

密钥管理方法、设备及系统

技术领域

本申请涉及通信技术领域，尤其涉及密钥管理方法、设备及系统。

背景技术

目前，终端设备可支持应用程序的身份验证和密钥管理（authentication and key management for applications, AKMA）服务。在 AKMA 服务中，终端设备与应用功能网元进行数据传输，终端设备需要与应用功能网元之间协商两者之间的通信密钥，该通信密钥可以用来进行身份鉴权和通信保护。应用功能网元从 AKMA 的锚点功能网元获取该应用功能网元与终端设备之间的通信密钥，AKMA 的锚点功能网元根据 AKMA 密钥生成该应用功能网元与终端设备之间的通信密钥。AKMA 的锚点功能网元可以从终端设备对应的鉴权服务器功能网元获取 AKMA 密钥。

而当前的 AKMA 流程中未考虑重鉴权的发生，重鉴权会导致 AKMA 密钥的更新和删除，该种情况下，如何保证终端设备与应用功能网元之间成功协商该应用功能网元与该终端设备之间的通信密钥是亟待解决的问题。

发明内容

本申请提供一种密钥管理方法、通信装置及通信系统，保证 AKMA 流程中发生重鉴权后终端设备与应用功能网元之间仍能成功协商该应用功能网元与该终端设备之间的通信密钥。

第一方面，本申请提供一种密钥管理方法，该方法包括：终端设备向第一应用功能网元发送第一应用会话建立请求消息，该第一应用会话建立请求消息携带第一密钥的标识信息，该第一密钥为应用的认证和密钥管理 AKMA 密钥；该终端设备接收重鉴权流程中的第一鉴权请求消息；该终端设备发送该重鉴权流程中的该第一鉴权请求消息的响应消息；该终端设备接收来自该第一应用功能网元的该第一应用会话建立请求消息的响应消息；该终端设备使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。

该方法中，发送重鉴权后，终端设备仍使用重鉴权前生成的第一密钥推演终端设备和应用功能网元之间的通信密钥，保证和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。该方法还可以避免应用会话业务中断，减少业务时延，提高用户体验。

在一个可能的设计中，该终端设备发送该第一鉴权请求消息的响应消息后，不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，若该重鉴权流程成功，该终端设备不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，若该重鉴权流程之前发送了该第一应用会话建立请求，且未收到该第一应用会话建立请求消息的响应消息，该终端设备不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中,若该重鉴权流程之前该终端设备发送了该第一应用会话建立请求,且已收到该第一应用会话建立请求消息的响应消息但未推演该终端设备和该第一应用功能网元之间的通信密钥,该终端设备不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中,若未推演该终端设备和该第一应用功能网元之间的通信密钥,该终端设备不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中,该终端设备接收来自该第一应用会话建立请求消息的响应消息后,确定使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。

在一个可能的设计中,该终端设备发送该第一鉴权请求消息的响应消息后,生成第二密钥,该第二密钥为 AKMA 密钥。

在一个可能的设计中,当该终端设备确定该第一应用会话建立请求消息为该重鉴权流程前发送的,则该终端设备确定使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。

在一个可能的设计中,当该终端设备确定该第一应用会话建立请求消息携带的是该第一密钥的标识信息,则该终端设备确定使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。

在一个可能的设计中,该终端设备根据第一应用会话上下文中的第一密钥的标识信息确定该第一应用会话建立请求消息携带的是该第一密钥的标识信息。

在一个可能的设计中,该终端设备发送该第一鉴权请求消息的响应消息后,保存发送该第一应用会话建立请求消息和该重鉴权流程的先后关系。

在一个可能的设计中,当携带该第一密钥的标识信息的应用会话请求消息都得到了响应,该终端设备删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中,当该终端设备未得到响应消息的应用会话请求消息都为该重鉴权流程之后发送的,该终端设备删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中,该终端设备发送该第一鉴权请求消息的响应消息后,该终端设备向第二应用功能网元发送第二应用会话建立请求消息,该第二应用会话建立请求消息携带第二密钥的标识信息,该第二密钥为 AKMA 密钥。

在一个可能的设计中,该终端设备还使用第一密钥的标识信息或第一应用功能网元的标识信息推演该终端设备和该第一应用功能网元之间的通信密钥。

第二方面,本申请提供了一种密钥管理方法,该方法包括:鉴权服务功能网元接收重鉴权流程中的第二鉴权请求;该鉴权服务功能网元发送该重鉴权流程中的该第二鉴权请求的响应消息;该鉴权服务功能网元接收来自应用的认证和密钥管理 AKMA 锚点功能网元的第一密钥请求消息,该第一密钥请求消息携带第一密钥的标识信息,该第一密钥为该重鉴权流程前生成的 AKMA 密钥;该鉴权服务功能网元向该 AKMA 锚点功能网元发送该第一密钥。

该方法中,发送重鉴权后,鉴权服务功能网元仍向 AKMA 锚点功能网元发送重鉴权前生成的第一密钥,以使 AKMA 锚点功能网元使用第一密钥生成终端设备和应用功能网元之间的通信密钥,保证终端设备生成的终端设备和应用功能网元之间的通信密钥和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致,从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥,实现终端设备和应用功能网元之间的安全通信。该方法还可以避免应用会话业务中断,减少业务时延,提高用户体验。

在一个可能的设计中,该鉴权服务功能网元发送该第二鉴权请求的响应消息后,不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，该鉴权服务功能网元接收来自终端设备的第一指示，该第一指示用于指示不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，该第一指示携带在该第二鉴权请求中。

在一个可能的设计中，当该重鉴权流程成功，该鉴权服务功能网元不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，该鉴权服务功能网元发送该第二鉴权请求的响应消息后，生成第二密钥，该第二密钥为 AKMA 密钥。

在一个可能的设计中，该鉴权服务功能网元根据该第一密钥的标识信息，确定该第一密钥。

第三方面，本申请提供了一种密钥管理方法，该方法包括：重鉴权流程后，应用的认证和密钥管理 AKMA 锚点功能网元接收来自第一应用功能网元的第一请求消息，该第一请求消息用于请求终端设备和该第一应用功能网元之间的通信密钥，该第一请求消息携带第一密钥的标识信息，该第一密钥为该重鉴权流程前生成的 AKMA 密钥；该 AKMA 锚点功能网元使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥；该 AKMA 锚点功能网元向该应用功能网元发送该通信密钥。

该方法中，发送重鉴权后，AKMA 锚点功能网元仍使用重鉴权前生成的第一密钥生成终端设备和应用功能网元之间的通信密钥，保证终端设备生成的终端设备和应用功能网元之间的通信密钥和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

在一个可能的设计中，该重鉴权流程后，该 AKMA 锚点功能网元不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，该 AKMA 锚点功能网元接收来自该终端设备或鉴权服务功能网元的第二指示，该第二指示用于指示不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，当该重鉴权流程成功，该 AKMA 锚点功能网元不删除该第一密钥和该第一密钥的标识信息。

在一个可能的设计中，该重鉴权流程后，该 AKMA 锚点功能网元获取第二密钥，该第二密钥为该重鉴权流程后生成的 AKMA 密钥。

在一个可能的设计中，该 AKMA 锚点功能网元根据该第一密钥的标识信息，确定该第一密钥。

第四方面，本申请提供了一种密钥管理方法，该方法包括：终端设备向第一应用功能网元发送第一应用会话建立请求消息，该第一应用会话建立请求消息携带第一密钥的标识信息，该第一密钥为应用的认证和密钥管理 AKMA 密钥；该终端设备接收重鉴权流程中的第一鉴权请求消息；该终端设备发送该重鉴权流程中的该第一鉴权请求消息的响应消息；该终端设备接收来自该第一应用功能网元的该第一应用会话建立请求消息的响应消息；该终端设备向该第一应用功能网元发送第二应用会话建立请求消息，该第二应用会话建立请求消息携带第二密钥的标识信息，该第二密钥为该重鉴权流程后生成的 AKMA 密钥。

该方法中，发生重鉴权前，终端设备使用重鉴权前生成的第一密钥的标识信息和应用功能网元发起应用会话建立流程，发送重鉴权后，终端设备使用重鉴权后生成的第二密钥的标识信息重新和该应用功能网元发起应用会话建立流程，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的

安全通信。

在一个可能的设计中，该终端设备根据该第一应用会话建立请求消息的响应消息，确定该第一应用会话建立失败；该终端设备向该第一应用功能网元发送第二应用会话建立请求消息。

在一个可能的设计中，该第一应用会话建立请求消息的响应消息包括以下任意一项或多项：第三指示、第一失败原因值或第二失败原因值，其中，第三指示用于指示该第一应用会话建立失败，该第一失败原因值用于指示无法找到鉴权服务功能网元，该第二失败原因值用于指示无法确定该第一密钥的标识信息对应的该第一密钥，该鉴权服务功能网元用于生成该第一密钥。

在一个可能的设计中，该终端设备根据第一标识向该第一应用服务器发送该第二应用会话建立请求消息，该第一标识用于标识该终端设备上执行了该重鉴权流程。

在一个可能的设计中，该第一标识用于标识执行该主鉴权流程之前该终端设备发送了该第一应用会话建立请求消息。

在一个可能的设计中，该重主鉴权流程后，该终端设备在该终端设备上设置该第一标识。

在一个可能的设计中，若该第一应用会话建立请求消息的响应消息受到该第一应用功能网元和终端设备之间的通信密钥的安全保护，该终端设备解安全保护失败，则该终端设备向该第一应用服务器发送该第二应用会话建立请求消息，该第一应用功能网元和终端设备之间的通信密钥由该第一密钥推演而来。

在一个可能的设计中，若该终端设备收到该第一应用会话建立请求消息的响应消息后，使用该第一应用功能网元和终端设备之间的通信密钥与该第一应用功能网元进行安全通信失败，则该终端设备向该第一应用服务器发送该第二应用会话建立请求消息，该第一应用功能网元和终端设备之间的通信密钥为由该第一密钥推演而来。

在一个可能的设计中，该终端设备删除该第一应用会话的上下文；或者该终端设备指示该第一应用功能网元删除该第一应用会话的上下文。

第五方面，本申请提供了一种密钥管理方法，该方法包括：重鉴权流程后，应用的认证和密钥管理 AKMA 锚点功能网元接收来自第一应用功能网元的第一请求消息，该第一请求消息用于请求终端设备和该第一应用功能网元之间的通信密钥，该第一请求消息携带第一密钥的标识信息，该第一密钥为该重鉴权流程前生成的 AKMA 密钥；该 AKMA 锚点功能网元无法确定该第一密钥的标识信息对应的鉴权服务功能网元；该 AKMA 锚点功能网元向该第一应用功能网元发送第一请求消息的响应消息，该第一请求消息的响应消息指示该终端设备和该第一应用功能网元之间的通信密钥请求失败。

该方法中，发送重鉴权后，若无法确定该第一密钥的标识信息对应的鉴权服务功能网元，AKMA 锚点功能网元指示该第一应用功能网元无法确定鉴权服务功能网元，以便第一应用功能网元指示终端设备第一应用会话建立失败，使得终端设备可以重新发起应用会话建立流程，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

在一个可能的设计中，该 AKMA 锚点功能网元向数据管理网元发送鉴权服务功能网元路径信息请求消息，该鉴权服务功能网元路径信息请求消息携带该第一密钥的标识信息；该 AKMA 锚点功能网元接收来自该数据管理网元的该鉴权服务功能网元路径信息请求消息的响应消息，该鉴权服务功能网元路径信息请求消息的响应消息指示鉴权服务功能网元路径信息请求失败。

在一个可能的设计中,该 AKMA 锚点功能网元向该第一应用功能网元发送第一失败原因值,该第一失败原因值指示无法找到该鉴权服务功能网元。

第六方面,本申请提供了一种密钥管理方法,该方法包括:鉴权服务功能网元接收重鉴权流程中的第二鉴权请求;该鉴权服务功能网元发送该重鉴权流程中的该第二鉴权请求的响应消息;

该鉴权服务功能网元接收来自应用的认证和密钥管理 AKMA 锚点功能网元的第一密钥请求消息,该第一密钥请求消息携带第一密钥的标识信息,该第一密钥为该重鉴权流程前该鉴权服务功能网元生成的 AKMA 密钥;

该鉴权服务功能网元无法确定该第一密钥的标识信息对应的该第一密钥;

该鉴权服务功能网元向该 AKMA 锚点功能网元发送该第一密钥请求消息的响应消息,该第一密钥请求消息的响应消息用于指示该第一密钥请求失败。

该方法中,发送重鉴权后,若无法确定该第一密钥的标识信息对应的该第一密钥,鉴权服务功能网元指示 AKMA 锚点功能网元无法确定该第一密钥,以便 AKMA 锚点功能网元指示应用功能网元终端设备和应用功能网元之间的通信密钥请求失败,进而使得应用功能网元指示终端设备第一应用会话建立失败,这样终端设备可以重新发起应用会话建立流程,从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥,实现终端设备和应用功能网元之间的安全通信。

在一个可能的设计中,该鉴权服务功能网元向该 AKMA 锚点功能网元发送第二失败原因值,该第二失败原因值指示无法确定该第一密钥的标识信息对应的该第一密钥。

第七方面,本申请提供了一种终端设备,该终端设备具有实现上述第一方面或第四方面中该方法的功能。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。该硬件和软件包括一个或多个与上述功能相对应的模块。

在一种可能的设计中,终端设备的结构包括处理器和收发器,该处理器被配置为支持终端设备执行上述第一方面或第四方面中的方法,该收发器用于支持终端设备与其他设备之间的通信。该终端设备还可以包括存储器,该存储器用于与处理器耦合,其保存该终端设备必要的程序指令和数据。

第八方面,本申请提供了一种鉴权服务功能网元,该鉴权服务功能网元具有实现上述第二方面或第六方面中该方法的功能。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。该硬件和软件包括一个或多个与上述功能相对应的模块。

结合第八方面,在一种可能的设计中,鉴权服务功能网元的结构包括处理器和收发器,该处理器被配置为支持鉴权服务功能网元执行上述第二方面或第六方面中该的方法,该收发器用于支持鉴权服务功能网元与其他设备之间的通信。该鉴权服务功能网元还可以包括存储器,该存储器用于与处理器耦合,其保存该鉴权服务功能网元必要的程序指令和数据。

第九方面,本申请提供了一种应用的认证和密钥管理 AKMA 锚点功能网元,该 AKMA 锚点功能网元具有实现上述第三方面或第五方面中该方法的功能。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。该硬件和软件包括一个或多个与上述功能相对应的模块。

结合第九方面,在一种可能的设计中,AKMA 锚点功能网元的结构包括处理器和收发器,该处理器被配置为支持 AKMA 锚点功能网元执行上述第三方面或第五方面中该的方法,该收发器用于支持 AKMA 锚点功能网元与其他设备之间的通信。该 AKMA 锚点功能网元还可以包括存储器,该存储器用于与处理器耦合,其保存该 AKMA 锚点功能网元必要的程序指

令和数据。

第十方面，本申请提供了一种装置（例如，该装置可以是芯片系统），该装置包括处理器，可以执行上述第一方面至第六方面中该的任意一种或多种方法。

结合第十方面，在一种可能的设计中，该装置还包括存储器，用于保存必要的程序指令和数据。

第十一方面，本申请提供了一种计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面至第六方面中该的任意一种或多种方法。

第十二方面，本申请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指令，当其在计算机上运行时，使得计算机可以执行上述第一方面至第六方面中该的任意一种或多种方法。

第十三方面，本申请提供了一种通信系统，该系统包括上述第二方面所涉及的鉴权服务功能网元和上述第二方面所涉及的应用的认证和密钥管理 AKMA 锚点功能网元。

结合第十三方面，在一种可能的设计中，该系统还包括与第二方面所涉及的应用功能网元等其他设备。

附图说明

- 图 1 为一种 5G 系统的网络架构示意图；
- 图 2 为一种 AKMA 架构示意图；
- 图 3 为一种生成 AKMA 密钥的流程示意图；
- 图 4 为一种主鉴权的触发和执行流程示意图；
- 图 5 为一种 AKMA 流程示意图；
- 图 6 为场景 1 中 AKMA 流程中发生重鉴权的示意图；
- 图 7 为场景 2 中 AKMA 流程中发生重鉴权的示意图；
- 图 8 为本申请提供的一种密钥管理系统的架构示意图；
- 图 9 为本申请提供的另一种密钥管理系统的架构示意图；
- 图 10 为本申请提供的一种密钥管理方法的流程示意图；
- 图 11 为本申请提供的一种密钥管理方法的流程示意图；
- 图 12 为本申请提供的另一种密钥管理方法的流程示意图；
- 图 13 为本申请提供的另一种密钥管理方法的流程示意图；
- 图 14 为本申请提供的又一种密钥管理方法的流程示意图；
- 图 15 为本申请提供的再一种密钥管理方法的流程示意图；
- 图 16 为本申请提供的再一种密钥管理方法的流程示意图；
- 图 17 为本申请提供的再一种密钥管理方法的流程示意图；
- 图 18 为本申请还提供的一种密钥管理方法的流程示意图；
- 图 19 为本申请提供的一种通信装置的结构示意图；
- 图 20 为本申请提供的另一种通信装置的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例的技术方案进行描述。

本申请实施例的技术方案可以应用于各种通信系统，例如：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)、通用移动通信系统 (universal mobile telecommunication system, UMTS)、全球互联微波接入 (worldwide interoperability for microwave access, WiMAX) 通信系统、第五代 (5th generation, 5G) 系统或新无线 (new radio, NR) 等。

如图 1 所示, 为 5G 系统的网络架构示意图。5G 系统可包括终端设备、接入网和核心网。

其中, 终端设备是一种具有无线收发功能的设备, 可以部署在陆地上, 包括室内或室外、手持、穿戴或车载; 也可以部署在水面上 (如轮船等); 还可以部署在空中 (例如飞机、气球和卫星上等)。终端设备可以是手机 (mobile phone)、平板电脑 (Pad)、带无线收发功能的电脑、虚拟现实 (virtual reality, VR) 终端设备、增强现实 (augmented reality, AR) 终端设备、工业控制 (industrial control) 中的无线终端、车载终端设备、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、可穿戴终端设备等等。终端设备有时也可以称为终端、用户设备 (user equipment, UE)、接入终端设备、车载终端、工业控制终端、UE 单元、UE 站、移动站、移动台、远方站、远程终端设备、移动设备、UE 代理或 UE 装置等。终端设备也可以是固定的或者移动的。图 1 以及本申请中终端设备以 UE 为例进行介绍。

其中, 接入网用于实现接入有关的功能, 可以为特定区域的授权用户提供入网功能。接入网在终端设备与核心网之间转发控制信号和用户数据。接入网可以包括接入网络设备, 接入网络设备可以是为终端设备提供接入的设备, 可以包括无线接入网 (radio access network, RAN) 设备和 AN 设备。RAN 设备主要是 3GPP 网络中的无线网络设备, AN 设备可以是非 3GPP 定义的接入网络设备。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 5G 系统中, 称为 RAN 或者下一代基站 (next-generation Node basestation, gNB); 在 LTE 系统中, 称为演进的节点 B (evolved NodeB, eNB 或 eNodeB)。

其中, 核心网负责维护移动网络的签约数据, 为 UE 提供会话管理、移动性管理、策略管理以及安全认证等功能。核心网可以包括如下网元: 用户面功能 (user plane function, UPF)、认证服务功能 (authentication server function, AUSF)、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)、网络开放功能 (network exposure function, NEF)、网络功能仓储功能 (network function repository function, NRF)、策略控制功能 (policy control function, PCF)、统一数据管理 (unified data management, UDM) 和应用功能 (application function, AF)。

AMF, 主要负责移动网络中的移动性管理, 例如用户位置更新、用户注册网络、用户切换等。SMF, 主要负责移动网络中的会话管理, 例如会话建立、修改、释放。UPF, 负责终端设备中用户数据的转发和接收, 可以从数据网络接收用户数据, 通过接入网络设备传输给终端设备; 还可以通过接入网络设备从终端设备接收用户数据, 转发至数据网络。PCF, 主要支持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, 同时负责获取与策略决策相关的用户签约信息。AUSF, 用于执行 UE 的安全认证。NEF, 主要用于支持能力和事件的开放。NRF, 用于为其它网元提供网络功能实体信息的存储功能和选择功能。UDM, 用于存储用户数据, 例如签约数据、鉴权/授权数据等。AF 与 3GPP 核心网交互用于提供应用层服务, 例如提供关于应用层数据路由, 提供接入网络能力开放功能, 与策略框架进行交互以提供策略控制, 与 5G 网络的 IP 多媒体子系统 (IP multimedia subsystem, IMS) 交互等。

其中, 数据网络 (data network, DN) 用于为用户提供业务服务, 可以是私有网络, 例如局域网; 也可以是不受运营商管控的外部网络, 例如互联网 (Internet); 还可以是运营商共同

部署的专有网络，例如 IMS 的网络。终端设备可通过建立的协议数据单元（protocol data unit, PDU）会话，来访问 DN。

本申请实施例的技术方案涉及 AKMA（authentication and key management for applications）服务。支持 AKMA 服务的 UE 与支持 AKMA 服务的 AF 进行数据传输时，可以基于 AKMA 流程的安全保护以提高数据传输的安全性。相比于传统 UE 和 AF 的无保护的传输方法，使用 AKMA 可提高数据传输的安全性。

基于 5G 系统的网络架构，AKMA 架构定义了 AKMA 流程涉及的网元。如图 2 所示，为 AKMA 架构示意图。AKMA 架构包括 UE、（R）AN、AUSF、AMF、AF、NEF、AKMA 的锚点功能（AKMA anchor function, AAnF）和 UDM。

图 2 中，UE 与 AF 进行通信存在三种方式，一种是 UE 通过（R）AN 和 AMF 与 AF 进行通信，一种是 UE 通过 AMF 与 AF 进行通信，一种是 UE 通过 Ua*接口直接与 AF 进行通信。其中，Ua*接口为 UE 与 AF 之间的通信接口。

其中，UE 可以生成 AKMA 密钥和 AKMA 密钥标识信息，并向 AF 发起应用会话建立请求消息，该应用会话请求消息携带 AKMA 密钥标识信息。AF 可以使用 AKMA 密钥标识信息向 AAnF 请求 AF 与 UE 之间的通信密钥。AAnF 可以向 AUSF 请求 AKMA 密钥，并根据 AKMA 密钥生成 AF 与 UE 之间的通信密钥以及该通信密钥的有效时间。AUSF 可以生成 AKMA 密钥。AKMA 密钥例如可以是 Kakma，Kakma 也可以称为 AKMA 的根密钥；AKMA 密钥标识信息可以是任何用于标识该 AKMA 密钥的信息，例如可以是 A-KID（AKMA-Key identifier）或者 Kakma ID（Kakma identifier）；AF 与 UE 之间的通信密钥，例如可以是 Kaf。AF 使用 Kaf 与 UE 进行数据传输可以提高该 AF 与 UE 之间的数据传输的安全性。

示例性的，AUSF 和 UE 生成 AKMA 密钥（以 Kakma 为例）的过程可参见图 3 所示。该过程具体包括：

步骤 101：UE 和 AUSF 执行主鉴权流程（Primary Authentication）

主鉴权，即为 UE 向 5G 核心网的注册过程中，UE 对 AMF 和/或 AUSF 进行鉴权，AUSF 对 UE 进行鉴权的过程，也可以描述为双向鉴权，具体可参见图 4 所示的流程。具体可以是在注册过程中，核心网设备和终端通过消息交互，终端和核心网设备分别将对方提供的待验证参数，与自己生成的另一个参数进行对比，若对方提供的待验证参数与自身生成的参数相同，则终端和核心网设备之间的鉴权验证通过。

步骤 102：UE 使用主鉴权过程中生成的中间密钥（以 Kausf 为例）生成 Kakma 和 AKMA 密钥标识信息（以 A-KID 为例）

UE 在对 AMF 和/或 AUSF 进行鉴权之后，发起应用会话建立请求之前，使用主鉴权过程中生成的中间密钥如 Kausf，生成 Kakma 以及生成 AKMA 密钥标识信息如 A-KID。

步骤 103：AUSF 使用 Kausf 生成 Kakma 和 A-KID

AUSF 对 UE 进行鉴权之后，AUSF 可以使用 Kausf，生成 Kakma，以及生成 A-KID。

需要说明的是，AUSF 可以是主鉴权流程后直接生成 Kakma 和 A-KID，也可以是在下述图 5 中 AAnF 向 AUSF 请求 Kakma 时生成 Kakma 和 A-KID，还可以在不同时刻分别生成 Kakma 和 A-KID，本申请对此不作限定。

可以理解的是，UE 和 AUSF 分别在本地生成相同的 Kausf、Kakma 以及 A-KID。

需要说明的是，步骤 102 和步骤 103 之间没有时序关系，可以步骤 102 先执行，步骤 103 后执行，或者步骤 103 先执行，步骤 102 后执行，又或者，可以步骤 102 和步骤 103 同时执行，本申请对此不作限制。

示例性的，主鉴权的触发和执行流程可参见图 4 所示，该流程具体包括：

步骤 201：UE 通过 RAN 向 AMF 发送注册请求（Registration Request）。

其中，注册请求携带 UE 的身份信息，AMF 根据 UE 的身份信息（例如隐藏的身份标识（subscriber concealed identifier, SUCI））选择 AUSF。

在鉴权场景下，AMF 可以称为安全锚点功能（Security Anchor Function, SEAF）网元，也就是说，本申请实施例中的 AMF 皆可以替换为 SEAF。

步骤 202：AMF 向 AUSF 发送 UE 认证鉴权请求消息（UEAuthentication_Authenticate Request message）。

其中，UE 认证鉴权请求消息携带 UE 的身份信息。

步骤 203：AUSF 向 UDM 发送 UE 鉴权获取请求（UEAuthentication_Get Request）消息，触发主鉴权流程。

UE 鉴权获取请求消息中携带 UE 的身份信息。当身份信息为 SUCI 时，UDM 解析 SUCI 并获得 UE 的永久身份标识，并查找 UE 的根密钥。

步骤 204：UDM 向 AUSF 发送 UE 鉴权获取请求消息的响应消息（Authentication_Get response）

步骤 205：AUSF 向 AMF 发送 UE 认证鉴权请求消息的响应消息（UEAuthentication_Authenticate Response）。UE 认证鉴权请求消息的响应消息携带 AMF 的鉴权参数。

步骤 206：AMF 向 UE 发送第一鉴权请求（Authentication-Request）消息。第一鉴权请求消息携带 AMF 的鉴权参数。

步骤 207：UE 使用本地保存的根密钥计算鉴权参数，并校验 AMF 的鉴权参数，校验通过代表核心网可信。校验通过后，UE 向 AMF 发送第一鉴权请求消息的响应消息（Authentication Response），第一鉴权请求消息的响应消息中携带 UE 的鉴权参数。AMF 根据 UE 的鉴权参数，确定鉴权中 AMF 没有欺骗 AUSF。

步骤 208：AMF 向 AUSF 发送第二鉴权请求（UEAuthentication_Authenticate Request message）消息，第二鉴权请求消息携带 UE 的鉴权参数，AUSF 校验 UE 的鉴权参数，校验成功则代表鉴权成功。

步骤 209：AUSF 根据 UE 的鉴权参数对 UE 进行鉴权，并向 AMF 发送第二鉴权请求消息的响应消息（UEAuthentication_Authenticate Response），告知 AMF AUSF 对 UE 鉴权的结果。

上述主鉴权流程中，AUSF 和 UE 生成 Kausf，可用于 AUSF 和 UE 生成 Kakma，具体可参见图 3 所示的过程。

需要说明的是，上述主鉴权流程（即步骤 204-209）是对现有技术中 5G 网络的主鉴权流程的一个简要介绍。5G 网络的主鉴权流程具体细节可参考 5G AKA（authentication and key agreement）流程或 EAP-AKA'（Extensible Authentication Protocol-Authentication and Key Agreement）流程。LTE 网络的主鉴权流程具体细节可参考 EPS（evolved packet system）AKA 流程，本申请不作赘述。

示例性的，AKMA 的流程可参见图 5 所示，该流程具体包括：

步骤 301：UE 和 AUSF 执行主鉴权，并生成 Kakma 和 Kakma 对应的 A-KID。

主鉴权流程以及生成 Kakma 和 A-KID 可参考图 3 和图 4 中的描述，此处不作赘述。

在 UE 生成 Kakma 和 A-KID 后, AAnF 可能会保存 Kakma 和 A-KID。

步骤 302: UE 向 AF 发送应用会话建立请求(例如 application session establishment request)。

其中, 应用会话建立请求携带 A-KID。

步骤 303: AF 在收到应用会话建立请求后, 向 AAnF 发送 Kaf 请求消息(例如 key request)。

其中, Kaf 请求消息携带 A-KID 和应用服务功能网元的标识信息, 应用服务功能网元的标识信息例如可以是 AF ID。

步骤 304: 若 AAnF 保存有 A-KID 对应的 Kakma, 那么 AAnF 直接根据 Kakma 和 AF ID 生成 Kaf 和 Kaf 的有效时间, 并执行步骤 307-311。

若 AAnF 未保存 A-KID 对应的 Kakma, 那么执行步骤 305-311。

步骤 305: AAnF 向 AUSF 发送 Kakma 密钥请求(例如 AKMA key request)。

Kakma 密钥请求携带 A-KID。

步骤 306: AUSF 根据 A-KID 查找对应的 Kakma, 向 AAnF 发送 Kakma 密钥请求的响应消息(例如 AKMA key response)。

Kakma 密钥请求的响应消息携带 Kakma。

步骤 307: AAnF 使用 Kakma 推演 Kaf, 进一步的 AAnF 还会生成 Kaf 的有效时间。

步骤 308: AAnF 向 AF 发送 Kaf 请求消息的响应消息(例如 key response)。

其中, Kaf 请求消息的响应消息携带 Kaf 和 Kaf 的有效时间。

步骤 309: AF 在接收到 Kaf 请求消息的响应消息之后, 向 UE 发送应用会话建立请求的响应消息(例如 application session establishment response)。

步骤 310: UE 接收应用会话建立请求的响应消息后, 可以使用 Kakma 推演 Kaf。

需要说明的是, UE 推演 Kaf 可以在接收应用会话建立请求的响应消息后, 或者可以在发送应用会话建立请求之后, 又或者可以在发送应用会话建立请求之前, 本申请对此不作限定。

对于不同 AF 与同一 UE 之间的 Kaf 可以不同, 例如 AF1 与 UE1 之间的 Kaf 为 Kaf1, AF2 与 UE1 之间的 Kaf 为 Kaf2。

步骤 311: UE 和 AF 之间使用 Kaf 进行数据传输或者身份鉴权, 从而提高 AF 与 UE 之间的数据传输的安全性。

本申请实施例的技术方案还涉及重鉴权, 即 UE 对核心网设备(在 5G 中例如可以是 AMF 和/或 AUSF)再次进行鉴权, 核心网设备(在 5G 中例如可以是 AUSF)对 UE 再次进行鉴权。具体可以是核心网设备(在 5G 中例如可以是 AMF)发现某种参数即将无法使用从而触发对 UE 的重鉴权, 某种参数即将无法使用例如可以是 NAS(non-access stratum) COUNT 即将翻转, 或者是根据运营商的配置要求达到了核心网设备(在 5G 中例如可以是 AMF)对 UE 再次进行鉴权的触发条件。核心网设备对终端进行重鉴权的过程中, 核心网设备和终端会进行消息交互, 终端和核心网设备分别将对方提供的待验证参数, 与自己生成的另一个参数进行对比, 若对方提供的待验证参数与自身生成的参数相同, 则终端和核心网设备之间的鉴权验证通过。5G 重鉴权流程的具体步骤可参考图 4 所示的步骤 202-209。可以理解的是, 重鉴权就是在发生过主鉴权之后, 由核心网设备再次为这个 UE 发起主鉴权的过程, 本申请中的重鉴权是核心网设备发起的, 而 UE 注册过程中的主鉴权是由 UE 向核心网设备发送注册请求, 再由核心网设备发起的。重鉴权之后, UE 和 AUSF 会生成新的 Kausf, 旧的 Kausf 会被删除。相应的, 重鉴权之后, 旧的 Kakma 和 A-KID 会被删除, UE 有发起新的应用会话建立请求消息需求时, 会生成新的 Kakma 和 A-KID。

在 AKMA 流程中, Kakma 的生存周期可以与 UE 再次发生主鉴权的间隔周期相同。比

如，UE 第一次发生了主鉴权，并生产了 Kakma。那么 Kakma 会一直保存到重鉴权发生时。因为重鉴权的发生无法明确判断，因此 Kakma 的保存时间也无法判断。而 Kaf 是有一个明确的有效时间的，进而造成了 Kakma 和 Kaf 的过期时间是解耦的，没有办法互相影响。

目前的 AKMA 流程未考虑重鉴权的发生，进而没有考虑到重鉴权会生成新的 Kakma 和 A-KID 所导致的问题。

具体的，在 5G 网络中存在 UE 可以通过 3GPP 接入技术单接入 5G 核心网的场景。在这个场景下，UE 和 5G 核心网之间交互控制面消息和用户面消息。AKMA 业务属于用户面业务，主鉴权和重鉴权属于控制面流程。当 UE 处于连接态后，可能出现 UE 和核心网之间一边进行 AKMA 业务，核心网一边发起对 UE 发起重鉴权过程。UE 侧保存的 Kakma 和 AUSF 侧保存的 Kakma，或者 UE 侧生成的 Kaf 和 AAnF 生成的 Kaf 会存在失步的可能。失步，即代表 UE 侧保存的 Kakma 和 AUSF 侧保存的 Kakma 不一样，或者 UE 生成的和 AF 获得的 Kaf 是不一样的。

在 5G 网络中还存在 UE 可以同时通过 3GPP 接入技术和 non-3GPP 接入技术多接入 5G 核心网的场景。在这个场景下，UE 可以同时使用 2 种接入技术时会有如下场景发生：1：UE 通过一种接入技术与 5G 核心网交互控制面 NAS 消息，UE 通过另一个接入技术传递用户面数据；2：UE 同时使用 2 种技术传递不同的 DN 对应的用户面数据；3：UE 同时使用 2 种接入技术与 5G 核心网交互控制面 NAS 消息。同样的，因为 AKMA 业务属于用户面业务，主鉴权和重鉴权属于控制面流程，那么针对场景 1 就可能出现 UE 一边发起 AKMA 业务，核心网一边发起对 UE 的重鉴权过程。UE 侧保存的 Kakma 和 AUSF 侧保存的 Kakma，或者 UE 侧生成的 Kaf 和 AAnF 生成的 Kaf 会存在失步的可能。

针对上述 UE 侧生成的 Kaf 和 AAnF 生成的 Kaf 失步，本申请实施例提供以下具体场景：

场景 1：UE 侧生成了一个新的 Kakma（记为 Kakma-2），并用新的 Kakma 生成 Kaf-2，但是 AAnF 却在使用旧的 Kakma（记为 Kakma-1）生成 Kaf-1。

比如，对应 AAnF 未保有 A-KID-1 对应的 Kakma-1 的情形，UE 发送了应用会话建立请求消息，AAnF 向 AUSF 请求 Kakma-1 完成后，即 AAnF 得到了 Kakma-1 后发生了重鉴权，AAnF 使用 Kakma-1 生成 Kaf-1，而 UE 接收应用会话建立请求消息后使用新的 Kakma 生成的是 Kaf-2；

或者，对应 AAnF 保有 A-KID-1 对应的 Kakma-1 的情形，UE 发送了应用会话建立请求消息，AAnF 直接生成 Kaf-1 后发生了重鉴权，而 UE 接收应用会话建立请求消息后使用新的 Kakma 生成的是 Kaf-2；

场景 2：UE 侧使用 Kakma-1 生成 Kaf-1，但是 AAnF 却无法使用 A-KID-1 找到 Kakma-1。

比如，对应 AAnF 未保有 A-KID-1 对应的 Kakma-1 的情形，UE 发送了应用会话建立请求消息后，AAnF 向 AUSF 请求 Kakma-1 前发生了重鉴权，AUSF 上的 Kakma-1 被删除，AAnF 无法使用 A-KID-1 找到 Kakma-1，而 UE 可以在发送了应用会话建立请求消息后重鉴权前生成 Kaf-1；

或者，对应 AAnF 保有 A-KID-1 对应的 Kakma-1 的情形，UE 发送了应用会话建立请求消息后，AAnF 生成 Kaf-1 前发生了重鉴权，AAnF 上的 Kakma-1 被删除，而 UE 可以在发送了应用会话建立请求消息后重鉴权前生成 Kaf-1。

场景 3：UE 侧使用 Kakma-1 生成 Kaf-1-1，但是 AAnF 却使用 Kakma-2 生成 Kaf-2。

比如，对应 AAnF 未保有 A-KID-1 对应的 Kakma-1 的情形，UE 发送了应用会话建立请

求消息后, AAnF 向 AUSF 请求 Kakma-1 之前发生重鉴权, AUSF 仍保存 A-KID-1 却生成了 Kakma-2, AUSF 误以为 A-KID-1 对应 Kakma-2, 相应返回给 AAnF 的是 Kakma-2。

这种极端情况可能发生在 UE 首次请求一个 AF 的 AKMA 业务, 但却不巧的伴随着重鉴权的发生

如图 6 所示, 为场景 1 中 AKMA 流程中发生重鉴权的过程。该过程具体包括如下步骤:

步骤 401: UE 和 AUSF 执行主鉴权流程。

UE 与 AUSF 执行主鉴权流程, 可参考图 3 和图 4 中对主鉴权流程的详细描述, 在此不再赘述。

步骤 402: UE 生成 Kakma-1 和 A-KID-1。

其中, A-KID-1 用于标记重鉴权前为 Kakma-1 生成的密钥标识信息。UE 在主鉴权流程之后, 使用主鉴权流程中生成的 Kausf 生成 Kakma-1, 为 Kakma-1 生成 A-KID-1。

UE 生成的 A-KID 具有唯一性, 即 A-KID 具有全球唯一性, 一个 A-KID 用于唯一标识一个 Kakma, 不同 Kakma 对应不同的 A-KID。

步骤 403: UE 向 AF1 发起应用会话请求, A-KID-1 携带在应用会话请求中。

其中, AF1 用于标记重鉴权前 UE 请求建立应用会话的应用功能网元。应用会话请求例如是 application session establishment request。

步骤 404: AF1 收到应用会话请求后向 AAnF 请求 Kaf-1。

对于服务化的接口, AF1 向 AAnF 请求 Kaf 的请求消息为服务化消息, 该请求消息的名称为服务化消息名称, 具体可以为 key request。该请求消息携带 A-KID-1 和 AF 的标识, AF 的标识例如可以是 AF ID (identifier)。

步骤 405: 如果 AAnF 处有保存 A-KID-1 对应的 Kakma-1, 则 AAnF 直接生成 Kaf-1 和 Kaf-1 的有效时间, 并执行步骤 409 至 414。如果 AAnF 处没有 A-KID-1 对应的 Kakma-1, 则 AAnF 向 AUSF 请求 Kakma-1, 并执行步骤 406 至 414。

对于服务化的接口, AAnF 向 AUSF 请求 Kakma-1 的请求消息为服务化消息, 该请求消息的名称为服务化消息名称, 具体可以为 AKMA key request。该请求消息携带 A-KID-1。

步骤 406: AUSF 根据 A-KID-1, 找到对应的 Kakma-1。

步骤 407: AUSF 将 Kakma-1 发送给 AAnF。

具体的, Kakma-1 可以携带在 AKMA Key Response 消息中发送给 AAnF。

步骤 408: AAnF 使用 Kakma 生成 Kaf-1 和 Kaf-1 的有效时间。

步骤 409: AAnF 将生成的 Kaf-1 和 Kaf-1 的有效时间发送给 AF1。

具体的, Kaf-1 和 Kaf-1 的有效时间可以携带在 Key response 消息中发送给 AF1。

步骤 410: UE 和 AUSF 之间发生重鉴权。

步骤 411: 重鉴权后, UE 侧的 Kakma-1 和 A-KID-1 会被删除, 若重鉴权成功后, UE 侧会生成 Kakma-2。

步骤 412: AF1 在收到 Kaf 和 Kaf 的有效时间后, 向 UE 发送应用会话建立响应。应用会话建立响应例如是 Application session establishment Response。

步骤 413: UE 接收应用会话建立响应, 如果 UE 侧密钥为 Kakma-2, 则 UE 推演出来 AF 密钥为 Kaf-2, 造成 UE 侧和 AF 侧的 Kaf 失步。如果 UE 侧 Kakma 被删除时, 则 UE 侧无法推演出来 Kaf。

步骤 414: 可选的, UE 和 AF2 发起应用会话建立协商过程, A-KID-2 会被 UE 携带向 AF2 发送的应用会话请求消息中。

如图 7 所示, 为场景 2 中 AKMA 流程中发生重鉴权的过程。该过程具体包括如下步骤:
步骤 501: UE 和 AUSF 执行主鉴权流程。

UE 与 AUSF 执行主鉴权流程, 可参考图 3 和图 4 中对主鉴权流程的详细描述, 在此不再赘述。

步骤 502: UE 生成 Kakma-1 和 A-KID-1。

UE 生成的 A-KID 具有唯一性, 即 A-KID 具有全球唯一性, 一个 A-KID 用于唯一标识一个 Kakma, 不同 Kakma 对应不同的 A-KID。

步骤 503: UE 向 AF1 发起应用会话请求, A-KID-1 携带在应用会话请求中。

其中, 应用会话请求例如是 application session establishment request。

步骤 504: UE 和 AUSF 之间发生重鉴权;

步骤 505: 重鉴权后, UE 侧和 AUSF 侧的 Kakma-1 和 A-KID-1 会被删除, 若重鉴权成功后, UE 侧和 AUSF 侧会生成 Kakma-2。

如果 AAnF 在重鉴权前保有 Kakma-1 和 A-KID-1, 重鉴权之后, AAnF 中的 Kakma-1 和 A-KID-1 会被删除, 若重鉴权成功后, AAnF 会获取 Kakma-2 和 A-KID-2。

步骤 506: AF1 收到应用会话请求后向 AAnF 请求 Kaf-1。

对于服务化的接口, AF1 向 AAnF 请求 Kaf-1 的请求消息为服务化消息, 该请求消息的名称为服务化消息名称, 具体可以为 key request。该请求消息携带 A-KID-1 和 AF 的标识。

步骤 507: 如果 AAnF 在重鉴权前保有 Kakma-1 和 A-KID-1, 因重鉴权后 AAnF 中的 Kakma-1 和 A-KID-1 被删除, AAnF 根据 A-KID-1 无法找到 Kakma-1, 导致 AF 侧的 Kaf 无法生成。

如果 AAnF 在接收 AF1 请求 Kaf-1 的请求消息时未保有 Kakma-1 和 A-KID-1, 则 AAnF 向 AUSF 请求 Kakma-1。对于服务化的接口, AAnF 向 AUSF 请求 Kakma-1 的请求消息为服务化消息, 该请求消息的名称为服务化消息名称, 具体可以为 AKMA key request。该请求消息携带 A-KID-1。因重鉴权后 AUSF 中的 Kakma-1 和 A-KID-1 被删除, AUSF 根据 A-KID-1 无法找到 Kakma-1, 进而导致 AF 侧的 Kaf 无法生成。

在一种实现方式中, AAnF 通过访问 UDM 查找 AUSF 的路由信息, 所需的标识信息为 A-KID-1。因重鉴权后 UDM 中关于 A-KID-1 的相关信息被删除, UDM 根据 A-KID-1 无法找到 AUSF 路由信息, 进而导致 AF 侧的 Kaf 无法生成。

根据上述图 6 或图 7 所示的流程可知, 当 UE 需要与 AF 建立应用通信时, UE 向 AF 发起应用连接建立流程。在 UE 侧和 AF 侧 Kaf 密钥协商完成之前, UE 和核心网发生重鉴权, 将导致重鉴权前生成的 Kakma 被删除, 进而导致 UE 生成的 Kaf 和 AF 获取的 Kaf 失步或者导致 AF 向 AAnF 请求 AF 密钥失败。在重鉴权场景下, 如何保证 UE 和 AF 侧成功协商 AF 密钥, 从而实现 UE 和 AF 之间的安全通信是亟待解决的技术问题。

鉴于此, 本申请提供密钥管理方法、设备及系统, 以保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥, 实现终端设备和应用功能网元之间的安全通信。

如图 8 所示, 为本申请提供的一种密钥管理系统的架构示意图。该系统包括至少一个终端设备和至少一个应用功能网元。终端设备的描述可参见前述 5G 系统中对终端设备的具体描述。应用功能网元可以是 5G 系统中的 AF, 也可以是未来通信系统中用于实现 AF 全部或部分功能的网元。

在一种可能的实现方式中, 终端设备用于向应用功能网元发送第一应用会话建立请求消

息，第一应用会话建立请求消息携带第一密钥的标识信息，第一密钥为应用的认证和密钥管理 AKMA 密钥；接收重鉴权流程中的第一鉴权请求消息；发送重鉴权流程中的第一鉴权请求消息的响应消息；接收来自应用功能网元的第一应用会话建立请求消息的响应消息；以及使用第一密钥推演终端设备和应用功能网元之间的通信密钥。

应用功能网元接收来自终端设备的第一应用会话建立请求消息；以及向终端设备发送第一应用会话建立请求消息的响应消息。

具体的，终端设备发送第一鉴权请求消息的响应消息后，可以不删除第一密钥和第一密钥的标识信息。

在这种方式中，发送重鉴权后，终端设备仍使用重鉴权前生成的第一密钥推演终端设备和应用功能网元之间的通信密钥，保证和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

在另一种可能的实现方式中，终端设备用于向应用功能网元发送第一应用会话建立请求消息，第一应用会话建立请求消息携带第一密钥的标识信息，第一密钥为应用的认证和密钥管理 AKMA 密钥；终端设备接收重鉴权流程中的第一鉴权请求消息；发送重鉴权流程中的第一鉴权请求消息的响应消息；接收来自应用功能网元的第一应用会话建立请求消息的响应消息；向应用功能网元发送第二应用会话建立请求消息，第二应用会话建立请求消息携带第二密钥的标识信息，第二密钥为重鉴权流程后生成的 AKMA 密钥。

应用功能网元接收来自终端设备的第一应用会话建立请求消息；向终端设备发送第一应用会话建立请求消息的响应消息；以及接收来自终端设备的第二应用会话建立请求消息。

在这种方式中，发生重鉴权前，终端设备使用重鉴权前生成的第一密钥的标识信息和应用功能网元发起应用会话建立流程，发送重鉴权后，终端设备使用重鉴权后生成的第二密钥的标识信息重新和该应用功能网元发起应用会话建立流程，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

如图 9 所示，为本申请提供的另一种密钥管理系统的架构示意图。该系统包括至少一个鉴权服务功能网元和至少一个 AKMA 锚点功能网元。鉴权服务功能网元可以是 5G 系统中的 AUSF，也可以是未来通信系统中用于实现 AUSF 全部或部分功能的网元。AKMA 锚点功能网元可以是 5G 系统中的 AAnF，也可以是未来通信系统中用于实现 AAnF 全部或部分功能的网元。

其中，鉴权服务功能网元，用于接收重鉴权流程中的第二鉴权请求；发送重鉴权流程中的第二鉴权请求的响应消息；接收来自 AKMA 锚点功能网元的第一密钥请求消息，第一密钥请求消息携带第一密钥的标识信息，第一密钥为重鉴权流程前生成的 AKMA 密钥；以及向 AKMA 锚点功能网元发送第一密钥。

AKMA 锚点功能网元用于接收来自应用服务功能网元的第一请求消息，第一请求消息用于请求终端设备和应用功能网元之间的通信密钥；向鉴权服务功能网元发送第一密钥请求消息；接收来自鉴权服务功能网元的第一密钥；使用第一密钥推演终端设备和应用功能网元之间的通信密钥；以及向应用服务功能网元发送终端设备和应用功能网元之间的通信密钥。

具体的，鉴权服务功能网元用于发送第二鉴权请求的响应消息后，不删除第一密钥和第一密钥的标识信息。

在一种可能的实现方式中，该系统还包括至少一个应用服务功能网元。应用功能网元可

以是 5G 系统中的 AF，也可以是未来通信系统中用于实现 AF 全部或部分功能的网元。应用服务功能网元用于接收来自终端设备的第一应用会话建立请求消息，第一应用会话建立请求消息携带第一密钥的标识信息；向 AKMA 锚点功能网元发送第一请求消息；接收来自 AKMA 锚点功能网元的终端设备和第一应用功能网元之间的通信密钥；以及向终端设备发送第一应用会话建立请求消息的响应消息。

该系统中，发送重鉴权后，鉴权服务功能网元仍向 AKMA 锚点功能网元发送重鉴权前生成的第一密钥，以使 AKMA 锚点功能网元使用第一密钥生成终端设备和应用功能网元之间的通信密钥，保证终端设备生成的终端设备和应用功能网元之间的通信密钥和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

下面将结合图 8 所示的网络架构，对本申请提供一种密钥管理方法进行介绍。

如图 10 所示，为本申请提供的一种密钥管理方法的流程示意图，该流程可包括但不限于如下步骤：

步骤 601：终端设备向第一应用功能网元发送第一应用会话建立请求消息。

其中，第一应用会话建立请求消息携带第一密钥的标识信息，第一密钥为 AKMA 密钥。

在一种实现方式中，终端设备将第一密钥的标识信息保存在第一应用会话的上下文中，也可以说，终端设备将第一密钥的标识信息和第一应用会话进行关联，即终端设备保存第一密钥的标识信息和第一应用会话的对应关系。

步骤 602：收到第一应用会话建立请求消息后，第一应用功能网元向 AKMA 锚点功能网元发送第一请求消息。

其中，第一请求消息用于请求终端设备和第一应用功能网元之间的通信密钥。第一请求消息携带第一密钥的标识信息和第一应用功能网元的标识信息。

步骤 603：收到第一请求消息后，如果 AKMA 锚点功能网元处保存第一密钥的标识信息和第一密钥的对应关系，则 AKMA 锚点功能网元根据第一密钥的标识信息确定第一密钥，直接使用确定的第一密钥生成终端设备和第一应用功能网元之间的通信密钥，并继续执行步骤 607-612，可选的，AKMA 锚点功能网元处还生成终端设备和第一应用功能网元之间的通信密钥的有效时间；

如果 AKMA 锚点功能网元处未保存第一密钥的标识信息和第一密钥的对应关系，则 AKMA 锚点功能网元向鉴权服务功能网元发送第一密钥请求消息并继续执行步骤 604-612，第一密钥请求消息携带第一密钥的标识信息。

在一种实现方式中，AKMA 锚点功能网元除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外，还可以使用第一密钥的标识信息中的部分或全部，或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。AKMA 锚点功能使用第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥，可以实现对于不同应用功能网元与同一终端设备之间的通信密钥不同，例如第一应用功能网元与终端设备之间的通信密钥为第一通信密钥，第二应用功能网元与该终端设备之间的通信密钥为不同于第一通信密钥的第二通信密钥。

步骤 604：收到第一密钥请求消息后，鉴权服务功能网元根据第一密钥的标识信息，确定第一密钥。

需要说明的是，鉴权服务功能网元可以在收到第一密钥请求消息后，生成第一密钥；或

者在主鉴权流程后，根据主鉴权流程中生成的中间密钥直接生成第一密钥。本申请对鉴权服务功能网元生成第一密钥的时间不作限定。

步骤 605：鉴权服务功能网元向 AKMA 锚点功能网元发送第一密钥。

步骤 606：AKMA 锚点功能网元使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

可选的，还生成终端设备和第一应用功能网元之间的通信密钥的有效时间。

在一种实现方式中，AKMA 锚点功能网元除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外，还可以使用第一密钥的标识信息中的部分或全部，或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。具体可参考步骤 603 中的描述，此处不作赘述。

步骤 607：AKMA 锚点功能网元向第一应用功能网元发送终端设备和第一应用功能网元之间的通信密钥。

可选的，AKMA 锚点功能网元还向第一应用功能网元发送终端设备和第一应用功能网元之间的通信密钥的有效时间。

步骤 608：发生重鉴权，其中，终端设备接收重鉴权流程中的第一鉴权请求消息。

重鉴权流程具体可参考图 2 中步骤 204-209，第一鉴权请求消息例如可以是图 2 中步骤 206 中的第一鉴权请求消息。终端设备接收重鉴权流程中来自安全锚点功能网元的第一鉴权请求消息。

步骤 609：终端设备发送重鉴权流程中的第一鉴权请求消息的响应消息。

其中，第一鉴权请求消息的响应消息例如可以是图 2 步骤 207 中的第一鉴权请求消息的响应消息。

在一种实现方式中，终端设备发送第一鉴权请求消息的响应消息后，保存发送第一应用会话建立请求消息和重鉴权流程的先后关系，具体可以保存在终端设备的上下文中，即将第一应用会话建立请求消息和重鉴权流程的先后关系与终端设备进行关联。

在一种实现方式中，终端设备发送第一鉴权请求消息的响应消息后，不删除第一密钥和第一密钥的标识信息。

具体的，终端设备确定不删除第一密钥和第一密钥的标识信息的触发条件可以是以下任意一项或多项：（1）重鉴权成功；（2）重鉴权流程之前终端设备发送第一应用会话建立请求，且未收到第一应用会话建立请求消息的响应消息；（3）当重鉴权流程之前终端设备发送第一应用会话建立请求，且收到第一应用会话建立请求消息的响应消息但不存在终端设备和第一应用功能网元之间的通信密钥；（4）不存在可用的终端设备和第一应用功能网元之间的通信密钥。

也就是说，当重鉴权成功，终端设备确定不删除第一密钥和第一密钥的标识信息；或者当重鉴权流程之前终端设备发送第一应用会话建立请求，且未收到第一应用会话建立请求消息的响应消息，终端设备确定不删除第一密钥和第一密钥的标识信息；或者当重鉴权流程之前终端设备发送第一应用会话建立请求，且收到第一应用会话建立请求消息的响应消息但未推演终端设备和第一应用功能网元之间的通信密钥，终端设备确定不删除第一密钥和第一密钥的标识信息；或者不存在终端设备和第一应用功能网元之间的通信密钥，终端设备确定不删除第一密钥和第一密钥的标识信息。

也就是说，终端设备确定重鉴权成功，从而确定不删除第一密钥和第一密钥的标识信息；或者终端设备确定当重鉴权流程之前终端设备发送第一应用会话建立请求，且未收到第一应

用会话建立请求消息的响应消息，从而确定不删除第一密钥和第一密钥的标识信息；或者终端设备确定重鉴权流程之前终端设备发送第一应用会话建立请求，且收到第一应用会话建立请求消息的响应消息但不存在终端设备和第一应用功能网元之间的通信密钥，从而确定不删除第一密钥和第一密钥的标识信息；或者终端设备确定不存在终端设备和第一应用功能网元之间的通信密钥，从而确定不删除第一密钥和第一密钥的标识信息。

在一种实现方式中，终端设备发送第一鉴权请求消息的响应消息后，生成第二密钥和第二密钥的标识信息，第二密钥为 AKMA 密钥。可以理解的是，第一密钥为重鉴权流程前生成的 AKMA 密钥，第二密钥为重鉴权流程后生成的 AKMA 密钥。需要说明的是，本申请中生成第二密钥和第二密钥的标识信息表示第二密钥和第二密钥的标识信息可以在同一时刻生成，也可以表示在不同时刻生成。相应的，生成第一密钥和第一密钥的标识信息表示第一密钥和第一密钥的标识信息可以在同一时刻生成，也可以表示在不同时刻生成。相应的，删除第一密钥和第一密钥的标识信息表示第一密钥和第一密钥的标识信息可以在同一时刻删除，也可以表示在不同时刻删除，本申请对此不作限定。该种方式中，终端设备同时保存第二密钥和第二密钥的标识信息，以及第一密钥和第一密钥的标识信息。

或者，在另一种实现方式中，终端设备发送第一鉴权请求消息的响应消息后，确定在重鉴权之前有发起第一应用会话建立请求，暂缓向除第一应用功能网元之外的其他应用功能网元发起应用会话建立请求，直到终端设备和第一应用功能网元完成通信密钥的协商。这种情况下，第一应用会话建立请求流程中，终端设备只需保存第一密钥和第一密钥标识符。等到终端设备和第一应用功能网元完成通信密钥的协商，向其他应用功能网元时发起应用会话建立请求时，终端设备再生成第二密钥。这样，不会存在终端设备上存在多个 AKMA 密钥的情况，节省了终端设备的存储空间，避免了终端设备选择哪一个 AKMA 密钥的判断动作。

需要注意的是，如果在步骤 603 中，AKMA 锚点功能网元处保存第一密钥的标识信息和第一密钥的对应关系，则步骤 608-609 在步骤 603 之后执行；如果在步骤 603 中，AKMA 锚点功能网元处未保存第一密钥的标识信息和第一密钥的对应关系，则步骤 608-609 在步骤 605 之后执行。也就是说，步骤 608-609 和步骤 606-607 之间没有时序关系，既可以步骤 608-609 先执行，步骤 606-607 后执行，也可以步骤 606-607 后执行，步骤 608-609 先执行，又可以步骤 606-607 和步骤 608-609 同时执行，本申请对此不作限定。

步骤 610：第一应用功能网元向终端设备发送第一应用会话建立请求消息的响应消息。

终端设备接收第一应用会话建立请求消息的响应消息后，确定使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

在终端设备上存在第一密钥和第一密钥的标识信息以及第二密钥和第二密钥的标识信息时，终端设备确定使用第一密钥推演终端设备和第一应用功能网元之间的通信密钥可以通过以下方式中的任意一项或多项：（1）当第一应用会话建立请求消息为重鉴权流程前发送的，终端设备确定使用第一密钥推演终端设备和第一应用功能网元之间的通信密钥；（2）当第一应用会话建立请求消息携带的是第一密钥的标识信息，终端设备确定使用第一密钥推演终端设备和第一应用功能网元之间的通信密钥。需要说明的是，对于重鉴权流程后发送的应用会话请求，终端设备确定使用第二密钥推演终端设备和第一应用功能网元之间的通信密钥。

也就是说，终端设备确定第一应用会话建立请求消息为重鉴权流程前发送的，从而确定使用第一密钥推演终端设备和第一应用功能网元之间的通信密钥；或者终端设备确定第一应用会话建立请求消息携带的是第一密钥的标识信息，从而确定使用第一密钥推演终端设备和第一应用功能网元之间的通信密钥。

步骤 611: 接收第一应用会话建立请求消息的响应消息后, 终端设备使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥, 并使用该通信密钥和第一应用功能网元进行安全通信。

在一种实现方式中, 终端设备除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外, 还可以使用第一密钥的标识信息中的部分或全部, 或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。具体可参考步骤 603 中的描述, 此处不作赘述。

在一种实现方式中, 步骤 611 之后, 终端设备删除第一密钥和第一密钥的标识信息, 其中, 终端设备删除第一密钥和第一密钥的标识信息可以通过以下方式中的任意一项或多项:

(1) 当携带第一密钥的标识信息的应用会话请求消息都得到了响应, 终端设备删除第一密钥和第一密钥的标识信息; (2) 当终端设备未得到响应消息的应用会话请求消息都为重鉴权流程之后发送的, 终端设备删除第一密钥和第一密钥的标识信息。

也就是说, 终端设备确定携带第一密钥的标识信息的应用会话请求消息都得到了响应(或者说重鉴权前发出的应用会话建立流程都已完成), 从而删除第一密钥和第一密钥的标识信息; 或者终端设备确定未得到响应消息的应用会话请求消息都为重鉴权流程之后发送的(或者说未完成的应用会话建立流程都是重鉴权后发起的), 从而删除第一密钥和第一密钥的标识信息。

例如, 终端设备向第一应用功能网元发送第一应用会话建立请求消息并携带第一密钥的标识信息, 向第三应用功能网元发送第三应用会话建立请求消息并携带第一密钥的标识信息。重鉴权之后, 终端设备已经收到来自第一应用功能网元的第一应用会话建立请求消息的响应消息和来自第三应用功能网元的第三应用会话建立请求消息的响应消息, 并无其他携带第一密钥的标识信息的应用会话建立请求没有得到响应, 则终端设备删除第一密钥和第一密钥的标识信息。

又例如, 终端设备向第一应用功能网元发送第一应用会话建立请求消息并携带第一密钥的标识信息, 重鉴权之后, 向第三应用功能网元发送第三应用会话建立请求消息并携带第二密钥的标识信息。终端设备已经收到来自第一应用功能网元的第一应用会话建立请求消息的响应消息, 还未收到来自第三应用功能网元的第三应用会话建立请求消息的响应消息, 未得到响应消息的应用会话请求消息为重鉴权流程之后发送的, 则终端设备删除第一密钥和第一密钥的标识信息。

步骤 612: 可选的, 终端设备向第二应用功能网元发送第二应用会话建立请求消息, 第二应用会话建立请求消息携带第二密钥的标识信息。

该方法中, 发送重鉴权后, 终端设备仍使用重鉴权前生成的第一密钥推演终端设备和应用功能网元之间的通信密钥, 保证和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致, 从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥, 实现终端设备和应用功能网元之间的安全通信。

下面结合图 2 所示的网络架构, 为对图 10 中所提供的密钥管理方法进行详细的说明。如图 11 所示, 为本申请提供的一种密钥管理方法的流程示意图, 该流程可包括但不限于如下步骤:

步骤 701: UE 和 AUSF 执行主鉴权流程, 并且 UE 生成 Kakma-1 和 Kakma 对应的 A-KID-1。

主鉴权流程以及 UE 生成 Kakma 和 A-KID 可参考图 3 和图 4 中的描述, 此处不作赘述。

UE 生成的 A-KID 具有唯一性, 即一个 A-KID 用于标识一个 Kakma, A-KID 和 Kakma

具有一对一的关系，不同 Kakma 对应不同的 A-KID。

步骤 702: UE 向 AF1 发送第一应用会话请求消息，A-KID-1 携带在第一应用会话请求消息中。

其中，第一应用会话请求消息例如是 application session establishment request。

在一种实现方式中，UE 可以将 A-KID-1 保存在第一应用会话的上下文中，也可以说，UE 将 A-KID-1 和第一应用会话进行关联。

步骤 703: 收到第一应用会话请求消息后，AF1 向 AAnF 发送第一请求消息。

其中，第一请求消息用于请求 UE 和 AF1 之间的通信密钥 Kaf1，携带 A-KID-1 和 AF1 ID。

对于服务化的接口，第一请求消息为服务化消息，该请求消息的名称为服务化消息名称，具体可以为 key request。

步骤 704: 如果 AAnF 处保存 A-KID-1 和 Kakma-1 的对应关系，则 AAnF 根据 A-KID-1 确定 Kakma-1，直接使用 Kakma-1 生成 Kaf-1，并继续执行步骤 709 至 716，可选的，AAnF 还生成 Kaf-1 的有效时间。

如果 AAnF 处未保存 A-KID-1 和 Kakma-1 的对应关系，则 AAnF 向 AUSF 发送 Kakma-1 请求消息，并继续执行步骤 705 至 716，Kakma-1 请求消息携带 A-KID-1。

对于服务化的接口，AAnF 向 AUSF 请求 Kakma-1 的请求消息为服务化消息，该请求消息的名称为服务化消息名称，具体可以为 AKMA key request。

在一种实现方式中，AAnF 除了使用 Kakma-1 生成 Kaf-1 外，还可以使用 A-KID-1 中的部分或全部，或者 AF1 ID 中的部分或全部生成 Kaf-1。例如，AAnF 使用 A-KID-1 或者 A-TID (AKMA-temporary identifier) -1 推演 Kaf-1，A-KID-1 包括 A-TID-1，即 A-TID-1 为 A-KID-1 的部分。AKMA 锚点功能使用 AF1 ID 中的部分或全部生成 Kaf-1，可以实现对于不同 AF 与同一 UE 之间 Kaf 的不同，例如 AF1 与 UE 之间的 Kaf 为 Kaf-1，AF2 与 UE 之间的 Kaf 为 Kaf-2。

步骤 705: 收到 Kakma-1 请求消息后，AUSF 根据 A-KID-1，确定 Kakma-1。

需要说明的是，AUSF 可以在收到 Kakma-1 请求消息后，生成 Kakma-1；或者在主鉴权流程后，根据主鉴权流程中生成的 Kausf 直接生成 Kakma-1。

步骤 706: AUSF 向 AAnF 发送 Kakma-1。

具体的，Kakma-1 可以携带在 AKMA Key Response 消息中发送给 AAnF。

步骤 707: AAnF 使用 Kakma-1 生成 Kaf-1。

可选的，AAnF 还生成 Kaf-1 的有效时间。

在一种实现方式中，AAnF 除了使用 Kakma-1 生成 Kaf-1 外，还可以使用 A-KID-1 中的部分或全部，或者 AF1 ID 中的部分或全部生成 Kaf-1。具体可参考步骤 704 中的描述，此处不作赘述。

步骤 708: AAnF 向 AF1 发送 Kaf-1

可选的，AAnF 还向 AF1 发送 Kaf-1 的有效时间。

具体的，Kaf-1 (可选的还包括 Kaf-1 的有效时间) 可以携带在 Key response 消息中发送给 AF1。

步骤 709: 发生重鉴权流程，其中，UE 接收重鉴权流程中的第一鉴权请求消息。

重鉴权流程具体可参考图 2 中步骤 204-209，第一鉴权请求消息例如可以是图 2 中步骤 206 中的第一鉴权请求消息。UE 接收重鉴权流程中来自 AMF 的第一鉴权请求消息。

步骤 710: UE 发送重鉴权流程中的第一鉴权请求消息的响应消息。

其中, 第一鉴权请求消息的响应消息例如可以是图 2 步骤 207 中的第一鉴权请求消息的响应消息。

在一种实现方式中, UE 发送第一鉴权请求消息的响应消息后, 保存发送第一应用会话建立请求消息和重鉴权流程的先后关系, 具体可以保存在 UE 的上下文中, 即将第一应用会话建立请求消息和重鉴权流程的先后关系与 UE 进行关联。

在一种实现方式中, UE 发送第一鉴权请求消息的响应消息后, 不删除 Kakma-1 和 A-KID-1。

具体的, UE 不删除 Kakma-1 和 A-KID-1 的触发条件可以是以下任意一项或多项:

- (1) 重鉴权成功;
- (2) 在重鉴权之前 UE 发送第一应用会话请求消息, 且未收到第一应用会话建立请求消息的响应消息;
- (3) UE 上不存在可用的 Kaf-1。

其中, 当 UE 不删除 Kakma-1 和 A-KID-1 的触发条件包括上述 (1) 和 (3) 时, UE 确定重鉴权成功且 UE 上不存在可以用的 Kaf-1, 则删除 Kakma-1 和 A-KID-1; 或者当 UE 不删除 Kakma-1 和 A-KID-1 的触发条件包括上述 (2) 和 (3) 时, UE 确定在重鉴权之前发送第一应用会话请求消息, 未收到第一应用会话建立请求消息的响应消息, 且 UE 上不存在可用的 Kaf-1, 则删除 Kakma-1 和 A-KID-1。

其中, 当 UE 不删除 Kakma-1 和 A-KID-1 的触发条件包括上述 (2) 时, UE 可以根据所保存的发送第一应用会话建立请求消息和重鉴权流程的先后关系, 确定该条件是否满足。

需要说明的是, 触发条件可以是 UE 出厂时预配置在 UE 上, 也可以是网络通过配置信息配置在 UE 上, 又可以是 UE 在发送第一应用会话建立请求前或者发送第一应用会话建立请求后从别的设备处获取的, 本申请对此不作限制。

在一种实现方式中, UE 发送第一鉴权请求消息的响应消息后, 生成 Kakma-2 和 A-KID-2。可以理解的是, Kakma-1 为重鉴权流程前生成的 AKMA 密钥, Kakma-2 为重鉴权流程后生成的 AKMA 密钥。

或者, 在另一种实现方式, UE 发送第一鉴权请求消息的响应消息后, 确定在重鉴权前向 AF1 发起第一应用会话请求消息, 重鉴权后若需要向其他 AF (例如 AF3) 发起应用会话建立请求, 则暂缓向 AF3 发起的应用会话建立请求, 直到 UE 侧和 AF1 完成 Kaf-1 协商后再向 AF3 发起会话建立请求。在该方式中, 在 UE 侧和 AF1 进行 Kaf 协商的过程中, UE 保存 Kakma-1 和对应的 A-KID-1 以及重鉴权流程中产生的 Kausf, 在 UE 侧和 AF1 完成 Kaf 协商后以及向 AF3 发起会话建立请求前, 删除 Kakma-1 和对应的 A-KID-1, 并根据重鉴权流程中产生的 Kausf 生成 Kakma-2 和对应的 A-KID-2。这样, UE 在同一时刻保存一个 Kakma 和对应的 A-KID, 无需保存多个 Kakma 和对应多个 A-KID, 减轻 UE 存储多个 Kakma 和对应多个 A-KID 的负担。

关于步骤 709-710 的步骤与 707-708 之间的关系, 可参考步骤 609 中的描述, 此处不作赘述。

步骤 711: AF1 向 UE 发送第一应用会话建立请求消息的响应消息。

第一应用会话建立请求消息的响应消息例如是 Application session establishment Response。

UE 接收来自第一应用会话建立请求消息的响应消息后, 确定使用 Kakma-1 生成 Kaf-1。

UE 确定使用 Kakma-1 生成 Kaf-1 可以通过以下方式中的任意一项或多项: (1) 当第一应

用会话建立请求消息为重鉴权流程前发送的, UE 确定使用 Kakma-1 推演 Kaf-1; (2) 当第一应用会话建立请求消息携带的是 A-KID-1, UE 确定使用 Kakma-1 推演 Kaf-1。

步骤 712: 接收第一应用会话建立请求消息的响应消息后, UE 使用 Kakma-1 生成 Kaf-1, 并使用 Kaf-1 和 AF1 进行安全通信。

在一种实现方式中, UE 除了使用 Kakma-1 生成 Kaf-1 外, 还可以使用 A-KID-1 中的部分或全部, 或者 AF1 ID 中的部分或全部生成 Kaf-1。具体可参考步骤 704 中的描述, 此处不作赘述。

在一种实现方式中, 步骤 712 之后, UE 删除 Kakma-1 和 A-KID-1, 其中, UE 删除 Kakma-1 和 A-KID-1 通过以下方式中的任意一项或多项: (1) 当携带 A-KID-1 的应用会话请求消息都得到了响应, UE 删除 Kakma-1 和 A-KID-1; (2) 当 UE 未得到响应消息的应用会话请求消息都为重鉴权流程之后发送的, UE 删除 Kakma-1 和 A-KID-1。

步骤 713: 可选的, UE 向 AF2 发送第二应用会话建立请求消息, 第二应用会话建立请求消息携带 A-KID-2。

下面将结合图 9 所示的网络架构, 对本申请提供的另一种密钥管理方法进行介绍。

如图 12 所示, 为本申请提供的另一种密钥管理方法的流程示意图, 该流程可包括但不限于如下步骤:

步骤 801: 终端设备向第一应用功能网元发送第一应用会话建立请求消息。

其中, 第一应用会话建立请求消息携带第一密钥的标识信息, 第一密钥为 AKMA 密钥。

可以理解的是, 步骤 801 之前, 终端设备保存第一密钥和第一密钥的标识信息。

步骤 802: 可选的, 终端设备使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

如果终端设备生成终端设备和第一应用功能网元之间的通信密钥不需要第一应用会话建立请求消息的响应消息携带的参数, 则终端设备生成终端设备和第一应用功能网元之间的通信密钥的时间可以是终端设备生成第一密钥之后, 也可以是在终端设备向第一应用功能网元发送第一应用会话建立请求消息之后。这样, 终端设备生成终端设备和第一应用功能网元之间的通信密钥不会受到重鉴权的影响。

在一种实现方式中, 终端设备除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外, 还可以使用第一密钥的标识信息中的部分或全部, 或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。终端设备使用第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥, 可以实现对于不同应用功能网元与同一终端设备之间的通信密钥不同, 例如第一应用功能网元与终端设备之间的通信密钥为第一通信密钥, 第二应用功能网元与该终端设备之间的通信密钥为不同于第一通信密钥的第二通信密钥。

步骤 803: 发生重鉴权, 其中, 鉴权服务功能网元接收重鉴权流程中的第二鉴权请求。

重鉴权流程具体可参考图 2 中步骤 204-209, 第二鉴权请求消息例如可以是图 2 中步骤 208 中的第二鉴权请求消息。鉴权服务功能网元接收重鉴权流程中来自安全锚点功能网元的第二鉴权请求消息。

在一种实现方式中, 第二鉴权请求携带第一指示, 第一指示用于指示不删除第一密钥和第一密钥的标识信息。

其中, 第一指示可以是终端设备发送给安全锚点功能网元, 进而由安全锚点功能网元发送给鉴权服务功能网元。终端设备向鉴权服务功能网元发送第一指示的触发条件可以是以下

任意一项或多项：(1) 重鉴权成功；(2) 重鉴权流程之前终端设备发送第一应用会话建立请求，且未收到第一应用会话建立请求消息的响应消息；(3) 当重鉴权流程之前终端设备发送第一应用会话建立请求，且收到第一应用会话建立请求消息的响应消息但不存在终端设备和第一应用功能网元之间的通信密钥；(4) 不存在可用的终端设备和第一应用功能网元之间的通信密钥。

也就是说，终端设备确定重鉴权成功，从而向鉴权服务功能网元发送第一指示；或者终端设备确定当重鉴权流程之前终端设备发送第一应用会话建立请求，且未收到第一应用会话建立请求消息的响应消息，从而向鉴权服务功能网元发送第一指示；或者终端设备确定重鉴权流程之前终端设备发送第一应用会话建立请求，且收到第一应用会话建立请求消息的响应消息但不存在终端设备和第一应用功能网元之间的通信密钥，从而确定向鉴权服务功能网元发送第一指示；或者终端设备确定不存在终端设备和第一应用功能网元之间的通信密钥，从而确定向鉴权服务功能网元发送第一指示。

步骤 804：鉴权服务功能网元发送重鉴权流程中的第二鉴权请求消息的响应消息。

其中，第二鉴权请求消息的响应消息例如可以是图 2 步骤 209 中的第二鉴权请求消息的响应消息。

在一种实现方式中，鉴权服务功能网元发送第二鉴权请求的响应消息后，不删除第一密钥和第一密钥的标识信息。

其中，鉴权服务功能网元确定不删除第一密钥和第一密钥的标识信息可以通过以下方式中的任一项：(1) 鉴权服务功能网元接收来自终端设备的第一指示，根据第一指示，确定不删除删除第一密钥和第一密钥的标识信息。第一指示可以携带在步骤 803 中的第二鉴权请求消息中；(2) 当重鉴权流程成功，鉴权服务功能网元确定不删除第一密钥和第一密钥的标识信息，也就是说，鉴权服务功能网元确定重鉴权流程成功，从而确定不删除第一密钥和第一密钥的标识信息。

其中，鉴权服务功能网元不删除第一密钥和第一密钥的标识信息一段时间，该时间的长度可由运营商决定，本申请对此不作限定。

可选的，如果数据管理网元中保有第一密钥的标识信息或第一密钥相关的信息时，如鉴权服务功能网元的路由信息，数据管理网元也继续保有该信息一段时间。

在一种实现方式中，鉴权服务功能网元发送第二鉴权请求的响应消息后，生成第二密钥，第二密钥为 AKMA 密钥。可以理解的是，第一密钥为重鉴权流程前生成的 AKMA 密钥，第二密钥为重鉴权流程后生成的 AKMA 密钥。该方式中，鉴权服务功能网元同时保存第二密钥和第二密钥的标识信息，以及第一密钥和第一密钥的标识信息。

步骤 805：收到第一应用会话建立请求消息后，第一应用服务功能网元向 AKMA 锚点功能网元发送第一请求消息。

其中，第一请求消息用于请求终端设备和第一应用功能网元之间的通信密钥。第一请求消息携带第一密钥的标识信息和第一应用功能网元的标识信息。

步骤 806：收到第一请求消息后，如果 AKMA 锚点功能网元处未保存第一密钥的标识信息和第一密钥的对应关系，AKMA 锚点功能网元向鉴权服务功能网元发送第一密钥请求消息。第一密钥请求消息携带第一密钥的标识信息。

在一种实现方式中，AKMA 锚点功能网元可以通过访问数据管理网元查找鉴权服务功能网元的路由信息，查找鉴权服务功能网元的路由信息所需的标识信息为第一密钥的标识信息。

步骤 807：收到第一密钥请求消息后，鉴权服务功能网元根据第一密钥的标识信息，确定

第一密钥。

在一种实现方式中，鉴权服务功能网元同时保存第二密钥和第二密钥的标识信息，以及第一密钥和第一密钥的标识信息，鉴权服务功能网元根据第一密钥请求消息中的第一密钥的标识信息，确定第一密钥。

其中，鉴权服务功能网元可以在收到第一密钥请求消息后，生成第一密钥；或者在主鉴权流程后，根据主鉴权流程中生成的中间密钥直接生成第一密钥。本申请对鉴权服务功能网元生成第一密钥的时间不作限定。

需要说明的是，步骤 804-805 在步骤 807 之前执行。也就是说，步骤 804-805 和 806 之间没有时序关系，既可以步骤 804-805 先执行，步骤 806 后执行，也可以步骤 804-805 后执行，步骤 806 先执行，又可以步骤 804-805 和步骤 806 同时执行，本申请对此不作限定。

步骤 808：鉴权服务功能网元向 AKMA 锚点功能网元发送第一密钥。

步骤 809：AKMA 锚点功能网元使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

可选的，AKMA 锚点功能网元还生成终端设备和第一应用功能网元之间的通信密钥的有效时间。

在一种实现方式中，AKMA 锚点功能网元除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外，还可以使用第一密钥的标识信息中的部分或全部，或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。具体可参考步骤 802 中的描述，此处不作赘述。

步骤 810：AKMA 锚点功能网元向第一应用功能网元发送终端设备和第一应用功能网元之间的通信密钥。

可选的，AKMA 锚点功能网元还向第一应用功能网元发送终端设备和第一应用功能网元之间的通信密钥的有效时间。

步骤 811：第一应用功能网元向终端设备发送第一应用会话建立请求消息的响应消息。

该方法中，发送重鉴权后，鉴权服务功能网元仍向 AKMA 锚点功能网元发送重鉴权前生成的第一密钥，以使 AKMA 锚点功能网元使用第一密钥生成终端设备和应用功能网元之间的通信密钥，保证终端设备生成的终端设备和应用功能网元之间的通信密钥和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

下面结合图 2 所示的网络架构，对图 12 中所提供的密钥管理方法进行详细的说明。如图 13 所示，为本申请提供的另一种密钥管理方法的流程示意图，该流程包括但不限于如下步骤：

步骤 901：UE 和 AUSF 执行主鉴权流程并且 UE 生成 Kakma-1 和 Kakma 对应的 A-KID-1。

主鉴权流程以及 UE 生成 Kakma 和 A-KID 可参考图 3 和图 4 中的描述，此处不作赘述。

UE 生成的 A-KID 具有唯一性，即一个 A-KID 用于标识一个 Kakma，A-KID 和 Kakma 具有一对一的关系，不同 Kakma 对应不同的 A-KID。

步骤 902：UE 向 AF1 发送第一应用会话请求消息，第一应用会话请求消息携带 A-KID-1。

其中，第一应用会话请求消息例如是 application session establishment request。

步骤 903：可选的，UE 使用 Kakma-1 生成 Kaf-1。

如果 UE 生成 Kaf-1 不需要第一应用会话建立请求消息的响应消息携带的参数,则 UE 生成 Kaf-1 的时间可以是 UE 生成 Kakma-1 之后,也可以是在 UE 向 AF1 发送第一应用会话建立请求消息之后。这样,UE 生成 Kaf-1 不会受到重鉴权的影响。

在一种实现方式中,UE 除了使用 Kakma-1 生成 Kaf-1 外,还可以使用 A-KID-1 中的部分或全部,或者 AF1 ID 中的部分或全部生成 Kaf-1。例如,UE 使用 A-KID-1 或者 A-TID-1 推演 Kaf-1,A-KID-1 包括 A-TID-1,即 A-TID-1 为 A-KID-1 的部分。UE 使用 AF1 ID 中的部分或全部生成 Kaf-1,可以实现对于不同 AF 与同一 UE 之间 Kaf 的不同,例如 AF1 与 UE 之间的 Kaf 为 Kaf-1,AF2 与 UE 之间的 Kaf 为 Kaf-2。

步骤 904:发生重鉴权,其中,AUSF 接收重鉴权流程中的第二鉴权请求。

重鉴权流程具体可参考图 2 中步骤 204-209,第二鉴权请求消息例如可以是图 2 中步骤 208 中的第二鉴权请求消息。AUSF 元接收重鉴权流程中来自 AMF 的第二鉴权请求消息。

在一种实现方式中,第二鉴权请求携带第一指示,第一指示用于指示不删除 Kakma-1 和 A-KID-1。

其中,第一指示可以是 UE 发送给 AMF,进而 AMF 发送给 AUSF。UE 向 AUSF 发送第一指示的触发条件可参考图 12 步骤 803 中的描述,此处不作赘述。

步骤 905:AUSF 发送重鉴权流程中的第二鉴权请求消息的响应消息。

其中,第二鉴权请求消息的响应消息例如可以是图 2 步骤 209 中的第二鉴权请求消息的响应消息。

在一种实现方式中,AUSF 发送第二鉴权请求的响应消息后,不删除 Kakma-1 和 A-KID-1。

其中,AUSF 确定不删除 Kakma-1 和 A-KID-1 的具体方式可参考图 12 步骤 804 中的描述,此处不作赘述。

其中,AUSF 不删除 Kakma-1 和 A-KID-1 一段时间,该时间的长度可由运营商决定,本申请对此不作限定。

可选的,如果 UDM 中保有 Kakma-1 或 A-KID-1 相关的信息时,如 AUSF 路由信息,UDM 也继续保有该信息一段时间。

在一种实现方式中,AUSF 发送第二鉴权请求的响应消息后,生成 Kakma-2。可以理解的是,Kakma-1 为重鉴权流程前生成的 AKMA 密钥,Kakma-2 为重鉴权流程后生成的 AKMA 密钥。该种方式中,AUSF 同时保存 Kakma-2 和 A-KID-2,以及 Kakma-1 和 A-KID-1。

步骤 906:收到第一应用会话请求后,AF1 向 AAnF 发送第一请求消息。

其中,第一请求消息用于请求 Kaf-1。第一请求消息携带 A-KID-1 和 AF1 的标识。

对于服务化的接口,第一请求消息为服务化消息,第一请求消息的名称为服务化消息名称,具体可以为 key request。

步骤 907:收到第一请求消息后,如果 AAnF 处未保存 A-KID-1 和 Kakma-1 的对应关系,AAnF 向 AUSF 发送 Kakma-1 请求消息。

对于服务化的接口,Kakma-1 请求消息为服务化消息,Kakma-1 请求消息的名称为服务化消息名称,具体可以为 AKMA key request。Kakma-1 请求消息携带 A-KID-1。

在一种实现方式中,AAnF 可以通过访问 UDM 查找 AUSF 的路由信息,查找 AUSF 的路由信息所需的标识信息为 A-KID-1。

步骤 908:收到第一密钥请求消息后,AUSF 根据 A-KID-1,确定 Kakma-1。

在一种实现方式中,AUSF 同时保存 Kakma-2 和 A-KID-2,以及 Kakma-1 和 A-KID-1,

AUSF 根据第一密钥请求消息中的 A-KID-1，确定 Kakma-1。

需要说明的是，步骤 905-906 在步骤 908 之前执行。关于步骤 905-906 和步骤 907 之间时序关系，可参考图 12 步骤 807 中的描述。

步骤 909：AUSF 向 AAnF 发送 Kakma-1。

具体的，Kakma-1 可以携带在 AKMA Key Response 消息中发送给 AAnF。

步骤 910：AAnF 使用 Kakma-1 生成 Kaf-1。

可选的，AAnF 还生成 Kaf-1 的有效时间。

在一种实现方式中，AAnF 除了使用 Kakma-1 生成 Kaf-1 外，还可以使用 A-KID-1 中的部分或全部，或者 AF1 ID 中的部分或全部生成 Kaf-1。具体可参考步骤 903 中的描述，此处不作赘述。

步骤 911：AAnF 向 AF1 发送 Kaf-1。

可选的，AAnF 还向 AF1 发送 Kaf-1 的有效时间。

具体的，Kaf-1（可选的还包括 Kaf-1 的有效时间）可以携带在 Key response 消息中发送给 AF1。

步骤 912：AF 向 UE 发送第一应用会话建立请求消息的响应消息。

第一应用会话建立请求消息的响应消息例如是 Application session establishment Response。

如图 14 所示，为本申请提供的又一种密钥管理方法的流程示意图，该流程可包括但不限于如下步骤：

步骤 1001：重鉴权流程后，第一应用服务功能网元向 AKMA 锚点功能网元发送第一请求消息。

其中，第一请求消息用于请求终端设备和第一应用功能网元之间的通信密钥。第一请求消息携带第一密钥的标识信息和第一应用功能网元的标识信息。第一密钥为重鉴权流程前生成的 AKMA 密钥。

在一种实现方式中，重鉴权流程后，AKMA 锚点功能网元不删除第一密钥和第一密钥的标识信息。

其中，AKMA 锚点功能网元不删除第一密钥和第一密钥的标识信息可以通过以下方式中的任一项：（1）AKMA 锚点功能网元接收来自终端设备或鉴权服务功能网元的第二指示，第二指示用于指示不删除第一密钥和第一密钥的标识信息。（2）当重鉴权流程成功，AKMA 锚点功能网元确定不删除第一密钥和第一密钥的标识信息，也就是说，AKMA 锚点功能网元确定重鉴权流程成功，从而确定不删除第一密钥和第一密钥的标识信息。

在一种实现方式中，重鉴权流程后，AKMA 锚点功能网元获取第二密钥，第二密钥为重鉴权流程后生成的 AKMA 密钥。该种方式中，AKMA 锚点功能网元同时保存第二密钥和第二密钥的标识信息，以及第一密钥和第一密钥的标识信息。

步骤 1002：AKMA 锚点功能网元根据第一密钥的标识信息，确定第一密钥。

在一种实现方式中，AKMA 锚点功能网元同时保存第二密钥和第二密钥的标识信息，以及第一密钥和第一密钥的标识信息，AKMA 锚点功能网元根据第一请求消息中的第一密钥的标识信息，确定第一密钥。

步骤 1003：AKMA 锚点功能网元使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

可选的，AKMA 锚点功能网元还生成终端设备和第一应用功能网元之间的通信密钥的有效时间。

在一种实现方式中，AKMA 锚点功能网元除了使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥外，还可以使用第一密钥的标识信息中的部分或全部，或者第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥。AKMA 锚点功能网元使用第一应用功能网元的标识信息中的部分或全部生成终端设备和第一应用功能网元之间的通信密钥，可以实现对于不同应用功能网元与同一终端设备之间的通信密钥不同，例如第一应用功能网元与终端设备之间的通信密钥为第一通信密钥，第二应用功能网元与该终端设备之间的通信密钥为不同于第一通信密钥的第二通信密钥。

步骤 1004: AKMA 锚点功能网元向应用功能网元发送终端设备和第一应用功能网元之间的通信密钥。

可选的，AKMA 锚点功能网元还向第一应用功能网元发送终端设备和第一应用功能网元之间的通信密钥的有效时间。

步骤 1005: 第一应用功能网元向终端设备发送第一应用会话建立请求消息的响应消息。

该方法中，发送重鉴权后，AKMA 锚点功能网元仍使用重鉴权前生成的第一密钥生成终端设备和应用功能网元之间的通信密钥，保证终端设备生成的终端设备和应用功能网元之间的通信密钥和应用功能网元获取的终端设备和应用功能网元之间的通信密钥一致，从而保证终端设备和应用功能网元之间成功协商终端设备和应用功能网元之间的通信密钥，实现终端设备和应用功能网元之间的安全通信。

下面将结合图 9 所示的网络架构，对本申请提供的再一种密钥管理方法进行介绍。

如图 15 所示，为本申请提供的再一种密钥管理方法的流程示意图，该流程可包括但不限于如下步骤：

步骤 1101: 终端设备向第一应用功能网元发送第一应用会话建立请求消息。

其中，第一应用会话建立请求消息携带第一密钥的标识信息，第一密钥为 AKMA 密钥。

步骤 1102: 发生重鉴权，其中，终端设备接收重鉴权流程中的第一鉴权请求消息。

重鉴权流程具体可参考图 2 中步骤 204-209，第一鉴权请求消息例如可以是图 2 中步骤 206 中的第一鉴权请求消息。终端设备接收重鉴权流程中来自安全锚点功能网元的第一鉴权请求消息。

步骤 1103: 终端设备发送重鉴权流程中的第一鉴权请求消息的响应消息。

其中，第一鉴权请求消息的响应消息例如可以是图 2 步骤 207 中的第一鉴权请求消息的响应消息。

在一种实现方式中，终端设备在终端设备上设置第一标识，第一标识用于标识终端设备上执行了重鉴权流程；或者第一标识用于标识执行主鉴权流程之前终端设备发送了第一应用会话建立请求消息。

步骤 1104: 第一应用功能网元向终端设备发送第一应用会话建立请求消息的响应消息。

在一种实现方式中，收到第一应用会话建立请求消息的响应消息后，终端设备删除第一应用会话的上下文。

步骤 1105: 接收第一应用会话建立请求消息的响应消息后，终端设备向第一应用功能网元发送第二应用会话建立请求消息。

其中，第二应用会话建立请求消息携带第二密钥的标识信息，第二密钥为重鉴权流程后生成的 AKMA 密钥。

在一种实现方式中，第二应用会话建立请求消息本身指示删除第一应用会话的上下文，

或者第二应用会话建立请求消息携带指示信息，第一应用功能网元根据该指示信息，删除第一应用会话的上下文。

在一种实现方式中，终端设备向第一应用功能网元发送第二应用会话建立请求消息的触发条件可以包括以下任意一项：

- (1) 终端设备根据第一标识向第一应用服务器发送第二应用会话建立请求消息；
- (2) 若第一应用会话建立请求消息的响应消息受到第一应用功能网元和终端设备之间的通信密钥的安全保护，终端设备解密安全保护失败，则终端设备向第一应用服务器发送第二应用会话建立请求消息；
- (3) 若终端设备收到第一应用会话建立请求消息的响应消息后，使用第一应用功能网元和终端设备之间的通信密钥与第一应用功能网元进行安全通信失败，则终端设备向第一应用服务器发送第二应用会话建立请求消息。
- (4) 终端设备无法确定第一密钥的标识信息对应的第一密钥，进而无法使用第一密钥生成终端设备和第一应用功能网元之间的通信密钥。

(5) 终端设备根据第一应用会话建立请求消息的响应消息，确定第一应用会话建立失败。具体可以是第一应用会话建立请求消息的响应消息本身指示第一应用会话建立失败，或者第一应用会话建立请求消息的响应消息携带指示信息，使得终端设备根据指示信息，确定第一应用会话建立失败。指示信息可以包括以下任意一项或多项：第三指示、第一失败原因值、第二失败原因值。其中，第三指示用于指示第一应用会话建立失败，第一失败原因值用于指示无法找到鉴权服务功能网元，第二失败原因值用于指示无法确定第一密钥的标识信息对应的第一密钥，鉴权服务功能网元用于生成第一密钥。

对于因为无法找到鉴权服务功能网元而导致第一应用会话建立失败，步骤 1102 和步骤 1103 之间还可以包括以下步骤：

步骤 11021：收到第一应用会话建立请求消息后，第一应用功能网元向 AKMA 锚点功能网元发送第一请求消息。

其中，第一请求消息用于请求终端设备和第一应用功能网元之间的通信密钥，第一请求消息携带第一密钥的标识信息和第一应用功能网元的标识信息。

步骤 11022：AKMA 锚点功能网元无法确定第一密钥的标识信息对应的鉴权服务功能网元。

在一种实现方式中，AKMA 锚点功能网元向数据管理网元发送鉴权服务功能网元路径信息请求消息，鉴权服务功能网元路径信息请求消息携带第一密钥的标识信息。AKMA 锚点功能网元接收来自数据管理网元的鉴权服务功能网元路径信息请求消息的响应消息，鉴权服务功能网元路径信息请求消息的响应消息指示鉴权服务功能网元路径信息请求失败。

步骤 11023：AKMA 锚点功能网元向第一应用功能网元发送第一请求消息的响应消息，第一请求消息的响应消息指示终端设备和第一应用功能网元之间的通信密钥请求失败。

可选的，AKMA 锚点功能网元向第一应用功能网元发送第一失败原因值。

对于因为无法确定第一密钥的标识信息对应的第一密钥而导致第一应用会话建立失败，步骤 1102 和步骤 1103 之间还可以包括以下步骤：

步骤 11024：鉴权服务功能网元接收重鉴权流程中的第二鉴权请求。

步骤 11025：鉴权服务功能网元发送重鉴权流程中的第二鉴权请求的响应消息。

步骤 11026：收到第一请求消息后，AKMA 锚点功能网元向鉴权服务功能网元发送第一密钥请求消息。

其中，第一密钥请求消息携带第一密钥的标识信息。

步骤 11027：收到第一密钥请求消息后，鉴权服务功能网元无法确定第一密钥的标识信息对应的第一密钥；

步骤 11028：鉴权服务功能网元向 AKMA 锚点功能网元发送第一密钥请求消息的响应消息，第一密钥请求消息的响应消息用于指示第一密钥请求失败。

可选的，鉴权服务功能网元向 AKMA 锚点功能网元发送第二失败原因值，第二失败原因值指示无法确定第一密钥的标识信息对应的第一密钥。

或者，对于因为无法确定第一密钥的标识信息对应的第一密钥而导致第一应用会话建立失败，步骤 1102 和步骤 1103 之间还可以包括以下步骤：

步骤 11029：收到第一应用会话建立请求消息后，第一应用功能网元向 AKMA 锚点功能网元发送第一请求消息。

其中，第一请求消息用于请求终端设备和第一应用功能网元之间的通信密钥，第一请求消息携带第一密钥的标识信息和第一应用功能网元的标识信息。

步骤 110210：AKMA 锚点功能网元无法确定第一密钥的标识信息对应的第一密钥。

步骤 110211：AKMA 锚点功能网元向第一应用功能网元发送第一请求消息的响应消息，第一请求消息的响应消息指示终端设备和第一应用功能网元之间的通信密钥请求失败。

可选的，AKMA 锚点功能网元向应用功能网元发送第二失败原因值，第二失败原因值指示无法确定第一密钥的标识信息对应的第一密钥。

下面结合图 2 所示的网络架构，对图 15 中所提供的密钥管理方法进行详细的说明。如图 16 所示，为本申请提供的再一种密钥管理方法的流程图，该流程中，终端设备触发条件 (1) (2) (3) 向第一应用服务器发送第二应用会话建立请求消息。该流程包括但不限于如下步骤：

步骤 1201-1209 同图 11 中的步骤 701-709，不作赘述。

步骤 1210：UE 发送重鉴权流程中的第一鉴权请求消息的响应消息。

可选的，UE 上在 UE 上设置 flag。其中，该 flag 可以标识 UE 进行了重鉴权，也可以标识 UE 在重鉴权之前发送了第一应用会话建立请求。

步骤 1211：收到 Kaf（可选的，还收到 Kaf 的有效时间）后，AF1 向 UE 发送第一应用会话建立请求消息的响应消息。

第一应用会话建立请求消息的响应消息例如是 Application session establishment Response。

步骤 1212：收到第一应用会话建立请求消息的响应消息后，UE 释放第一应用会话，向 AF1 发送第二应用会话建立请求消息。第二应用会话建立请求消息携带重鉴权后生成的 A-KID-2。

其中，UE 向 AF1 发送第二应用会话建立请求消息的触发条件可以包括以下任意一项或多项：

(1) UE 上存储有 flag；

(2) 如果第一应用会话建立请求消息的响应消息受到 Kaf-1 的安全保护，UE 解安全保护失败；

(3) UE 收到第一应用会话建立请求消息的响应消息后，使用 Kakma-2 推演 Kaf-2，UE 使用 Kaf-2 与 AF-1 进行认证或者安全通信失败。

可选的，第二应用会话建立请求消息携带指示信息，该指示信息指示第一应用会话建立失

败或者指示 UE 发起应用会话重建，或者第二应用会话建立请求消息用于 UE 和 AF1 之间重新建立应用会话。

在一种实现方式中，UE 删除与 AF-1 建立失败的第一应用会话上下文。

步骤 1213：收到第二应用会话建立请求消息后，AF-1 删除与 UE 建立失败的第一应用会话上下文，如删除 Kaf-1 等信息。

收到第二应用会话建立请求消息后，AF-1 和 UE 基于 Kakma-2 和/或 A-KID-2 进行 Kaf-2 的协商，与现有技术相同，不作赘述。

下面结合图 2 所示的网络架构，对图 15 中所提供的密钥管理方法进行详细的说明。如图 17 所示，为本申请提供的再一种密钥管理方法的流程图，该流程中，终端设备触发条件（4）向第一应用服务器发送第二应用会话建立请求消息。该流程包括但不限于如下步骤：

步骤 1301-1306 同图 13 中的步骤 901-906，不作赘述。

步骤 1307：如果 AAnF 在重鉴权前保有 Kakma-1 和 A-KID-1，因重鉴权后 AAnF 中的 Kakma-1 和 A-KID-1 被删除，AAnF 根据 A-KID-1 无法找到 Kakma-1，AF 侧的 Kaf-1 无法生成。AAnF 生成失败指示 1 并执行步骤 1309a-1311a 和 1312，失败指示 1 指示 Kaf 请求失败。可选的，AAnF 还生成失败原因值 2，失败原因即无法找到 A-KID-1 对应的 Kakma-1，该原因值记为 Cause 2。

如果 AAnF 在接收 AF1 第一请求消息时未保有 Kakma-1 和 A-KID-1，则 AAnF 向 AUSF 请求 Kakma-1，并执行步骤 1308、1309a-1311a 和 1312。对于服务化的接口，第一请求消息为服务化消息，第一请求消息的名称为服务化消息名称，具体可以为 AKMA key request。第一请求消息携带 A-KID-1。

在一种实现方式中，AAnF 通过访问 UDM 查找 AUSF 的路由信息，查找 AUSF 的路由信息所需的标识信息为 A-KID-1。因重鉴权后 UDM 中关于 A-KID-1 的相关信息被删除，UDM 根据 A-KID-1 无法找到 AUSF 路由信息，向 AAnF 返回失败指示 2，失败指示 2 指示 AUSF 的路由信息查找失败，可选的，还返回失败原因值 1，失败原因即无法找到 AUSF 的路由信息，该原因值记为 cause 1。AAnF 接收失败指示 2 或失败原因值 1 中的一个或多个后，执行步骤 1309b-1311b 和 1312。

步骤 1308：AUSF 无法根据 A-KID-1 找到对应的 Kakma-1，AUSF 向 AAnF 返回失败指示 3，失败指示 3 指示 Kakma 请求失败，可选的，还返回失败原因值 2，失败原因即无法找到 A-KID-1 对应的 Kakma-1，该原因值记为 cause 2。

步骤 1309a：AAnF 将失败指示 1 或 cause 2 中的一个或多个发给 AF1，失败指示 1 指示 Kaf 请求失败。

具体的，失败指示 1 或 cause 2 中的一个或多个可以携带在 Key response 消息中发送给 AF1。

步骤 1310a：收到失败指示 1 或 cause 2 中的一个或多个后，AF1 向 UE 发送第一应用会话建立请求消息的响应消息，可选的，第一应用会话建立请求消息的响应消息包括失败指示 4 或 cause 2 中的一个或多个，失败指示 4 指示第一应用会话建立失败。

第一应用会话建立请求消息的响应消息例如是 Application session establishment Response。

步骤 1311a：UE 收到失败指示 4 或 cause 2 中的一个或多个后，释放第一应用会话连接，重新发起应用会话建立过程。

步骤 1309b：AAnF 将失败指示 1 或 cause1 中的一个或多个发给 AF，失败指示 1 指示

K_{AF} 请求失败。

具体的，失败指示 1 或 cause 1 中的一个或多个可以携带在 Key response 消息中发送给 AAnF。

步骤 1310b: AF 收到失败指示 1 或 cause 1 中的一个或多个后，向 UE 发送第一应用会话建立请求消息的响应消息，第一应用会话建立请求消息的响应消息包括失败指示 4 或 cause 1 中的一个或多个，失败指示 4 指示第一应用会话建立失败。

步骤 1311b: UE 收到失败指示 4 或 cause 1 中的一个或多个后，释放第一应用会话连接，重新发起应用会话建立过程。

步骤 1312: UE 使用重鉴权后的 A-KID-2 请求建立应用会话，与现有技术相同，不作赘述。

本申请还提供的一种密钥管理方法的流程示意图，图 18 为该方法的流程图，该流程包括但不限于如下步骤：

步骤 1401-1410 同图 6 中的步骤 401-410，不作赘述。

步骤 1412，重鉴权成功后，UE 不删除第一密钥和第一密钥的标识信息。UE 使用重鉴权后的第二 K_{AUSF} 推演第二 K_{AKMA}。可以理解的是，UE 保存有两套 K_{AKMA} 和对应的密钥标识信息；

步骤 1413，AF 向 UE 发送应用会话建立响应消息，消息中可能携带用于生成 K_{AF} 的推演参数、用于完整性保护的 MAC（message authentication code）1 等，其中，推演参数可以是随机数、计数器值等，MAC1 的输入密钥可以是 K_{AF}，输入参数可以是整条应用会话建立响应消息或者应用会话建立响应消息中的部分信元。

步骤 1414，UE 接收 AF 发送的应用会话建立响应消息，并推演 K_{AF}。

UE 根据推演参数和 K_{AKMA} 推演 K_{AF}。可以理解的是，UE 根据推演参数和第一 K_{AKMA} 推演得到第一 K_{AF}，UE 根据推演参数和第二 K_{AKMA} 推演得到第二 K_{AF}。应用会话建立响应消息携带的推演参数可以是推演 K_{AF} 的推演参数的部分或者全部。

步骤 1415，UE 判断 AF 使用的密钥 K_{AF}。

当应用会话建立响应消息中携带用于完整性保护的 MAC1 时，UE 分别使用第一 K_{AF} 和第二 K_{AF} 计算 MAC2 和 MAC3，输入参数和安全算法与 MAC1 的计算时使用的输入参数和安全算法相同。

此时，UE 将 MAC1 分别与 MAC2 和 MAC3 进行比较，当 MAC1 与 MAC2 相同时，表示 AF 使用的密钥为第一 K_{AF}，并且应用会话建立响应消息未被篡改，则 UE 和 AF 进行后续会话时选择第一 K_{AF}，可选删除第二 K_{AF} 和对应的密钥标识信息；当 MAC1 与 MAC3 相同时，表示 AF 使用的密钥为第二 K_{AF}，并且应用会话建立响应消息未被篡改，则 UE 和 AF 进行后续会话时选择第二 K_{AF}，可选删除第一 K_{AF} 和对应的密钥标识信息。当 MAC1 与 MAC2 和 MAC3 均不相同时，表示应用会话建立响应消息可能被篡改，则 UE 丢弃应用会话建立响应消息。UE 根据本地配置，UE 重新发起应用会话建立过程，即 UE 重新发送应用会话建立请求消息，消息中携带第二和 AF 进行后续会话时选择第二 K_{AKMA} 的密钥标识信息，可选删除第一和第二 K_{AF} 和对应的密钥标识信息。本地配置可以是在 UE 一次或者多次收到错误的会话建立响应消息。

当应用会话建立响应消息中未携带用于完整性保护的 MAC1 时，UE 分别尝试使用第一 K_{AF} 和第二 K_{AF} 与 AF 进行后续应用会话业务，根据后续应用会话业务成功或失败判断 UE 选择使用哪一个 K_{AF}。可以理解的是 K_{AF} 可以是 UE 和 AF 进行鉴权的凭证，或者进行通信的对

称密钥。后续应用会话业务成功可以是 UE 使用 K_{AF} 与 AF 进行成功鉴权，或者 UE 与 AF 使用 K_{AF} 或其衍生密钥进行通信时安全保护成功。反之，后续应用会话业务失败可以是 UE 使用 K_{AF} 与 AF 进行鉴权失败，或者 UE 与 AF 使用 K_{AF} 或其衍生密钥进行通信时安全保护失败。当 UE 使用第一 K_{AF} ，与 AF 进行后续应用会话成功时，表示 AF 使用的密钥为第一 K_{AF} ，则 UE 和 AF 进行后续会话时选择第一 K_{AF} ，可选删除第二 K_{AF} 和对应的密钥标识信息；当 UE 使用第一 K_{AF} ，与 AF 进行后续应用会话失败时，UE 使用第二 K_{AF} ，与 AF 进行后续应用会话，如果成功时，表示 AF 使用的密钥为第二 K_{AF} ，则 UE 和 AF 进行后续会话时选择第二 K_{AF} ，可选删除第二 K_{AF} 和对应的密钥标识信息；当 UE 分别使用第一和第二 K_{AF} ，与 AF 进行后续应用会话均失败时，UE 根据本地配置，UE 重新发起应用会话建立过程，即 UE 重新发送应用会话建立请求消息，消息中携带第二和 AF 进行后续会话时选择第二 K_{AKMA} 的密钥标识信息，可选删除第一和第二 K_{AF} 和对应的密钥标识信息。本地配置可以在 UE 和 AF 由于两侧 K_{AF} 不一致发生一次或者多次应用会话失败。

相应于上述方法实施例给出的方法，本申请实施例还提供了密钥管理设备，包括用于执行上述实施例相应的模块。模块可以是软件，也可以是硬件，或者是软件和硬件结合。

参见图 19，为本申请提供的一种通信装置的结构示意图。图 19 所示的通信装置 1500 包括收发模块 1501 和处理模块 1502，可选的，还包括存储模块 1503。

在一种设计中，装置 1500 为终端设备：

示例性的，收发模块 1501 用于向第一应用功能网元发送第一应用会话建立请求消息，该第一应用会话建立请求消息携带第一密钥的标识信息，该第一密钥为应用的认证和密钥管理 AKMA 密钥；接收重鉴权流程中的第一鉴权请求消息；发送该重鉴权流程中的该第一鉴权请求消息的响应消息；以及接收来自该第一应用功能网元的该第一应用会话建立请求消息的响应消息；处理模块 1502 用于使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。

可选的，收发模块 1501 用于发送该第一鉴权请求消息的响应消息后，处理模块 1502 用于不删除该第一密钥和该第一密钥的标识信息

该示例中，装置 1500 用于实现图 10-18 所示实施例中终端设备或 UE 的功能，处理模块 1502 被配置为支持终端设备执行图 10-18 所示实施例中的方法，收发模块 1501 用于支持终端设备与其他设备之间的通信，具体可参见图 10-18 中终端设备或 UE 的相应描述。

在一种设计中，装置 1500 为鉴权服务功能网元：

示例性的，收发模块 1501 用于接收重鉴权流程中的第二鉴权请求；发送该重鉴权流程中的该第二鉴权请求的响应消息；接收来自应用的认证和密钥管理 AKMA 锚点功能网元的第一密钥请求消息，该第一密钥请求消息携带第一密钥的标识信息，该第一密钥为该重鉴权流程前生成的 AKMA 密钥；以及向该 AKMA 锚点功能网元发送该第一密钥。

可选的，收发模块 1501 用于发送该第二鉴权请求的响应消息后，处理模块 1502 用于不删除该第一密钥和该第一密钥的标识信息。

装置 1500 用于实现图 10-18 所示实施例中鉴权服务功能网元或 AUSF 的功能，处理模块 1502 被配置为支持鉴权服务功能网元执行图 10-18 所示实施例中的方法，收发模块 1501 用于支持鉴权服务功能网元与其他设备之间的通信，具体可参见图 10-18 中鉴权服务功能网元或 AUSF 的相应描述。

在一种设计中，装置 1500 为应用的认证和密钥管理 AKMA 锚点功能网元：

示例性的，收发模块 1501 重鉴权流程后，用于接收来自第一应用功能网元的第一请求消

息，该第一请求消息用于请求终端设备和该第一应用功能网元之间的通信密钥，该第一请求消息携带第一密钥的标识信息，该第一密钥为该重鉴权流程前生成的 AKMA 密钥；处理模块 1502 用于使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥；收发模块 1501 还用于向该应用功能网元发送该通信密钥。

可选的，该重鉴权流程后，处理模块 1502 用于不删除该第一密钥和该第一密钥的标识信息。

装置 1500 用于实现图 10-18 所示实施例中 AKMA 锚点功能网元或 AAnF 的功能，处理模块 1502 被配置为支持 AKMA 锚点功能网元执行图 10-18 所示实施例中的方法，收发模块 1501 用于支持 AKMA 锚点功能网元与其他设备之间的通信，具体可参见图 10-18 中 AKMA 锚点功能网元或 AAnF 的相应描述。

请参见图 20，为本申请提供的另一种通信装置的结构示意图。图 20 所示的通信装置 1600 包括至少一个处理器 1601、收发器 1602，可选的，还包括存储器 1603 或总线 1604。处理器 1601、收发器 1602 以及存储器 1603 通过总线 1604 连接。其中，处理器 1601 例如可以是中央处理器(central processing unit, CPU)，通用处理器，数字信号处理器(digital signal processor, DSP)，专用集成电路(application-specific integrated circuit, ASIC)，现场可编程门阵列(field programmable gate array, FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或其任意组合。其可以实现或执行结合本申请所描述的各个示例性的逻辑方框、模块和电路。处理器也可以是实现计算功能的组合，例如包括一个或多个微处理器组合，DSP 和微处理器的组合等等。总线 1604 可以是外设部件互连标准(peripheral component interconnect, 简称 PCI)总线或扩展工业标准结构(extended industry standard architecture, 简称 EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 20 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本申请实施例还提供的一种芯片系统 1700，包括至少一个处理器 1701、接口电路 1702，处理器 1701 和接口电路 1702 相连。

处理器 1701 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1701 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1701 可以是通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(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。可以实现或者执行本申请实施例中的公开的各方法、步骤。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。

接口电路 1702 可以完成数据、指令或者信息的发送或者接收，处理器 1701 可以利用接口电路 1702 接收的数据、指令或者其他信息，进行加工，可以将加工完成信息通过接口电路 1702 发送出去。

可选的，芯片系统还包括存储器 1703，存储器 1703 可以包括只读存储器和随机存取存储器，并向处理器提供操作指令和数据。存储器 1703 的一部分还可以包括非易失性随机存取存储器(NVRAM)。

可选的，存储器 1703 存储了可执行软件模块或者数据结构，处理器 1703 可以通过调用存储器存储的操作指令(该操作指令可存储在操作系统中)，执行相应的操作。

可选的，芯片系统可以使用在本申请实施例涉及的终端设备、鉴权服务功能网元或者 AKMA 锚点功能网元中。可选的，接口电路 1702 用于执行图 10 至图 18 所示的实施例中终端设备、鉴权服务功能网元或者 AKMA 锚点功能网元的接收和发送的步骤。处理器 1701 用

于执行图 10 至图 18 所示的实施例中的终端设备、鉴权服务功能网元或者 AKMA 锚点功能网元处理的步骤。存储器 1703 用于存储图 10 至图 18 所示的实施例中的终端设备、鉴权服务功能网元或者 AKMA 锚点功能网元的数据和指令。

本申请实施例还提供了一种计算机可读存储介质。上述方法实施例中描述的方法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。如果在软件中实现，则功能可以作为一个或多个指令或代码存储在计算机可读介质上或者在计算机可读介质上传输。计算机可读介质可以包括计算机存储介质和通信介质，还可以包括任何可以将计算机程序从一个地方传送到另一个地方的介质。存储介质可以是可由计算机访问的任何可用介质。

作为一种可选的设计，计算机可读介质可以包括 RAM，ROM，EEPROM，CD-ROM 或其它光盘存储器，磁盘存储器或其它磁存储设备，或可用于承载的任何其它介质或以指令或数据结构的形式存储所需的程序代码，并且可由计算机访问。而且，任何连接被适当地称为计算机可读介质。例如，如果使用同轴电缆，光纤电缆，双绞线，数字用户线（DSL）或无线技术（如红外，无线电和微波）从网站，服务器或其它远程源传输软件，则同轴电缆，光纤电缆，双绞线，DSL 或诸如红外，无线电和微波之类的无线技术包括在介质的定义中。如本文所使用的磁盘和光盘包括光盘（CD），激光盘，光盘，数字通用光盘（DVD），软盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘利用激光光学地再现数据。上述的组合也应包括在计算机可读介质的范围内。

本申请实施例还提供了一种计算机程序产品。上述方法实施例中描述的方法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。如果在软件中实现，可以全部或者部分得通过计算机程序产品的形式实现。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上述计算机程序指令时，全部或部分地产生按照上述方法实施例中描述的流程或功能。上述计算机可以是通用计算机、专用计算机、计算机网络、网络设备、用户设备或者其它可编程装置。

可以理解，说明书通篇中提到的“实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各个实施例未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。可以理解，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。

可以理解，在本申请中，“当...时”、“若”以及“如果”均指在某种客观情况下装置会做出相应的处理，并非限定时间，且也不要求装置实现时一定要有所判断的动作，也不意味着存在其它限定。

本申请中的“同时”可以理解为在相同的时间点，也可以理解为在一段时间段内，还可以理解为在同一个周期内。

本申请中对于使用单数表示的元素旨在用于表示“一个或多个”，而并非表示“一个且仅一个”，除非有特别说明。本申请中，在没有特别说明的情况下，“至少一个”旨在用于表示“一个或者多个”，“多个”旨在用于表示“两个或两个以上”。

另外，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A 可以是单数或者复数，B 可以是单数或者复数。

可以理解,在本申请各实施例中,“与 A 相应的 B”表示 B 与 A 相关联,根据 A 可以确定 B。但还应理解,根据 A 确定 B 并不意味着仅仅根据 A 确定 B,还可以根据 A 和/或其它信息确定 B。

本申请中各表所示的对应关系可以被配置,也可以是预定义的。各表中的信息的取值仅是举例,可以配置为其他值,本申请并不限定。在配置信息与各参数的对应关系时,并不一定要求必须配置各表中示意出的所有对应关系。例如,本申请中的表格中,某些行示出的对应关系也可以不配置。又例如,可以基于上述表格做适当的变形调整,例如,拆分,合并等等。上述各表中标题示出参数的名称也可以采用通信装置可理解的其他名称,其参数的取值或表示方式也可以通信装置可理解的其他取值或表示方式。上述各表在实现时,也可以采用其他的数据结构,例如可以采用数组、队列、容器、栈、线性表、指针、链表、树、图、结构体、类、堆、散列表或哈希表等。

本申请中的预定义可以理解为定义、预先定义、存储、预存储、预协商、预配置、固化、或预烧制。

本领域普通技术人员可以理解,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。

本领域普通技术人员可以理解,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。

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

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。