单元，用以实现上述方法实施例中 PKMF 网元的收发功能。例如执行图 7 中的步骤 S701-S703，图 8-图 11 中 PKMF 网元的收发功能。收发模块 1402 可以称为收发电路、收发机、收发器或者通信接口。

20 示例性的，收发模块 1402 用于接收远端终端设备的第一标识和中继服务码，第一标识为远端终端设备的与中继服务码对应的标识或者第一标识为远端终端设备的匿名标识；处理模块 1401 用于根据第一标识获取远端终端设备与中继终端设备通信的根密钥，根密钥由第一共享密钥、中继服务码，以及，至少一个第一新鲜性参数生成，第一共享密钥为远端终端设备与远端认证服务功能网元共享的密钥；收发模块 1402 还用于发送根密钥。

25 在一种可能的实施方式中，收发模块 1402 还用于向统一数据管理功能网元发送第一标识；从统一数据管理功能网元接收远端认证服务功能网元的标识信息；根据标识信息，向对应的远端认证服务功能网元发送第一标识；从远端认证服务功能网元接收根密钥。

30 在一种可能的实施方式中，收发模块 1402 还用于向统一数据管理功能网元发送第一标识；从统一数据管理功能网元接收远端认证服务功能网元的标识信息以及远端终端设备的永久身份标识；根据标识信息，向对应的远端认证服务功能网元发送远端终端设备的永久身份标识；从远端认证服务功能网元接收根密钥。

35 在一种可能的实施方式中，收发模块 1402 还用于从远端认证服务功能网元接收至少一个第二共享密钥，第二共享密钥为远端终端设备与临近业务密钥管理功能网元共享的密钥，第二共享密钥由第一共享密钥和中继服务码生成；处理模块 1401 还用于根据第一标识对应的第二共享密钥，以及，至少一个第一新鲜性参数，生成远端终端设备与中继终端设备通信的根密钥。

在一种可能的实施方式中，还包括：收发模块 1402 还用于接收第二验证信息；处

理模块 1401 还用于根据第一新鲜性参数和第二共享密钥,生成第四验证信息;比较第二验证信息和第四验证密信息以对远端终端设备进行验证。

在一种可能的实施方式中,至少一个第一新鲜性参数包括第一随机数,收发模块 1402 还用于接收第一随机数。

- 5 在一种可能的实施方式中,至少一个第一新鲜性参数包括第二随机数,收发模块 1402 还用于发送第二随机数。

在一种可能的实施方式中,至少一个第一新鲜性参数为临近业务密钥管理功能网元本地维护的计数器的值。

- 10 在一种可能的实施方式中,第一共享密钥为远端终端设备接入网络时与远端认证服务功能网元协商的密钥 Kausf。

在本实施例中,上述通信装置以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定 ASIC,电路,执行一个或多个软件或固件程序的处理器和存储器,集成逻辑电路,和/或其他可以提供上述功能的器件。

- 15 具体的,处理模块的功能/实现过程可以通过通信装置中的处理器调用存储器中存储的计算机执行指令来实现。收发模块的功能/实现过程可以通过通信设备中的收发器或通信接口来实现。

由于本实施例提供的通信装置可执行上述方法,因此其所能获得的技术效果可参考上述方法实施例,在此不再赘述。

- 20 如图 15 所示,本申请实施例还提供了一种通信装置,该通信装置 150 包括处理器 1501、存储器 1502 和收发器 1503,处理器 1501 与存储器 1502 耦合,当处理器 1501 执行存储器 1502 中的计算机程序或指令时,图 2-图 11 中远端终端设备对应的方法被执行。

- 25 如图 16 所示,本申请实施例还提供了一种通信装置,该通信装置 160 包括处理器 1601、存储器 1602 和通信接口 1603,处理器 1601 与存储器 1602 耦合,当处理器 1601 执行存储器 1602 中的计算机程序或指令时,图 2-图 11 中 AUSF 网元(例如远端 AUSF 网元、中继 AUSF 网元)对应的方法被执行。

- 30 如图 17 所示,本申请实施例还提供了一种通信装置,该通信装置 170 包括处理器 1701、存储器 1702 和通信接口 1703,处理器 1701 与存储器 1702 耦合,当处理器 1701 执行存储器 1702 中的计算机程序或指令时,图 2-图 11 中 PKMF 网元对应的方法被执行。

本申请实施例还提供了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计算机程序,当其在计算机或处理器上运行时,使得计算机或处理器执行图 2-图 11 中远端终端设备对应的方法。

- 35 本申请实施例还提供了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计算机程序,当其在计算机或处理器上运行时,使得计算机或处理器执行图 2-图 11 中 AUSF 网元(例如远端 AUSF 网元、中继 AUSF 网元)对应的方法。

本申请实施例还提供了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计算机程序,当其在计算机或处理器上运行时,使得计算机或处理器执行图 2-图 11 中 PKMF 网元对应的方法。

本申请实施例还提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器执行图 2-图 11 中远端终端设备对应的方法。

本申请实施例还提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器执行图 2-图 11 中 AUSF 网元（例如远端 AUSF 网元、中继 AUSF 网元）对应的方法。

本申请实施例还提供了一种包含指令的计算机程序产品，当指令在计算机或处理器上运行时，使得计算机或处理器执行图 2-图 11 中 PKMF 网元对应的方法。

本申请实施例提供了一种芯片系统，该芯片系统包括处理器，用于通信装置执行图 2-图 11 中远端终端设备对应的方法，或者，执行图 2-图 11 中 AUSF 网元（例如远端 AUSF 网元、中继 AUSF 网元）对应的方法，或者，执行图 2-图 11 中 PKMF 网元对应的方法。

在一种可能的设计中，该芯片系统还包括存储器，该存储器，用于保存必要的程序指令和数据。该芯片系统，可以包括芯片，集成电路，也可以包含芯片和其他分立器件，本申请实施例对此不作具体限定。

其中，本申请提供的通信装置、芯片、计算机存储介质、计算机程序产品或芯片系统均用于执行上文所述的方法，因此，其所能达到的有益效果可参考上文所提供的实施方式中的有益效果，此处不再赘述。

本申请实施例涉及的处理器可以是一个芯片。例如，可以是现场可编程门阵列（field programmable gate array, FPGA），可以是专用集成电路（application specific integrated circuit, ASIC），还可以是系统芯片（system on chip, SoC），还可以是中央处理器（central processor unit, CPU），还可以是网络处理器（network processor, NP），还可以是数字信号处理电路（digital signal processor, DSP），还可以是微控制器（micro controller unit, MCU），还可以是可编程控制器（programmable logic device, PLD）或其他集成芯片。

本申请实施例涉及的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。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），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如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, SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM, DR RAM）。应注意，本文描述的系统和方法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。

应理解，在本申请的各种实施例中，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，而不对本申请实施例的

实施过程构成任何限定。

本领域普通技术人员可以意识到，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，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，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。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

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、设备和方法，可以通过其它的方式实现。例如，以上所描述的设备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，设备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。

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单元上。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，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

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。当使用软件程序实现时，可以全部或部分地以计算机程序产品的形式来实现。该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、服务器或者数据中心通过有线（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以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。

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

1、一种密钥获取方法，其特征在于，包括：

5 远端终端设备向中继终端设备发送第一标识和中继服务码，所述第一标识为所述远端终端设备的与所述中继服务码对应的标识或者所述第一标识为所述远端终端设备的匿名标识；

所述远端终端设备根据第一共享密钥、所述中继服务码，以及，至少一个第一新鲜性参数，生成所述远端终端设备与所述中继终端设备通信的根密钥，所述远端认证服务功能网元为服务所述远端终端设备的认证服务功能网元，所述第一共享密钥为所述远端终端设备与所述远端认证服务功能网元共享的密钥。

10 2、根据权利要求1所述的方法，其特征在于，所述第一标识为所述远端终端设备的订阅隐藏标识 SUCI。

3、根据权利要求1所述的方法，其特征在于，还包括：

所述远端终端设备获取所述第一标识。

15 4、根据权利要求3所述的方法，其特征在于，所述远端终端设备获取所述第一标识，包括：

所述远端终端设备发送所述中继服务码；

所述远端终端设备接收与所述中继服务码对应的所述第一标识。

5、根据权利要求3所述的方法，其特征在于，还包括：

所述远端终端设备根据所述第一共享密钥、所述中继服务码，生成临时标识；

20 所述远端终端设备根据所述临时标识获取所述第一标识。

6、根据权利要求5所述的方法，其特征在于，所述远端终端设备根据所述第一共享密钥、所述中继服务码生成临时标识，包括：

所述远端终端设备根据所述第一共享密钥、所述中继服务码和第二新鲜性参数，生成所述临时标识。

25 7、根据权利要求3所述的方法，其特征在于，所述远端终端设备获取所述第一标识，包括：

所述远端终端设备根据第二新鲜性参数、路由指示和家乡网络标识，生成所述第一标识。

8、根据权利要求6或7所述的方法，其特征在于，还包括：

30 所述远端终端设备发送所述中继服务码；

所述远端终端设备接收所述中继服务码对应的所述第二新鲜性参数。

9、根据权利要求6或7所述的方法，其特征在于，所述第二新鲜性参数为所述远端终端设备本地维护的计数器的值。

10、根据权利要求3-9任一项所述的方法，其特征在于，所述第一标识包括路由指示和家乡网络标识。

35 11、根据权利要求1-10任一项所述的方法，其特征在于，还包括：

所述远端终端设备向所述中继终端设备发送第一验证信息，所述第一验证信息由第一临时密钥，以及，携带所述第一验证信息的全部或部分信元生成，所述第一临时密钥由所述第一共享密钥生成。

12、根据权利要求 11 所述的方法，其特征在于，所述第一临时密钥由所述中继服务码、第三新鲜性参数、所述远端终端设备的第二标识以及所述第一标识中的至少一项，以及，所述第一共享密钥生成，其中，所述第三新鲜性参数为所述远端终端设备生成。

5 13、根据权利要求 1-12 任一项所述的方法，其特征在于，还包括：

所述远端终端设备向所述中继终端设备发送第二验证信息，所述第二验证信息由所述第一新鲜性参数、所述中继服务码和所述第一共享密钥生成。

14、根据权利要求 1-13 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数包括第一随机数，还包括：

10 所述远端终端设备向所述中继终端设备发送所述第一随机数。

15、根据权利要求 1-14 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数包括第二随机数，还包括：

所述远端终端设备从所述中继终端设备接收所述第二随机数。

15 16、根据权利要求 1-13 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数为所述远端终端设备本地维护的计数器的值。

17、根据权利要求 1-16 任一项所述的方法，其特征在于，所述第一共享密钥为所述远端终端设备接入网络时与所述远端认证服务功能网元协商的密钥 Kausf。

20 18、根据权利要求 1-17 任一项所述的方法，其特征在于，所述远端终端设备根据第一共享密钥、所述中继服务码，以及，至少一个第一新鲜性参数，生成所述远端终端设备与所述中继终端设备通信的根密钥，包括：

所述远端终端设备根据所述第一共享密钥和所述中继服务码生成第二共享密钥，根据所述第二共享密钥以及所述至少一个第一新鲜性参数，生成所述根密钥，所述第二共享密钥为所述远端终端设备与临近业务密钥管理功能网元共享的密钥。

19、一种密钥获取方法，其特征在于，包括：

25 远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个，以及，中继服务码；所述第二标识为所述远端终端设备的永久身份标识，所述第一标识为所述远端终端设备的与所述中继服务码对应的标识；

所述远端认证服务功能网元获取所述第一标识或所述第二标识对应的第一共享密钥；所述第一共享密钥为所述远端终端设备与所述远端认证服务功能网元共享的密钥；

30 所述远端认证服务功能网元根据所述第一共享密钥、所述中继服务码，以及，至少一个第一新鲜性参数，生成所述远端终端设备与所述中继终端设备通信的根密钥；

所述远端认证服务功能网元发送所述根密钥。

20、根据权利要求 19 所述的方法，其特征在于，所述远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个，包括：

35 所述远端认证服务功能网元接收所述远端终端设备的第一标识或第二标识中的一个。

21、根据权利要求 19 所述的方法，其特征在于，所述远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个，包括：

所述远端认证服务功能网元根据所述第一共享密钥、所述中继服务码，生成临时

标识;

所述远端认证服务功能网元根据所述临时标识生成所述第一标识。

22、根据权利要求 21 所述的方法,其特征在于,所述远端认证服务功能网元根据所述第一共享密钥、所述中继服务码,生成临时标识,包括:

- 5 所述远端终端设备根据所述第一共享密钥、所述中继服务码和第二新鲜性参数,生成所述临时标识。

23、根据权利要求 19 所述的方法,其特征在于,所述远端认证服务功能网元获取远端终端设备的第一标识或第二标识中的一个,包括:

- 10 所述远端认证服务功能网元根据第二新鲜性参数、路由指示和所述远端终端设备的家乡网络标识,生成所述第一标识。

24、根据权利要求 22 或 23 所述的方法,其特征在于,所述第二新鲜性参数为所述远端认证服务功能网元本地维护的计数器的值。

25、根据权利要求 22 或 23 所述的方法,其特征在于,还包括:

- 15 所述远端认证服务功能网元接收所述中继服务码;
 所述远端认证服务功能网元发送所述第二新鲜性参数。

26、根据权利要求 19-25 任一项所述的方法,其特征在于,还包括:

 所述远端认证服务功能网元接收所述中继服务码;
 所述远端认证服务功能网元发送所述第一标识。

- 20 27、根据权利要求 19-26 任一项所述的方法,其特征在于,所述第一标识包括路由指示和家乡网络标识。

28、根据权利要求 19-27 任一项所述的方法,其特征在于,还包括:

- 所述远端认证服务功能网元接收第一验证信息;
 所述远端认证服务功能网元根据所述第一共享密钥,生成第一临时密钥;并根据所述第一临时密钥,以及,携带所述第一验证信息的全部或部分信元,得到第
25 三验证信息;

 所述远端认证服务功能网元比较所述第一验证信息和所述第三验证信息以对所述远端终端设备进行验证。

29、根据权利要求 28 所述的方法,其特征在于,所述远端认证服务功能网元根据所述第一共享密钥,生成第一临时密钥,包括:

- 30 所述远端认证服务功能网元根据所述中继服务码、第三新鲜性参数、所述第二标识以及所述远端终端设备的第一标识中的至少一项,以及,所述第一共享密钥,生成所述第一临时密钥,所述第三新鲜性参数为所述远端终端设备生成。

30、根据权利要求 19-29 任一项所述的方法,其特征在于,所述至少一个第一新鲜性参数包括第一随机数,还包括:

- 35 所述远端认证服务功能网元接收所述第一随机数。

31、根据权利要求 19-30 任一项所述的方法,其特征在于,所述至少一个第一新鲜性参数包括第二随机数,还包括:

 所述远端认证服务功能网元发送所述第二随机数。

32、根据权利要求 19-30 任一项所述的方法,其特征在于,所述至少一个第一新

鲜性参数为所述远端认证服务功能网元本地维护的计数器的值。

33、根据权利要求 19-32 任一项所述的方法，其特征在于，还包括：

所述远端认证服务功能网元向统一数据管理网元发送所述第一标识。

34、根据权利要求 19-33 任一项所述的方法，其特征在于，所述第一共享密钥为
5 所述远端终端设备接入网络时与所述远端认证服务功能网元协商的密钥 Kauf。

35、一种密钥获取方法，其特征在于，包括：

临近业务密钥管理功能网元接收远端终端设备的第一标识和中继服务码，所述第一标识为所述远端终端设备的与所述中继服务码对应的标识或者所述第一标识为所述远端终端设备的匿名标识；

10 所述临近业务密钥管理功能网元根据所述第一标识获取所述远端终端设备与所述中继终端设备通信的根密钥，所述根密钥由第一共享密钥、所述中继服务码，以及，至少一个第一新鲜性参数生成，所述第一共享密钥为所述远端终端设备与远端认证服务功能网元共享的密钥；

所述临近业务密钥管理功能网元发送所述根密钥。

15 36、根据权利要求 35 所述的方法，其特征在于，所述临近业务密钥管理功能网元根据所述第一标识获取所述远端终端设备与所述中继终端设备通信的根密钥，包括：

所述临近业务密钥管理功能网元向统一数据管理功能网元发送所述第一标识；

所述临近业务密钥管理功能网元从所述统一数据管理功能网元接收所述远端认证服务功能网元的标识信息；

20 所述临近业务密钥管理功能网元根据所述标识信息，向对应的所述远端认证服务功能网元发送所述第一标识；

所述临近业务密钥管理功能网元从所述远端认证服务功能网元接收所述根密钥。

37、根据权利要求 35 所述的方法，其特征在于，所述临近业务密钥管理功能网元根据所述第一标识获取所述远端终端设备与所述中继终端设备通信的根密钥，包括：

25 所述临近业务密钥管理功能网元向统一数据管理功能网元发送所述第一标识；

所述临近业务密钥管理功能网元从所述统一数据管理功能网元接收所述远端认证服务功能网元的标识信息以及所述远端终端设备的永久身份标识；

所述临近业务密钥管理功能网元根据所述标识信息，向对应的所述远端认证服务功能网元发送所述远端终端设备的永久身份标识；

30 所述临近业务密钥管理功能网元从所述远端认证服务功能网元接收所述根密钥。

38、根据权利要求 35 所述的方法，其特征在于，所述临近业务密钥管理功能网元根据所述第一标识获取所述远端终端设备与所述中继终端设备通信的根密钥，包括：

所述临近业务密钥管理功能网元从远端认证服务功能网元接收至少一个第二共享密钥，所述第二共享密钥为所述远端终端设备与所述临近业务密钥管理功能网元共享的密钥，所述第二共享密钥由所述第一共享密钥和所述中继服务码生成；
35

所述临近业务密钥管理功能网元根据所述第一标识对应的所述第二共享密钥，以及，至少一个第一新鲜性参数，生成所述远端终端设备与中继终端设备通信的根密钥。

39、根据权利要求 38 所述的方法，其特征在于，还包括：

所述临近业务密钥管理功能网元接收第二验证信息；

所述临近业务密钥管理功能网元根据所述第一新鲜性参数和所述第二共享密钥，生成第四验证信息；

所述临近业务密钥管理功能网元比较所述第二验证信息和所述第四验证密信息以对所述远端终端设备进行验证。

- 5 40、根据权利要求 35-39 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数包括第一随机数，还包括：

所述临近业务密钥管理功能网元接收所述第一随机数。

- 41、根据权利要求 35-40 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数包括第二随机数，还包括：

- 10 所述临近业务密钥管理功能网元发送所述第二随机数。

- 42、根据权利要求 35-39 任一项所述的方法，其特征在于，所述至少一个第一新鲜性参数为所述临近业务密钥管理功能网元本地维护的计数器的值。

- 43、根据权利要求 35-42 任一项所述的方法，其特征在于，所述第一共享密钥为所述远端终端设备接入网络时与所述远端认证服务功能网元协商的密钥 Kausf。

- 15 44、一种通信装置，其特征在于，包括处理器，所述处理器与存储器相连，所述存储器用于存储计算机程序，所述处理器用于执行存储器中存储的计算机程序，以使
得所述通信装置执行如权利要求 1-18 任一项所述的方法。

- 45、一种通信装置，其特征在于，包括处理器，所述处理器与存储器相连，所述存储器用于存储计算机程序，所述处理器用于执行存储器中存储的计算机程序，以使
20 得所述通信装置执行如权利要求 19-34 任一项所述的方法。

- 46、一种通信装置，其特征在于，包括处理器，所述处理器与存储器相连，所述存储器用于存储计算机程序，所述处理器用于执行存储器中存储的计算机程序，以使
得所述通信装置执行如权利要求 35-43 任一项所述的方法。