

一种终端参数更新的保护方法和通信装置

技术领域

本申请涉及终端参数安全技术领域，尤其涉及一种终端参数更新的保护方法和通信装置。

背景技术

在新无线（new radio, NR）网络系统中，存在可执行不同网络功能的多个网络实体。例如 NR 系统包括拜访公共陆地移动网（visited public land mobile network, VPLMN）和归属公共陆地移动网（home public land mobile network, HPLMN）。在通信过程中，HPLMN 中的实体需要向终端发送一些配置参数，在发送这些配置参数的过程中，HPLMN 中的实体需要通过 VPLMN 中的实体，将配置参数发送给终端。例如，HPLMN 中的统一数据管理（unified data management, UDM）实体需要将更新的签约数据通过 VPLMN 的接入和移动性管理功能（access and mobility management function, AMF）实体发送给终端；再例如 HPLMN 的策略控制功能（policy control function, PCF）实体需要将策略信息，依次通过 VPLMN 的 PCF 实体、VPLMN 的 AMF 实体发送给终端。

可见，HPLMN 中的实体发送给终端的参数，只能通过 VPLMN 中的实体进行转发。然而，在转发过程中，参数可能会被 VPLMN 中的实体窃听或篡改，安全性较低。为此，UDM 会请求 HPLMN 中的认证服务功能（authentication server function, AUSF）实体保护 HPLMN 与终端之间的配置参数或者更新的签约参数等，即请求 AUSF 实体对参数加密，然后经 AMF 实体发送给终端。

AUSF 可使用终端认证过程中生成的密钥对上述参数进行保护，终端使用在认证过程中生成的密钥对 AUSF 发送的上述参数进行校验。但是在双注册场景中，即终端通过两个服务网络注册，这种情况下，一个 AUSF 存在多个密钥，如果 AUSF 随机选择密钥对参数进行加密，AUSF 所选择的密钥与终端认证过程中生成的密钥不一致，最终导致终端对参数校验失败。

发明内容

本申请提供一种终端参数更新的保护方法和通信装置，能够保证 HPLMN 发送给终端的参数在传输过程中的安全性。

第一方面，本申请实施例提供了一种终端参数更新的保护方法，该方法可由第一通信装置执行，第一通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片系统。下面以所述通信设备为 UDM 实体为例进行描述。该方法包括：

UDM 向第一 AUSF 发送保护请求消息，之后，UDM 接收第一 AUSF 发送的该保护请

求消息的响应消息,并通过第一服务网络对应的 AMF 发送终端的参数更新信息;其中,该保护请求消息用于请求保护终端的参数更新信息,该保护请求消息携带终端的参数更新信息和第一服务网络信息。

在本申请实施例中,UDM 向第一 AUSF 发送的用于保护终端的参数更新信息的保护请求消息中携带了用于标识第一服务网络的信息(即第一服务网络信息),从而第一 AUSF 可根据该第一服务网络信息选择与第一服务网络对应的第一密钥(也可以认为是认证服务功能密钥,下文中简称密钥)对终端的参数更新信息进行加密保护。这样即使在终端通过多个服务网络注册到归属网络(home network, HN),即在一个 AUSF 对应多个密钥的情况下,通过该方案,也可明确第一 AUSF 采用哪个密钥,保证终端成功校验 HPLMN 通过 AMF 发送的终端的参数更新信息。

在一种可能的实现方式中,所述 UDM 在向第一 AUSF 发送保护请求消息之前,该 UDM 根据本地策略确定第一服务网络信息。该方案中,UDM 可向第一 AUSF 指定后续进行终端参数更新过程的第一服务网络,即指定第一 AUSF 后续要使用的密钥,从而保证终端处于双注册状态(即终端通过至少两个服务网络进行注册)的情况下,即使这至少两个服务网络中的 AMF 选择同一个 AUSF,也能够保证第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。

在另一种可能的实现方式中,所述 UDM 在确定存在多个服务网络的情况下,确定进行终端参数更新过程的第一服务网络。该方案中,UDM 在确定存在多个服务网络的情况下,才确定第一服务网络,以避免终端通过一个服务网络注册的情况下,也判断后续进行 SoR 流程的所述第一服务网络,即避免执行不必要的步骤。

在一种可能的实现方式中,所述方法还包括:UDM 根据第一服务网络信息确定第一 AUSF。该方案中,在终端先后通过不同的多个服务网络注册到 HN,且不同的服务网络选择不同的 AUSF 的情况下,UDM 指定第一 AUSF 保护 SoR 信息,由于一个 AUSF 对应一个密钥,因此可保证第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。

在一种可能的实现方式中,UDM 在向第一 AUSF 发送保护请求消息之前,UDM 还可以确定第一 AUSF 有终端在多个服务网络的认证结果,这多个服务网络包括第一服务网络;或者,UDM 还可以确定终端在多个服务网络,这多个服务网络包括第一服务网络;或者,UDM 还可以确定终端处于双注册状态,即终端通过两个服务网络注册到 HN。该方案可包括 UDM 在确定存在多个密钥(例如一个 AUSF 对应多个密钥或者存在多个 AUSF(每个 AUSF 对应有密钥))的情况下,通过第一服务网络的第一服务网络信息指定某个密钥,使得第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。可避免发送的保护请求消息携带不必要的第一服务网络信息。

在一种可能的实现方式中,例如该第一服务网络信息包括第一服务网络的名称;又例如,该第一服务网络信息包括第一服务网络的公共陆地移动网络(public land mobile network, PLMN)的标识 ID 或第一服务网络的 ID;又例如,该第一服务网络信息包括终端的认证事件的标识。如上只是列举了第一服务网络信息的 4 种实现方式,应理解,本申请实施例不限制该第一服务网络信息的具体实现方式,只要可以标识第一服务网络即可。

在一种可能的实现方式中,终端的参数更新信息包括漫游处理(steering of roaming,

SoR) 信息。

第二方面，本申请实施例提供了一种终端参数更新的保护方法，该方法可由第二通信装置执行，第二通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片系统。下面以所述通信设备为 AUSF 实体为例进行描述。该方法包括：

第一 AUSF 接收 UDM 发送的保护请求消息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带参数更新信息和第一服务网络信息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带所述参数更新信息和第一服务网络信息；之后，第一 AUSF 根据上述第一服务网络信息确定第一密钥，该第一密钥用于保护终端的参数更新信息，并根据第一密钥对终端的参数更新信息进行安全保护。

在一种可能的实现方式中，该第一服务网络信息为 UDM 存储的多个第一服务网络信息中的一个服务网络信息。

在一种可能的实现方式中，存在多个 AUSF，第一 AUSF 为与所述第一服务网络信息对应的 AUSF。

在一种可能的实现方式中，第一 AUSF 有终端在多个服务网络的认证结果，这多个服务网络包括第一服务网络；或者，终端在多个服务网络，这多个服务网络包括第一服务网络；或者，终端处于双注册状态。

在一种可能的实现方式中，该第一服务网络信息包括第一服务网络的名称；或者，

该第一服务网络信息包括所述第一服务网络的 PLMN ID；或者，该述第一服务网络信息包括终端的认证事件的标识。

在一种可能的实现方式中，终端的参数更新信息包括漫游处理 (steering of roaming, SoR) 信息。

关于第二方面或第二方面的各种可能的实施方式所带来的技术效果，可以参考对第一方面或第一方面的各种可能的实施方式的技术效果的介绍。

第三方面，本申请实施例提供了一种终端参数更新的保护方法，该方法可由第三通信装置执行，第三通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片系统。下面以所述通信设备为 UDM 实体为例进行描述。该方法包括：

UDM 向第一 AUSF 发送第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；之后，UDM 在确定终端处于单注册状态的情况下，确定通过第二 AMF 发送终端的参数更新信息。

在本申请实施例中，UDM 可以指示 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥。这样即使终端在第二 AMF 所在的第二服务网络注册，也能够保证 AUSF 上的密钥是唯一的，也就是与终端认证过程中的密钥一致。

在一种可能的实现方式中，UDM 在向第一 AMF 发送第二消息或在接收到第一 AMF 发送的第三消息的情况下，UDM 向第一 AUSF 发送所述第一消息，其中，第二消息用于删除终端的注册信息，第三消息为第二消息的响应消息。该方案中，UDM 在终端通过第二 AMF 所在的第二服务网络进行注册时，UDM 可向第一 AUSF 发送第一消息，即保证终端处于单注册的状态，从而保证第一 AUSF 上的密钥是唯一的。

在一种可能的实现方式中，所述第一消息携带所述第一服务网络的标识信息或所述终端的身份标识信息。

第四方面，本申请实施例提供了一种终端参数更新的保护方法，该方法可由第四通信装置执行，第四通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片系统。下面以所述通信设备为 AUSF 实体为例进行描述。该方法包括：

第一 AUSF 接收 UDM 发送的第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；之后，第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时使用的的第一密钥。

在一种可能的实现方式中，所述第一消息携带所述第一服务网络的标识信息或所述终端的身份标识信息。

关于第四方面或第四方面的各种可能的实施方式所带来的技术效果，可以参考对第三方面或第三方面的各种可能的实施方式的技术效果的介绍。

第五方面，提供了一种通信装置，例如该通信装置为如前所述的 UDM。该通信装置具有实现上述第一方面方法实施例中的行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，所述通信装置例如包括相互耦合的处理模块和收发模块，其中，该收发模块用于向第一 AUSF 发送保护请求消息，以及接收第一 AUSF 发送的保护请求消息的响应消息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带所述参数更新信息和第一服务网络信息；该处理模块用于控制收发模块通过第一服务网络对应的 AMF 发送所述参数更新信息。

在一种可能的实现方式中，该收发模块还用于：在向所述第一 AUSF 发送所述保护请求消息之前，根据本地策略确定所述第一服务网络信息。

在一种可能的实现方式中，该处理模块具体用于：在确定存在多个服务网络的情况下，确定进行终端的参数更新的所述第一服务网络。

在一种可能的实现方式中，该处理模块具体用于：根据所述第一服务网络信息确定所述第一 AUSF。

在一种可能的实现方式中，该处理模块具体用于在向所述第一 AUSF 发送保护请求消息之前，确定：

所述第一 AUSF 有所述终端在多个服务网络的认证结果，所述多个服务网络包括所述第一服务网络；或者，

所述终端在多个服务网络，所述多个服务网络包括所述第一服务网络；或者，

所述终端处于双注册状态。

在一种可能的实现方式中，所述第一服务网络信息包括所述第一服务网络的名称；或者，

所述第一服务网络信息包括所述第一服务网络的 PLMN 的标识 ID 或所述第一服务网络的 ID；或者，

所述第一服务网络信息包括所述终端的认证事件的标识。

在一种可能的实现方式中，所述参数更新信息包括 SoR 信息。

第六方面，提供了一种通信装置，例如该通信装置为如前所述的 AUSF。该通信装置具有实现上述第二方面方法实施例中的行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，所述通信装置例如包括相互耦合的处理模块和收发模块，其中，该收发模块用于接收 UDM 发送的保护请求消息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带所述参数更新信息和第一服务网络信息；所述处理模块用于根据第一服务网络信息确定第一密钥，以及根据第一密钥对所述参数更新信息进行安全保护，其中，第一密钥用于保护所述参数更新信息；

在一种可能的实现方式中，第一服务网络信息为 UDM 存储的多个第一服务网络信息中的一个服务网络信息。

在一种可能的实现方式中，存在多个 AUSF，所述第一 AUSF 为与所述第一服务网络信息对应的 AUSF。

在一种可能的实现方式中，第一 AUSF 有终端在多个服务网络的认证结果，这多个服务网络包括第一服务网络；或者，

终端在多个服务网络，多个服务网络包括第一服务网络；或者，

终端处于双注册状态。

在一种可能的实现方式中，第一服务网络信息包括第一服务网络的名称；或者，

第一服务网络信息包括第一服务网络的 PLMN 标识；或者，

第一服务网络信息包括终端的认证事件的标识。

在一种可能的实现方式中，所述参数更新信息包括漫游处理 SoR 信息。

第七方面，提供了一种通信装置，例如该通信装置为如前所述的 UDM。该通信装置具有实现上述第三方面方法实施例中的行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，所述通信装置例如包括相互耦合的处理模块和收发模块，其中，该收发模块用于向第一 AUSF 发送第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；所述处理模块用于在确定终端处于单注册状态的情况下，确定通过第二 AMF 发送终端的参数更新信息。

在一种可能的实现方式中，所述收发模块具体用于在向第一 AMF 发送第二消息或在接收到第一 AMF 发送的第三消息的情况下，向第一 AUSF 发送所述第一消息，其中，第二消息用于删除终端的注册信息，第三消息为第二消息的响应消息。

在一种可能的实现方式中，第一消息携带第一服务网络的标识信息或终端的身份标识信息。

第八方面，提供了一种通信装置，例如该通信装置为如前所述的 AUSF。该通信装置具有实现上述第四方面方法实施例中的行为的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，所述通信装置例如包括相互耦合的处理模块和收发模块，其中，该

收发模块用于接收 UDM 发送的第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；所述处理模块用于删除终端在第一 AMF 所在的第一服务网络注册时使用的的第一密钥。

在一种可能的实现方式中，第一消息携带第一服务网络的标识信息或终端的身份标识信息。

第九方面，提供了一种通信装置。该通信装置可以为上述方法实施例中的 UDM 或者设置在 UDM 中的芯片；该通信装置也可以为上述方法实施例中的 AUSF 或者设置在 AUSF 或中的芯片。该通信装置包括通信接口以及处理器，可选的，还包括存储器。其中，该存储器用于存储计算机程序或指令，处理器与存储器、通信接口耦合，当处理器执行所述计算机程序或指令时，使通信装置执行上述方法实施例中对功能实体所执行的方法。例如当处理器执行所述计算机程序或指令时，使通信装置执行上述方法实施例中 UDM 所执行的方法；又例如当处理器执行所述计算机程序或指令时，使通信装置执行上述方法实施例中 AUSF 或所执行的方法。

其中，第九方面的通信装置中的通信接口可以是通信装置中的收发器，例如通过所述通信装置中的天线、馈线和编解码器等实现，或者，如果通信装置为设置在通信装置中的芯片，则通信接口可以是该芯片的输入/输出接口，例如输入/输出管脚等。

第十方面，提供了一种通信系统，所述通信系统包括前述的第五方面所述的任一通信装置、第六方面所述的任一通信装置；或者，所述通信系统包括前述的第七方面所述的任一通信装置、第八方面所述的任一通信装置。

第十一方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于实现上述各方面的方法中 UDM 或 AUSF 的功能。在一种可能的设计中，所述芯片系统还包括存储器，用于保存程序指令和/或数据。该芯片系统，可以由芯片构成，也可以包括芯片和其他分立器件。

第十二方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码并运行时，使得上述各方面中由 UDM 或 AUSF 执行的方法被执行。

第十一方面，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存储有计算机程序，当该计算机程序被运行时，实现上述各方面中 UDM 或 AUSF 执行的方法。

在本申请实施例中，UDM 向第一 AUSF 发送的用于保护终端的参数更新信息的保护请求消息中携带了用于指示第一服务网络的标识。即使终端通过多个服务网络注册到 HN，即在一个 AUSF 对应多个密钥的情况下，能够明确第一 AUSF 采用哪个密钥，保证终端成功校验 UDM 进行终端参数更新流程中的参数更新信息。

附图说明

图 1 为本申请实施例提供的一种网络架构示意图；

图 2 为本申请实施例提供的网络架构下的一种漫游架构示意图；

图 3 为本申请实施例提供的网络架构下的另一种漫游架构示意图；

图 4 为本申请实施例提供的一种终端参数更新的保护方法的一流程示意图；

图 5 为本申请实施例提供的一种终端参数更新的保护方法的另一流程示意图；

图 6 为本申请实施例提供的另一种终端参数更新的保护方法的流程示意图；

图 7 为本申请实施例提供的通信装置的一种结构示意图；

图 8 为本申请实施例提供的通信装置的另一种结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。另外，需要理解的是，在本申请实施例的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

本申请实施例适用的网络架构的示意图，该网络架构可以用于 NR 通信系统，也可以用于下一代通信系统。该网络架构包括核心网、接入网和终端。

其中，接入网的主要功能是控制终端通过无线接入到移动通信网络。接入网是移动通信系统的一部分。它实现了一种无线接入技术。从概念上讲，它驻留某个设备之间（如移动电话、一台计算机，或任何远程控制台），并提供与其核心网的连接。

核心网包括 VPLMN 和 HPLMN，VPLMN 包括移动性管理网元（本文以 AMF 实施例为例）、会话管理网元（本文以 SMF 实施例为例）、策略控制网元（本文以 PCF 实施例为例）等。HPLMN 中包括认证服务功能网元（本文以 AUSF 实施例为例）、数据管理网元（本文以 UDM 实施例为例）、AMF 实体、PCF 实体等。

其中，AMF 可负责终端的认证、终端的移动性管理、选择 SMF 实体，以及维护和管理终端的状态信息等。在 5G 中，移动性管理网元可以是 AMF 网元，在未来通信如第六代（the 6th generation, 6G）中，移动性管理网元仍可以是 AMF 网元，或有其它的名称，本申请不做限定。

SMF 包括会话管理（如会话建立、修改和释放，包含 UPF 和 RAN 之间的隧道维护）、UPF 网元的选择和控制、业务和会话连续性（Service and Session Continuity, SSC）模式选择、漫游等会话相关的功能。在 5G 中，会话管理网元可以是 SMF 网元，在未来通信如 6G 中，会话管理网元仍可以是 SMF 网元，或有其它的名称，本申请不做限定。

UPF 包括数据包路由和传输、包检测、业务用量上报、服务质量（Quality of Service, QoS）处理、合法监听、上行包检测、下行数据包存储等用户面相关的功能。在 5G 中，用户面网元可以是 UPF 网元，在未来通信如 6G 中，用户面网元仍可以是 UPF 网元，或有其它的名称，本申请不做限定。

UDM 是由运营商提供的控制面网元，负责存储运营商网络中签约用户的用户永久标识符(subscriber permanent identifier, SUPI)、信任状(credential)、安全上下文(security context)、签约数据等信息。UDM 网元所存储的这些信息可用于终端设备接入运营商网络的认证和授权。其中，上述运营商网络的签约用户具体可为使用运营商网络提供的业务的用户，例如使用中国电信的手机芯卡的用户，或者使用中国移动的手机芯卡的用户等。上述签约用户的永久签约标识(Subscription Permanent Identifier, SUPI)可为该手机芯卡的号码等。上述签约用户的信任状、安全上下文可为该手机芯卡的加密密钥或者跟该手机芯卡加密相关的

信息等存储的小文件，用于认证和/或授权。上述安全上下文可为存储在用户本地终端（例如手机）上的数据（cookie）或者令牌（token）等。上述签约用户的签约数据可为该手机芯卡的配套业务，例如该手机芯卡的流量套餐或者使用网络等。需要说明的是，永久标识符、信任状、安全上下文、认证数据（cookie）、以及令牌等同认证、授权相关的信息，在本发明本申请文件中，为了描述方便起见不做区分、限制。如果不做特殊说明，本申请实施例将以用安全上下文为例进行来描述，但本申请实施例同样适用于其他表述方式的认证、和/或授权信息。在 5G 中，数据管理网元可以是 UDM 网元，在未来通信如 6G 中，数据管理网元仍可以是 UDM 网元，或有其它的名称，本申请不做限定。

PCF 是由运营商提供的控制面功能，用于向 SMF 网元提供 PDU 会话的策略。策略可以包括计费相关策略、QoS 相关策略和授权相关策略等。在 5G 中，策略控制网元可以是 PCF 网元，在未来通信如 6G 中，策略控制网元仍可以是 PCF 网元，或有其它的名称，本申请不做限定。

AUSF 具有鉴权服务功能，用于终结对终端进行认证的网元请求的认证功能，在认证过程中，接收 UDM 发送的认证向量并对认证向量进行处理，将处理后的认证向量发送给对终端进行认证的网元。

终端，也可以称为用户设备（user equipment, UE），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）。所述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、增强现实（augmented reality, AR）终端、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程医疗（remote medical）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端等。

HPLMN 中的实体之间可以通过接口相互通信，也可以通过接口与 VPLMN 之间的实体进行通信。例如在漫游场景下，HPLMN 需要向终端发送参数，例如优选的 PLMN 等归属网络的参数或需要更新的签约数据。HPLMN 中的实体例如 UDM 需要通过 VPLMN 的实体例如 AMF 将这些参数发送给终端。再列如，HPLMN 的 PCF 实体需要将策略信息，依次通过 VPLMN 的 PCF 实体、VPLMN 的 AMF 实体发送给终端。由于这些参数的安全等级等，HPLMN 需要防止 VPLMN 等对这些参数进行篡改，所以 HPLMN 向终端发送这些参数的过程中，通过 HPLMN 中的 AUSF 生成的密钥对这些参数进行加密保护处理。由于终端在进行网络注册过程中会生成密钥，所以只要终端的密钥和 AUSF 保护 HPLMN 与终端之间的参数的密钥一致，那么对于终端而言，接收到这些参数可通过相应的密钥对其进行校验。

但是在终端双注册的场景中，可能会出现 AUSF 所选择的密钥与终端侧的密钥不一致，最终导致终端校验失败。

例如，图 2 示出了本申请实施例适用的一种的网络架构的漫游架构图。在该图 2 中，终端通过两个服务网络（serving network, SN）进行注册，即终端采用密钥 1 在 AMF1 进行注册，终端采用密钥 2 在 AMF2 注册。AMF1 和 AMF2 选择了终端的 HN 中的同一个

AUSF, 应理解, 该 AUSF 对应两个密钥 (即密钥 1 和密钥 2)。或者, 终端先通过 SN1 注册到 HN, 再通过 SN2 注册到 HN, 且 SN1 和 SN2 选择了终端的 HN 中的同一个 AUSF。这种情况下, 如果 UDM 需要进行 SoR 流程或终端参数更新 (UE parameters update, UPU) 流程, 则 UDM 向 AUSF 发送保护请求消息, 如果 AUSF 随机选择其中的一个密钥对 SoR 信息或 UPU 信息进行加密保护, AUSF 所选择的密钥可能与终端侧的密钥不一致, 导致终端对接收的 SoR 信息或 UPU 信息校验失败。例如 UDM 选择 AMF2 进行后续 SoR 流程, 但是 AUSF 所选择的密钥是密钥 1, 显然与终端侧的密钥 2 不一致, 最终导致终端侧对接收的 SoR 信息校验失败。

又例如, 图 3 示出了本申请实施例适用的一种的网络架构的漫游架构图。在该图 3 中, 终端通过两个 AN 进行注册, 即终端采用密钥 1 在 AMF1 进行注册, 终端采用密钥 2 在 AMF2 注册。AMF1 选择了终端的 HN 中的 AUSF1, AMF2 选择了终端的 HN 中的 AUSF2, 应理解, 该 AUSF1 存在密钥 1, AUSF2 存在密钥 2。与图 2 类似, AUSF 侧有两个密钥。这种情况下, 如果 UDM 随机选择一个 AUSF 对 SoR 信息或 UPU 信息进行加密保护, 所选择的 AUSF 上的密钥可能与终端侧的密钥不一致, 导致终端对接收的 SoR 信息或 UPU 信息校验失败。例如终端侧在 AMF1 进行后续 SoR 流程, 但是 UDM 选择 AUSF2 对 SoR 信息进行保护, 即 AUSF2 所选择的密钥是密钥 2, 显然与终端侧的密钥 1 不一致, 最终导致终端侧对接收的 SoR 信息校验失败。

鉴于此, 本申请实施例提供一种网络漫游保护方法和通信装置。在本申请实施例中, UDM 在向 AUSF 发送保护请求消息时携带 SN 的标识, 即 UDM 指示所选择的 SN, 从而 AUSF 选择与 SN 对应的密钥。由于终端的密钥与 SN 唯一对应, AUSF 选择的密钥也与 SN 唯一对应, 所以可保证 AUSF 侧的密钥和终端侧的密钥一致, 保证终端成功校验 UDM 进行的 SoR 流程中的 SoR 信息或者 UDM 进行 UPU 流程中的 UPU 信息。

下面结合附图对本申请实施例提供的定位方法进行详细介绍。

请参见图 4, 为本申请实施例提供的定位方法的流程图。在下文的介绍过程中, 以该方法应用于图 1-图 3 所示的通信系统为例。另外, 该方法可由两个通信装置执行, 这两个通信装置例如为第一通信装置和第二通信装置。为了便于介绍, 在下文中, 以该方法由 AUSF 和 UDM 执行为例, 也就是, 以第一通信装置是 UDM、第二通信装置是 AUSF 为例。需要说明的是, 本申请实施例只是以通过图 1-图 3 的通信系统为例, 并不限制于这种场景。且本申请实施例适用于保护 HPLMN 通过 AMF 向终端发送的参数更新信息的保护, 例如可适应 SoR 流程, 也可适用 UPU 流程。下文以终端的参数更新信息是 SoR 信息为例。

具体的, 本申请实施例提供的终端参数更新的保护方法的具体流程描述如下:

S401、UDM 向第一 AUSF 发送保护请求消息, 第一 AUSF 接收该保护请求消息, 该保护请求消息用于请求保护终端的参数更新信息, 该保护请求消息携带参数更新信息和第一 SN 信息。

本申请实施例旨在解决终端通过多个 SN 注册到 HN 的情况下, 用于保护 HPLMN 向终端之间发送的参数的 AUSF 采用的密钥与终端侧的密钥不一致的问题。为此, 本申请实施例中, UDM 在向第一 AUSF 发送的保护请求消息中携带 SN 的标识信息。应理解, 该标识信息用于指示为终端服务的某个 SN, 在本文中, 称为第一 SN。也就是 UDM 可事先从

多个 SN 中选择第一 SN，从而选择与该第一 SN 对应的 AUSF 对终端的参数更新信息进行加密保护。由于终端的密钥与第一 SN 唯一对应，AUSF 选择的密钥也与第一 SN 唯一对应，所以可保证 AUSF 侧的密钥和终端侧的密钥一致，保证终端成功校验 UDM 进行的 SoR 流程中的 SoR 信息或者 UDM 进行 UPU 流程中的 UPU 信息。

应理解，如果终端的参数更新信息是 SoR 信息，那么保护请求消息用于请求保护 SoR 信息的，所以在一些实施例中，该保护请求消息也称为 SoR 保护请求 (SoR protection request) 消息。需要说明的是，本申请实施例对该保护请求消息的具体名称不作限制，例如如果保护请求消息用于保护终端更新的签约数据，那么该保护请求消息也可以称为 UPU 保护请求消息。

标识第一 SN 的具体实现方式有多种，本申请实施例不作限制。示例性的，用于标识第一 SN 的 SN 信息可以是第一 SN 的名称，也可以是包括第一 SN 的 PLMN ID，或者可以是第一 SN 的 ID。或者，该第一 SN 信息可包括终端的认证事件的标识。应理解，终端的认证事件的标识 (authEvent ID) 是在认证流程中由 UDM 发送给 AUSF 用来标识 UE 在第一 SN 认证的一次认证事件，所以 authEvent ID 可唯一对应一个密钥。

S402、第一 AUSF 根据保护请求消息中的第一 SN 信息确定第一密钥，并根据第一密钥对终端的参数更新信息进行安全保护。

应理解，第一密钥可以认为是认证服务功能密钥 (Kausf)。如果第一服务网络信息为第一 SN 的名称或者第一 SN 的 ID 或者第一 SN 的 PLMN ID，第一 AUSF 可根据 SUPI 和第一服务网络信息选择对应的 Kausf，通过该 Kausf 对保护请求消息中携带的 SoR 信息进行加密保护。如果第一服务网络信息为 authEvent ID，那么第一 AUSF 可根据 authEvent ID 选择对应的 Kausf，通过该 Kausf 对保护请求消息中携带的 SoR 信息进行加密保护。第一 AUSF 对终端的参数进行保护之后，可以生成保护结果，例如 MAC 值等信息。

S403、第一 AUSF 向 UDM 发送该保护请求消息的响应消息。

应理解，第一 AUSF 生成保护结果之后，向 UDM 发送响应消息，该响应消息是前述保护请求消息的响应消息。

在一些实施例中，该响应消息可以包括 SoR 计数器或 UPU 计数器，SoR 消息认证码 MAC 或 UPU 消息认证码 MAC 等，以告知第一 AUSF 对终端的参数更新信息的保护结果。

S404、UDM 通过与第一服务网络对应的 AMF 发送终端的参数更新信息。

UDM 接收到第一 AUSF 发送的响应消息之后，可以通过第一 SN 进行终端的参数更新流程，例如 SoR 流程。示例性的，UDM 向位于第一 SN 中的 AMF 发起签约数据管理通知 (SDM notification) 服务调用请求消息，该请求消息中携带漫游配置信息，例如 PLMN 和接入技术组合的优先列表、SoR 的消息认证码 MAC 等信息。

在一些实施例中，UDM 在向第一 AUSF 发送保护请求消息之前，确定进行终端的参数更新流程的第一 SN。终端可能处于单注册状态，也可能处于双注册状态下，当终端处于单注册状态下，UDM 也可以不确定第一 SN，即不执行确定步骤。

示例性的，请参见图 5，为本申请实施例提供的终端参数更新的保护方法的一示例性的流程图。

S501、UDM 在向第一 AUSF 发送保护请求消息之前，确定进行终端的参数更新流程的

第一 SN。

本申请实施例中，UDM 发送保护请求消息之前，可确定发送终端的参数更新信息的 AMF 所在的第一 SN。由于在发送保护请求消息之前，选择了第一 SN，所以即使在终端处于双注册状态（即终端通过至少两个服务网络进行注册），且这至少两个服务网络中的 AMF 选择同一个 AUSF 的情况下，也能够保证第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。

在一些实施例中，UDM 可以根据本地策略确定发送终端的参数更新信息的 AMF 所在的第一 SN，例如根据优先级等确定发送终端的参数更新信息的 AMF 所在的第一 SN。

进一步的，UDM 在确定存在多个 SN 的情况下，确定后续进行终端的参数更新流程的第一 SN，可以避免存在一个 SN 的情况下，UDM 也判断后续进行终端的参数更新流程的第一 SN，与现有终端的参数更新流程机制更好地兼容。

S502、UDM 在向第一 AUSF 发送保护请求消息之前，判断 AUSF 是否存在多个密钥。

示例性的，UDM 在向第一 AUSF 发送保护请求消息之前，可以判断第一 AUSF 是否有终端在多个 SN 的认证结果。如果第一 AUSF 有终端在多个 SN 的认证结果，可以认为第一 AUSF 存在多个密钥，这种情况下，UDM 向第一 AUSF 发送的保护请求消息可以携带 SN 的标识。应理解，这多个 SN 包括第一 SN。相反，如果第一 AUSF 没有终端在多个 SN 的认证结果，可以认为第一 AUSF 不存在多个密钥，也就是第一 AUSF 存在一个密钥。这种情况下，UDM 向第一 AUSF 发送的保护请求消息可以不携带 SN 的标识。

又一示例性的，UDM 在向第一 AUSF 发送保护请求消息之前，可以判断终端是否在多个 SN。如果终端在多个 SN，可以认为第一 AUSF 存在多个密钥，此时 UDM 向第一 AUSF 发送的保护请求消息可以携带 SN 的标识。应理解，这多个 SN 包括第一 SN。相反，如果终端不在多个 SN，可以认为第一 AUSF 不存在多个密钥，也就是第一 AUSF 存在一个密钥。这种情况下，UDM 向第一 AUSF 发送的保护请求消息可以不携带 SN 的标识。

需要说明的是，终端有多个 SN 指的是终端设备接入多个 SN；或者，多个 SN 为终端提供服务；或者，终端在多个 SN 进行注册；或者，终端在多个 SN 进行认证；或者，终端在 UDM 上有在多个 SN 的注册状态；或者，终端在 UDM 上有在多个 SN 的认证状态。

再一示例性的，UDM 在向第一 AUSF 发送保护请求消息之前，可以判断终端是否处于双注册状态，即终端同时通过两个 SN 注册到 HN。如果终端处于双注册状态，可以认为第一 AUSF 存在多个密钥，此时 UDM 向第一 AUSF 发送的保护请求消息可以携带 SN 的标识。相反，如果终端没有处于双注册状态，可以认为第一 AUSF 不存在多个密钥，也就是第一 AUSF 存在一个密钥。这种情况下，UDM 向第一 AUSF 发送的保护请求消息可以不携带 SN 的标识。

UDM 在向第一 AUSF 发送保护请求消息之前，判断 AUSF 是否存在多个密钥，在确定 AUSF 存在多个密钥的情况下，UDM 才发送 SN 的标识，可避免发送的保护请求消息携带不必要的标识。且 UDM 通过第一 SN 的标识指定某个密钥，使得第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。

S503、UDM 在向第一 AUSF 发送保护请求消息之前，确定与第一 SN 对应的第一 AUSF。

在本申请实施例中，第一 AUSF 可以是终端双注册场景中，多个 SN 所选择的某个 AUSF，

如图 2 所示的 AUSF; 第一 AUSF 也可以是终端双注册场景中, 多个 AUSF 中的某个 AUSF, 例如图 3 所示的 2 个 AUSF 中的某个 AUSF。应理解, 在图 3 所示的场景中, 第一 AUSF 是 UDM 从多个 AUSF 中的选择的。所以 UDM 在向第一 AUSF 发送保护请求消息之前, 可以从多个 AUSF 选择第一 AUSF。这样即使终端先后通过不同的多个服务网络注册到 HN, 且不同的服务网络选择不同的 AUSF, 由于 UDM 指定第一 AUSF 保护 SoR 信息, 第一 AUSF 对应唯一 SN (也可认为对应唯一密钥), 因此可保证第一 AUSF 所选择的密钥与终端认证过程中生成的密钥一致。

需要说明的是, S501、S502 和 S503 不是必不可少的步骤, 因此在图 5 中用虚线进行示意。且本申请实施例对 S501、S502 和 S503 的先后顺序不作限制。

作为前述实施例的一种可替换的方案, 请参见图 6, 为本申请实施例提供的另一种终端参数更新的保护方法的流程示意图。该流程描述如下:

S601、UDM 向第一 AUSF 发送第一消息, 第一 AUSF 接收该第一消息, 该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一 SN 注册时所生成的第一密钥, 第一 AUSF 为终端在第一 SN 注册时进行认证的 AUSF。

S602、第一 AUSF 删除终端在所述第一 AMF 所在的第一 SN 注册时生成的第一密钥。

S603、UDM 在确定终端处于单注册状态的情况下, 确定通过第二 AMF 发送终端的参数更新信息。

在可能的一种场景中, 例如终端先通过 SN1 注册到 HN, 之后再通过 SN2 注册到 HN, 这种情况下, AUSF 上也存在两个第一密钥。对此, 在本申请实施例中, 当终端通过另一个 AMF (下文以第二 AMF 为例) 所在 SN 进行注册时, UDM 可以指示对应的 AUSF 删除终端在已注册 AMF (下文以第一 AMF 为例) 所在的第一 SN 注册时所使用的第一密钥。这样即使终端在第二 AMF 所在的第二 SN 注册, 也能够保证 AUSF 上的密钥是唯一的, 也就是与终端认证过程中的密钥一致。

应理解, 第一消息携带第一服务网络的标识信息或者终端的身份标识信息, 以使得 AUSF 确定删除与第一服务网络对应的密钥。

应理解, UDM 向第一 AMF 发送第二消息, 例如用于删除终端的注册信息的信息 (Nudm_UECM_DeregistrationNotify 消息) 时, 向第一 AUSF 发送第一消息; 或者 UDM 在接收到第一 AMF 发送的第二消息的响应消息, 即第三消息 (Nudm_SDM_Unsubscribe 消息) 时, 向第一 AUSF 发送第一消息。

在本申请实施例中, UDM 向第一 AUSF 发送的用于保护终端的参数更新信息的保护请求消息中携带了用于指示第一服务网络的标识。即使终端通过多个服务网络注册到 HN, 即在一个 AUSF 对应多个密钥的情况下, 能够明确第一 AUSF 采用哪个密钥, 保证终端成功校验 UDM 进行终端参数更新流程中的参数更新信息。

作为前述实施例的一种可替换的方案, 为保证终端和 AUSF 在需要使用认证服务功能密钥 K_{AUSF} 时获取到相同的 K_{AUSF} , UE, AUSF 以及 UDM 可以通过执行以下动作来保证:

终端在收到安全模式命令 SMC 消息后或收到安全模式命令 SMC 消息并验证成功后或收到 AUTN 并校验成功后或发送认证响应后或发送安全模式完成 security mode complete 消息之后或收到扩展认证协议成功消息 EAP success 或生成新的 K_{AUSF} 后删除存储的旧的

K_{AUSF}或删除存储的在同一服务网络生成的旧的 K_{AUSF}。作为一种可选的实施方式,终端在生成新的 K_{AUSF}和/或上述条件满足情况下,还可以设定一个定时器,在所述定时器结束时删除存储的旧的 K_{AUSF}或删除在同一服务网络生成的旧的 K_{AUSF}。

AUSF 在对终端返回的认证响应校验成功后或向 UDM 发送终端的认证结果确认请求后或生成新的 K_{AUSF}或收到 UDM 返回的终端的认证结果确认响应后则删除存储的所述终端认证中产生的旧的 K_{AUSF}或删除所述终端在同一服务网络认证中产生的旧的 K_{AUSF}。作为一种可选的实施方式,AUSF 在和终端认证中生成新的 K_{AUSF}和/或上述条件满足情况下,还可以设定一个定时器,在所述定时器结束时删除存储的所述终端认证中产生的旧的 K_{AUSF}或删除所述终端在同一服务网络认证中产生的旧的 K_{AUSF}。

UDM 在需要进行 SoR 或 UPU 时,则会选择最近与终端成功完成认证流程的 AUSF。应理解,AUSF 在完成与终端认证后会向 UDM 返回终端的认证结果,认证结果会记录认证的时间以及服务网络名称,所以 UDM 可以根据记录的时间选择最近完成认证的 AUSF。作为一种可选的实施方式,由于认证结果还记录有服务网络名称,所以 UDM 还可以选择进行 SoR 或 UPU 的服务网络中最近与终端成功完成认证流程的 AUSF。作为一种可选的实施方式,由于不同 AUSF 之间可以共享相同终端的 K_{AUSF},所以 UDM 也可以任选一个 AUSF。

这样即使终端先后通过不同的多个服务网络注册到 HN,且不同的服务网络选择相同的或不同的 AUSF,由于 UE 和 AUSF 侧保持了相同的 K_{AUSF},所以 UDM 指定 AUSF 保护 SoR 或 UPU 信息时,AUSF 处只有唯一的密钥 K_{AUSF}或针对同一服务网络只有唯一的 K_{AUSF},因此可保证 AUSF 所选择的密钥与终端选择的密钥一致。

具体的,例如在终端与网络进行主认证流程中,对于 EAP-AKA' 认证,UDM 向 AUSF 返回 UE 认证获取响应,携带密钥 CK' 和 IK'。AUSF 接收到 UDM 返回的 UE 认证获取响应后,向安全锚点功能 SEAF (可能与 AMF 共部署)返回 UE 认证响应。SEAF 在收到 AUSF 返回的 UE 认证响应后,向 UE 发起认证请求。UE 接收到 SEAF 发送的认证请求,计算认证响应以及密钥 CK' 和 IK',然后向 SEAF 返回认证响应,携带 EAP 响应。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求,携带所述 EAP 响应。AUSF 认证所收到的 EAP 响应,如果认证成功,AUSF 会根据从 UDM 获取的 CK' 和 IK' 生成第一 K_{AUSF},同时删除存储的旧的 K_{AUSF} (如果有的话)。接着 AUSF 会向 SEAF 返回 UE 认证响应,携带 EAP success 消息。SEAF 在收到 AUSF 的 UE 认证响应后,向 UE 返回 EAP success 消息。UE 收到 EAP success 消息后会根据计算的 CK' 和 IK' 生成第二 K_{AUSF},同时删除存储的旧的 K_{AUSF} (如果有的话)。其中,所述第一 K_{AUSF}和第二 K_{AUSF}相同。这就使得 UE 和 AUSF 侧在主认证流程中删除存储的旧的 K_{AUSF},从而保证 UE 和 AUSF 侧只存在唯一的第一和第二 K_{AUSF}。在 UDM 需要进行 SoR 或 UPU 时,UDM 选择最近与 UE 完成主认证的 AUSF,则所选择的 AUSF 只保存有与 UE 一致的 K_{AUSF},从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。

具体的,例如在终端与网络进行主认证流程中,对于 5G AKA 认证,UDM 向 AUSF 返回 UE 认证获取响应,携带第一 K_{AUSF}。AUSF 接收到 UDM 返回的 UE 认证获取响应后,向安全锚点功能 SEAF (可能与 AMF 共部署)返回 UE 认证响应,携带认证令牌 AUTN。SEAF 在收到 AUSF 返回的 UE 认证响应后,向 UE 发起认证请求,携带所述 AUTN。UE

接收到 SEAF 发送的认证请求, 校验所述 AUTN 成功后, 计算认证响应 RES*以及第二密钥 KAUSF, 同时删除存储的旧的 KAUSF (如果有的话), 然后向 SEAF 返回认证响应, 携带所述 RES*。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求, 携带所述 RES*。AUSF 认证所收到的所述 RES*后, 如果认证成功, AUSF 会删除存储的旧的 KAUSF (如果有的话), 如果校验失败则删除第一 KAUSF。其中, 所述第一 KAUSF 和第二 KAUSF 相同。这就使得 UE 和 AUSF 侧在主认证流程中删除存储的旧的 KAUSF, 从而保证 UE 和 AUSF 侧只存在唯一的第一和第二 KAUSF。在 UDM 需要进行 SoR 或 UPU 时, UDM 选择最近与 UE 完成主认证的 AUSF, 则所选择的 AUSF 只保存有与 UE 一致的 KAUSF, 从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。

具体的, 还例如在终端与网络进行主认证和安全模式命令 SMC 流程中。对于 EAP-AKA' 认证, UDM 向 AUSF 返回 UE 认证获取响应, 携带密钥 CK' 和 IK'。AUSF 接收到 UDM 返回的 UE 认证获取响应后, 向安全锚点功能 SEAF (可能与 AMF 共部署) 返回 UE 认证响应。SEAF 在收到 AUSF 返回的 UE 认证响应后, 向 UE 发起认证请求。UE 接收到 SEAF 发送的认证请求, 计算认证响应以及密钥 CK' 和 IK', 然后向 SEAF 返回认证响应, 携带 EAP 响应。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求, 携带所述 EAP 响应。AUSF 认证所收到的 EAP 响应, 如果认证成功, AUSF 会根据从 UDM 获取的 CK' 和 IK' 生成第一 KAUSF, 同时删除存储的旧的 KAUSF (如果有的话)。接着 AUSF 会向 SEAF 返回 UE 认证响应, 携带 EAP success 消息。SEAF 在收到 AUSF 的 UE 认证响应后, 向 UE 返回 EAP success 消息。UE 收到 EAP success 消息后会根据计算的 CK' 和 IK' 生成第二 KAUSF。其中, 所述第一 KAUSF 和第二 KAUSF 相同。在认证之后, AMF 则会向终端发送安全模式命令 SMC 消息, 终端对所述安全模式命令 SMC 消息完整性校验成功后则删除存储的旧的 KAUSF (如果有的话)。这就使得 UE 和 AUSF 侧在主认证流程和安全模式命令 SMC 流程中删除存储的旧的 KAUSF, 从而保证 UE 和 AUSF 侧只存在唯一的第一和第二 KAUSF。在 UDM 需要进行 SoR 或 UPU 时, UDM 选择最近与 UE 完成主认证的 AUSF, 则所选择的 AUSF 只保存有与 UE 一致的 KAUSF, 从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。

具体的, 还例如在终端与网络进行主认证和安全模式命令 SMC 流程中, 对于 5G AKA 认证, UDM 向 AUSF 返回 UE 认证获取响应, 携带第一 KAUSF。AUSF 接收到 UDM 返回的 UE 认证获取响应后, 向安全锚点功能 SEAF (可能与 AMF 共部署) 返回 UE 认证响应, 携带认证令牌 AUTN。SEAF 在收到 AUSF 返回的 UE 认证响应后, 向 UE 发起认证请求, 携带所述 AUTN。UE 接收到 SEAF 发送的认证请求, 校验所述 AUTN 成功后, 计算认证响应 RES*以及第二密钥 KAUSF, 然后向 SEAF 返回认证响应, 携带所述 RES*。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求, 携带所述 RES*。AUSF 认证所收到的所述 RES*后, 如果认证成功, AUSF 会删除存储的旧的 KAUSF (如果有的话), 如果校验失败则删除第一 KAUSF。其中, 所述第一 KAUSF 和第二 KAUSF 相同。在认证之后, AMF 则会向终端发送安全模式命令 SMC 消息, 终端对所述安全模式命令 SMC 消息完整性校验成功后则删除存储的旧的 KAUSF (如果有的话)。这就使得 UE 和 AUSF 侧在主认证流程和安全模式命令 SMC 流程中删除存储的旧的 KAUSF, 从而保证 UE 和 AUSF 侧只存在唯一的第一和第

二 K_{AUSF} 。在 UDM 需要进行 SoR 或 UPU 时, UDM 选择最近与 UE 完成主认证的 AUSF, 则所选择的 AUSF 只保存有与 UE 一致的 K_{AUSF} , 从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。具体的, 还例如在终端与网络进行主认证流程和安全模式命令 SMC 流程以及认证结果确认流程中。对于 EAP-AKA' 认证, UDM 向 AUSF 返回 UE 认证获取响应, 携带密钥 CK' 和 IK'。AUSF 接收到 UDM 返回的 UE 认证获取响应后, 向安全锚点功能 SEAF (可能与 AMF 共部署) 返回 UE 认证响应。SEAF 在收到 AUSF 返回的 UE 认证响应后, 向 UE 发起认证请求。UE 接收到 SEAF 发送的认证请求, 计算认证响应以及密钥 CK' 和 IK', 然后向 SEAF 返回认证响应, 携带 EAP 响应。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求, 携带所述 EAP 响应。AUSF 认证所收到的 EAP 响应, 如果认证成功, AUSF 会根据从 UDM 获取的 CK' 和 IK' 生成第一 K_{AUSF} 。接着 AUSF 会向 SEAF 返回 UE 认证响应, 携带 EAP success 消息。SEAF 在收到 AUSF 的 UE 认证响应后, 向 UE 返回 EAP success 消息。UE 收到 EAP success 消息后会根据计算的 CK' 和 IK' 生成第二 K_{AUSF} 。其中, 所述第一 K_{AUSF} 和第二 K_{AUSF} 相同。在认证之后, AMF 则会向终端发送安全模式命令 SMC 消息, 终端对所述安全模式命令 SMC 消息完整性校验成功后则删除存储的旧的 K_{AUSF} (如果有的话)。同时在 AUSF 完成对 UE 的认证后, 同时, AUSF 完成对 UE 的认证后, AUSF 会向 UDM 发送终端的认证结果确认请求, 并在收到 UDM 返回的终端的认证结果确认响应后, 删除存储的旧的 K_{AUSF} (如果有的话)。这就使得 UE 和 AUSF 侧在主认证流程和安全模式命令 SMC 流程以及认证结果确认流程中删除存储的旧的 K_{AUSF} , 从而保证 UE 和 AUSF 侧只存在唯一的第一和第二 K_{AUSF} 。在 UDM 需要进行 SoR 或 UPU 时, UDM 选择最近与 UE 完成主认证的 AUSF, 则所选择的 AUSF 只保存有与 UE 一致的 K_{AUSF} , 从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。

具体的, 还例如在终端与网络进行主认证流程和安全模式命令 SMC 流程以及认证结果确认流程中, 对于 5G AKA 认证, UDM 向 AUSF 返回 UE 认证获取响应, 携带第一 K_{AUSF} 。AUSF 接收到 UDM 返回的 UE 认证获取响应后, 向安全锚点功能 SEAF (可能与 AMF 共部署) 返回 UE 认证响应, 携带认证令牌 AUTN。SEAF 在收到 AUSF 返回的 UE 认证响应后, 向 UE 发起认证请求, 携带所述 AUTN。UE 接收到 SEAF 发送的认证请求, 校验所述 AUTN 成功后, 计算认证响应 RES* 以及第二密钥 K_{AUSF} , 然后向 SEAF 返回认证响应, 携带所述 RES*。SEAF 接收到 UE 的认证响应后向 AUSF 发起 UE 认证请求, 携带所述 RES*。其中, 所述第一 K_{AUSF} 和第二 K_{AUSF} 相同。在认证之后, AMF 则会向终端发送安全模式命令 SMC 消息, 终端对所述安全模式命令 SMC 消息完整性校验成功后则删除存储的旧的 K_{AUSF} (如果有的话)。同时, AUSF 完成对 UE 的认证后, AUSF 会向 UDM 发送终端的认证结果确认请求, 并在收到 UDM 返回的终端的认证结果确认响应后, 删除存储的旧的 K_{AUSF} (如果有的话)。这就使得 UE 和 AUSF 侧在主认证流程和安全模式命令 SMC 流程以及认证结果确认流程中删除存储的旧的 K_{AUSF} , 从而保证 UE 和 AUSF 侧只存在唯一的第一和第二 K_{AUSF} 。在 UDM 需要进行 SoR 或 UPU 时, UDM 选择最近与 UE 完成主认证的 AUSF, 则所选择的 AUSF 只保存有与 UE 一致的 K_{AUSF} , 从而可以保证 AUSF 所选择的密钥与终端选择的密钥一致。

上述本申请提供的实施例中, 从 UDM 和 AUSF 之间交互的角度对本申请实施例提供

的方法进行了介绍。为了实现上述本申请实施例提供的方法中的各功能，UDM 和 AUSF 可以包括硬件结构和/或软件模块，以硬件结构、软件模块、或硬件结构加软件模块的形式来实现上述各功能。上述各功能中的某个功能以硬件结构、软件模块、还是硬件结构加软件模块的方式来执行，取决于技术方案的特定应用和设计约束条件。

下面结合附图介绍本申请实施例中用来实现上述方法的装置。因此，上文中的内容均可以用于后续实施例中，重复的内容不再赘述。

如图 7 所示，为本申请所涉及的通信装置的一种可能的示例性框图，该通信装置 700 可以对应实现上述各个方法实施例中由 UDM 或 AUSF 实现的功能或者步骤。该通信装置可以包括收发模块 701 和处理模块 702。可选的，还可以包括存储模块，该存储模块可以用于存储指令（代码或者程序）和/或数据。收发模块 701 和处理模块 702 可以与该存储模块耦合，例如，处理模块 702 可以读取存储模块中的指令（代码或者程序）和/或数据，以实现相应的方法。上述各个模块可以独立设置，也可以部分或者全部集成。

应理解，处理模块 702 可以是处理器或控制器，例如可以是通用中央处理器（central processing unit, CPU），通用处理器，数字信号处理（digital signal processing, DSP），专用集成电路（application specific integrated circuits, 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、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述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。收发模块 701 是一种该装置的接口电路，用于从其它装置接收信号。例如，当该装置以芯片的方式实现时，该收发模块 701 是该芯片用于从其它芯片或装置接收信号的接口电路，或者，是该芯片用于向其它芯片或装置发送信号的接口电路。

该通信装置 700 可以为上述实施例中的 UDM 或 AUSF，还可以为用于 UDM 或 AUSF 的芯片。例如，当通信装置 700 为 UDM 或 AUSF 时，该处理模块 702 例如可以是处理器，该收发模块 701 例如可以是收发器。可选的，该收发器可以包括射频电路，该存储单元例如可以是存储器。例如，当通信装置 700 为用于 UDM 或 AUSF 的芯片时，该处理模块 702 例如可以是处理器，该收发模块 701 例如可以是输入/输出接口、管脚或电路等。该处理模块 702 可执行存储单元存储的计算机执行指令，可选地，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是该网络设备、终端或定位管理设备内的位于该芯片外部的存储单元，如只读存储器（read-only memory, ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory, RAM）等。

一些可能的实施方式中，通信装置 700 能够对应实现上述方法实施例中 UDM 的行为和功能。例如通信装置 700 可以为 UDM，也可以为应用于 UDM 中的部件（例如芯片或者电路）。收发模块 701 可以用于支持 UDM 与其他网络实体的通信，例如支持 UDM 与图 4 到图 6 所示的第一 AUSF 和/或 AMF 等之间的通信。处理模块 702 用于对 UDM 的动作进行控制管理，例如处理模块 702 用于支持网络设备执行图 4 到图 6 中 UDM 除收发之外的全部操作。

例如，收发模块 701 可以用于执行图 4 所示的实施例中由 UDM 所执行的全部接收或

发送操作，例如图 4 所示的实施例中的 S401、S403 和 S404，和/或用于支持本文所描述的技术的其它过程。其中，处理模块 702 用于执行如图 4 所示的实施例中的由 UDM 所执行的除了收发操作之外的全部操作，和/或用于支持本文所描述的技术的其它过程。

又例如，收发模块 701 可以用于执行图 5 所示的实施例中的由 UDM 所执行的全部接收或发送操作，例如图 5 所示的实施例中的 S401、S403 和 S404，和/或用于支持本文所描述的技术的其它过程。其中，处理模块 702 用于执行如图 5 所示的实施例中的由 UDM 所执行的除了收发操作之外的全部操作，例如图 5 所示的实施例中的 S501、S502 和 S503，和/或用于支持本文所描述的技术的其它过程。

在一些实施例中，收发模块 701 用于向第一 AUSF 发送保护请求消息，以及接收第一 AUSF 发送的保护请求消息的响应消息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带所述参数更新信息和第一服务网络信息；该处理模块 702 用于控制收发模块 701 通过第一服务网络对应的 AMF 发送所述参数更新信息。

作为一种可选的实施方式，该收发模块 701 还用于：在向第一 AUSF 发送保护请求消息之前，根据本地策略确定第一服务网络信息。

作为一种可选的实施方式，该处理模块 702 具体用于：在确定存在多个服务网络的情况下，确定进行终端的参数更新的所述第一服务网络。

作为一种可选的实施方式，该处理模块 702 具体用于：根据第一服务网络信息确定第一 AUSF。

作为一种可选的实施方式，该处理模块 702 具体用于在向第一 AUSF 发送保护请求消息之前，确定：第一 AUSF 有所述终端在多个服务网络的认证结果，多个服务网络包括所述第一服务网络；或者，

终端在多个服务网络，多个服务网络包括第一服务网络；或者，
终端处于双注册状态。

作为一种可选的实施方式，第一服务网络信息包括第一服务网络的名称；或者，
第一服务网络信息包括第一服务网络的 PLMN 的 ID 或第一服务网络的 ID；或者，
第一服务网络信息包括终端的认证事件的标识。

作为一种可选的实施方式，参数更新信息包括 SoR 信息。

应理解，本申请实施例中的处理模块 702 可以由处理器或处理器相关电路组件实现，收发模块 701 可以由收发器或收发器相关电路组件实现。

又例如，收发模块 701 可以用于执行图 5 所示的实施例中的由 UDM 所执行的全部接收或发送操作，例如图 6 所示的实施例中的 S601、S603，和/或用于支持本文所描述的技术的其它过程。其中，处理模块 702 用于执行如图 6 所示的实施例中的由 UDM 所执行的除了收发操作之外的全部操作，例如图 6 所示的实施例中的 S602，和/或用于支持本文所描述的技术的其它过程。

在一些实施例中，该收发模块 701 用于向第一 AUSF 发送第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；所述处理模块 702 用于在确定终端处于单注册状态的情况下，确定通过第二 AMF 发送终端的参数更新信息。

作为一种可选的实施方式，所述收发模块 701 具体用于在向第一 AMF 发送第二消息或在接收到第一 AMF 发送的第三消息的情况下，向第一 AUSF 发送所述第一消息，其中，第二消息用于删除终端的注册信息，第三消息为第二消息的响应消息。

作为一种可选的实施方式，第一消息携带第一服务网络的标识信息或终端的身份标识信息。

一些可能的实施方式中，通信装置 700 能够对应实现上述方法实施例中第一 AUSF 的行为和功能。例如通信装置 700 可以为 AUSF，也可以为应用于 AUSF 中的部件（例如芯片或者电路）。收发模块 701 可以用于支持 AUSF 与其他网络实体的通信，例如支持 AUSF 与图 4 至图 6 所示的 UDM 之间的通信。处理模块 702 用于对 AUSF 的动作进行控制管理，例如处理模块 702 用于支持 AUSF 执行图 4 至图 6 除收发之外的全部操作。

例如，收发模块 701 可以用于执行图 4 所示的实施例中的由第一 AUSF 所执行的全部接收或发送操作，例如图 4 所示的实施例中的 S401、S403 和 S404，和/或用于支持本文所描述的技术的其它过程。其中，处理模块 702 用于执行如图 4 所示的实施例中的由第一 AUSF 所执行的除了收发操作之外的全部操作，例如图 4 所示的实施例中的 S402，和/或用于支持本文所描述的技术的其它过程。

又例如，收发模块 701 可以用于执行图 5 所示的实施例中的由第一 AUSF 所执行的全部接收或发送操作，例如图 5 所示的实施例中的 S401、S403 和 S404，和/或用于支持本文所描述的技术的其它过程。其中，处理模块 702 用于执行如图 5 所示的实施例中的由第一 AUSF 所执行的除了收发操作之外的全部操作，例如图 5 所示的实施例中的 S402，和/或用于支持本文所描述的技术的其它过程。

该收发模块 701 用于接收 UDM 发送的保护请求消息，该保护请求消息用于请求保护终端的参数更新信息，该保护请求消息携带所述参数更新信息和第一服务网络信息；该处理模块 702 用于根据第一服务网络信息确定第一密钥，以及根据第一密钥对所述参数更新信息进行安全保护，其中，第一密钥用于保护所述参数更新信息；

作为一种可选的实施方式，第一服务网络信息为 UDM 存储的多个第一服务网络信息中的一个服务网络信息。

作为一种可选的实施方式，存在多个 AUSF，所述第一 AUSF 为与所述第一服务网络信息对应的 AUSF。

作为一种可选的实施方式，第一 AUSF 有终端在多个服务网络的认证结果，这多个服务网络包括第一服务网络；或者，

终端在多个服务网络，多个服务网络包括第一服务网络；或者，
终端处于双注册状态。

作为一种可选的实施方式，第一服务网络信息包括第一服务网络的名称；或者，
第一服务网络信息包括第一服务网络的 PLMN 标识；或者，
第一服务网络信息包括终端的认证事件的标识。

作为一种可选的实施方式，所述参数更新信息包括 SoR 信息。

又例如，收发模块 701 可以用于执行图 6 所示的实施例中的由第一 AUSF 所执行的全部接收或发送操作，例如图 6 所示的实施例中的 S601、S603，和/或用于支持本文所描述的技术

术的其它过程。其中，处理模块 702 用于执行如图 6 所示的实施例中由第一 AUSF 所执行的除了收发操作之外的全部操作，例如图 6 所示的实施例中的 S602，和/或用于支持本文所描述的技术的其它过程。

该收发模块 701 用于接收 UDM 发送的第一消息，该第一消息用于指示第一 AUSF 删除终端在第一 AMF 所在的第一服务网络注册时所使用的的第一密钥，第一 AUSF 为终端在第一服务网络注册时进行认证的 AUSF；该处理模块 702 用于删除终端在第一 AMF 所在的第一服务网络注册时使用的的第一密钥。

在一种可能的实现方式中，第一消息携带第一服务网络的标识信息或终端的身份标识信息。

如图 8 所示为本申请实施例提供的通信装置 800，其中，通信装置 800 可以是 UDM，能够实现本申请实施例提供的方法中 UDM 的功能，或者，通信装置 800 可以是 AUSF，能够实现本申请实施例提供的方法中第一 AUSF 的功能；或者，通信装置 800 也可以是能够支持 UDM 或 AUSF 实现本申请实施例提供的方法中对应的功能的装置。其中，该通信装置 800 可以为芯片系统。本申请实施例中，芯片系统可以由芯片构成，也可以包含芯片和其他分立器件。

在硬件实现上，上述收发模块 701 可以为收发器，收发器集成在通信装置 800 中构成通信接口 803。

通信装置 800 包括至少一个处理器 802，处理器 802 可以是一个 CPU，微处理器，ASIC，或一个或多个用于控制本申请方案程序执行的集成电路，用于实现或用于支持通信装置 800 实现本申请实施例提供的方法中 UDM 或 AUSF 实的功能。具体参见方法示例中的详细描述，此处不做赘述。

通信装置 800 还可以包括至少一个存储器 801，用于存储程序指令和/或数据。存储器 801 和处理器 802 耦合。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。处理器 802 可能和存储器 801 协同操作。处理器 802 可能执行存储器 801 中存储的程序指令和/或数据，以使得通信装置 800 实现相应的方法。所述至少一个存储器中的至少一个可以包括于处理器 802 中。

通信装置 800 还可以包括通信接口 803，使用任何收发器一类的装置，用于与其他设备或通信网络，如无线接入网（radio access network，RAN），无线局域网(wireless local area networks，WLAN)，有线接入网等通信。该通信接口 803 用于通过传输介质和其它设备进行通信，从而用于通信装置 800 中的装置可以和其它设备进行通信。示例性地，当该通信装置 800 为 UDM 时，该其它设备为 AUSF；或者，当该通信装置为 AUSF 时，该其它设备为 UDM。处理器 802 可以利用通信接口 803 收发数据。通信接口 803 具体可以是收发器。

本申请实施例中不限定上述通信接口 803、处理器 802 以及存储器 801 之间的具体连接介质。本申请实施例在图 8 中以存储器 801、处理器 802 以及通信接口 803 之间通过总线 804 连接，总线在图 8 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述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 8 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。

在本申请实施例中，处理器 802 可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列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、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

存储器 801 可以是 ROM 或可存储静态信息和指令的其他类型的静态存储设备，RAM 或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory, EEPROM）、只读光盘（compact disc read-only memory, CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 804 与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 801 用于存储执行本申请方案的计算机执行指令，并由处理器 802 来控制执行。处理器 802 用于执行存储器 801 中存储的计算机执行指令，从而实现本申请上述实施例提供的终端参数更新的保护方法。

可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

本申请实施例还提供一种通信装置，该通信装置可以是电路。该通信装置可以用于执行上述方法实施例中由 UDM 或第一 AUSF 所执行的动作。

本申请实施例还提供一种通信系统，具体的，通信系统包括 UDM 和 ASUF。示例性的，通信系统包括用于实现上述图 4、图 5、图 6 的相关功能的 UDM 和 ASUF。可选的，该通信系统还可以包括更多个 UDM 和/或 ASUF。

所述 UDM 用于实现上述图 4、图 5、图 6 相关 UDM 部分的功能。所述 ASUF 用于实现上述图 5、图 6、图 7 或图 8 相关 ASUF 部分的功能。具体请参考上述方法实施例中的相关描述，这里不再赘述。

本申请实施例中还提供一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行图 4、图 5、图 6 中 UDM 或 ASUF 执行的方法。

本申请实施例中还提供一种计算机程序产品，包括指令，当其在计算机上运行时，使得计算机执行图 4、图 5、图 6 中 UDM 或 ASUF 执行的方法。

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，还可以包括存储器，用于实现前述方法中 UDM 和 ASUF 的功能。该芯片系统可以由芯片构成，也可以包含芯片和其他分立器件。

本申请实施例提供的方法中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明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、网络设备、用户设备或者其他可编程装置。所述计算机指令可

以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，简称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可以存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，数字视频光盘（digital video disc，简称DVD））、或者半导体介质（例如，SSD）等。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权利要求书

1、一种终端参数更新的保护方法，其特征在于，包括：

统一数据管理 UDM 向第一认证服务功能 AUSF 发送保护请求消息，所述保护请求消息用于请求保护终端的参数更新信息；所述保护请求消息携带所述参数更新信息和第一服务网络信息；

所述 UDM 接收所述第一 AUSF 发送的所述保护请求消息的响应消息；

所述 UDM 通过所述第一服务网络对应的接入和移动性管理功能 AMF 发送所述参数更新信息。

2、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述 UDM 在向所述第一 AUSF 发送所述保护请求消息之前，所述 UDM 根据本地策略确定所述第一服务网络信息。

3、如权利要求 2 所述的方法，其特征在于，所述 UDM 在确定存在多个服务网络的情况下，确定进行终端的参数更新的所述第一服务网络。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述方法还包括：

所述 UDM 根据所述第一服务网络信息确定所述第一 AUSF。

5、如权利要求 1-4 任一所述的方法，其特征在于，所述方法还包括：

所述 UDM 在向所述第一 AUSF 发送保护请求消息之前，所述 UDM 确定：

所述第一 AUSF 有所述终端在多个服务网络的认证结果，所述多个服务网络包括所述第一服务网络；或者，

所述终端在多个服务网络，所述多个服务网络包括所述第一服务网络；或者，

所述终端处于双注册状态。

6、如权利要求 1-5 任一所述的方法，其特征在于，所述第一服务网络信息包括所述第一服务网络的名称；或者，

所述第一服务网络信息包括所述第一服务网络的公共陆地移动网络 PLMN 的标识 ID 或所述第一服务网络的 ID；或者，

所述第一服务网络信息包括所述终端的认证事件的标识。

7、如权利要求 1-6 任一所述的方法，其特征在于，所述参数更新信息包括漫游处理 SoR 信息。

8、一种终端参数更新的保护方法，其特征在于，包括：

第一认证服务功能 AUSF 接收统一数据管理 UDM 发送的保护请求消息，所述保护请求消息用于请求保护终端的参数更新信息，所述保护请求消息携带所述参数更新信息和第一服务网络信息；

所述第一 AUSF 根据所述第一服务网络信息确定第一密钥，所述第一密钥用于保护所述参数更新信息；

所述第一 AUSF 根据所述第一密钥对所述参数更新信息进行安全保护。

9、如权利要求 8 所述的方法，其特征在于，所述第一服务网络信息为所述 UDM 存储

的多个第一服务网络信息中的一个服务网络信息。

10、如权利要求 8 或 9 所述的方法，其特征在于，存在多个 AUSF，所述第一 AUSF 为与所述第一服务网络信息对应的 AUSF。

11、如权利要求 8 或 9 所述的方法，其特征在于，所述第一 AUSF 有所述终端在多个服务网络的认证结果，所述多个服务网络包括所述第一服务网络；或者，

所述终端在多个服务网络，所述多个服务网络包括所述第一服务网络；或者，
所述终端处于双注册状态。

12、如权利要求 8-11 任一所述的方法，其特征在于，所述第一服务网络信息包括所述第一服务网络的名称；或者，

所述第一服务网络信息包括所述第一服务网络的公共陆地移动网络 PLMN 标识；或者，
所述第一服务网络信息包括所述终端的认证事件的标识。

13、如权利要求 8-12 任一所述的方法，其特征在于，所述参数更新信息包括漫游处理 SoR 信息。

14、一种通信装置，其特征在于，包括处理模块和收发模块，其中：

所述收发模块，用于向第一认证服务功能 AUSF 发送保护请求消息，所述保护请求消息用于请求保护终端的参数更新信息；所述保护请求消息携带所述参数更新信息和第一服务网络信息；

所述收发模块，用于接收所述第一 AUSF 发送的所述保护请求消息的响应消息；

所述处理模块，用于控制所述收发模块通过所述第一服务网络对应的接入和移动性管理功能 AMF 发送所述参数更新信息。

15、如权利要求 14 所述的通信装置，其特征在于，所述收发模块还用于：

在向所述第一 AUSF 发送所述保护请求消息之前，根据本地策略确定所述第一服务网络信息。

16、如权利要求 15 所述的通信装置，其特征在于，所述处理模块具体用于：在确定存在多个服务网络的情况下，确定进行终端的参数更新的所述第一服务网络。

17、如权利要求 15 或 16 所述的通信装置，其特征在于，所述处理模块具体用于：

根据所述第一服务网络信息确定所述第一 AUSF。

18、如权利要求 14-17 任一所述的通信装置，其特征在于，所述处理模块具体用于在向所述第一 AUSF 发送保护请求消息之前，确定：

所述第一 AUSF 有所述终端在多个服务网络的认证结果，所述多个服务网络包括所述第一服务网络；或者，

所述终端在多个服务网络，所述多个服务网络包括所述第一服务网络；或者，
所述终端处于双注册状态。

19、如权利要求 14-18 任一所述的通信装置，其特征在于，所述第一服务网络信息包括所述第一服务网络的名称；或者，

所述第一服务网络信息包括所述第一服务网络的公共陆地移动网络 PLMN 的标识 ID 或所述第一服务网络的 ID；或者，

所述第一服务网络信息包括所述终端的认证事件的标识。

20、如权利要求 14-19 任一所述的通信装置，其特征在于，所述参数更新信息包括漫游处理 SoR 信息。

21、一种通信装置，其特征在于，包括处理模块和收发模块，其中：

所述收发模块，用于接收统一数据管理 UDM 发送的保护请求消息，所述保护请求消息用于请求保护终端的参数更新信息，所述保护请求消息携带所述参数更新信息和第一服务网络信息；

所述处理模块，用于根据所述第一服务网络信息确定第一密钥，所述第一密钥用于保护所述参数更新信息；

所述处理模块，用于根据所述第一密钥对所述参数更新信息进行安全保护。

22、如权利要求 21 所述的通信装置，其特征在于，所述第一服务网络信息为所述 UDM 存储的多个第一服务网络信息中的一个服务网络信息。

23、如权利要求 21 或 22 所述的通信装置，其特征在于，存在多个 AUSF，所述第一 AUSF 为与所述第一服务网络信息对应的 AUSF。

24、如权利要求 21 或 22 所述的通信装置，其特征在于，所述第一 AUSF 有所述终端在多个服务网络的认证结果，所述多个服务网络包括所述第一服务网络；或者，

所述终端在多个服务网络，所述多个服务网络包括所述第一服务网络；或者，
所述终端处于双注册状态。

25、如权利要求 21-24 任一所述的通信装置，其特征在于，所述第一服务网络信息包括所述第一服务网络的名称；或者，

所述第一服务网络信息包括所述第一服务网络的公共陆地移动网络 PLMN 标识；或者，
所述第一服务网络信息包括所述终端的认证事件的标识。

26、如权利要求 21-25 任一所述的通信装置，其特征在于，所述参数更新信息包括漫游处理 SoR 信息。

27、一种通信装置，其特征在于，所述通信装置包括处理器和存储器，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在所述存储器上的计算机程序，使得所述装置执行如权利要求 1~7 或 8~13 中任一项所述的通信方法。

28、一种通信系统，其特征在于，包括如权利要求 14~20 之一的通信装置，和如权利要求 21~26 之一的通信装置。

29、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序当被计算机执行时，使所述计算机执行如权利要求 1~7 或 8~13 中任意一项所述的方法。

30、一种计算机程序产品，其特征在于，所述计算机程序产品存储有计算机程序，所述计算机程序当被计算机执行时，使所述计算机执行如权利要求 1~7 或 8~13 中任意一项所述的方法。