

一种密钥推衍方法及其装置、系统

技术领域

本申请涉及通信技术领域，尤其涉及一种密钥推衍方法及其装置、系统。

背景技术

信息安全的重要性毋庸置疑。随着通信技术的不断发展，对信息的安全传递提出了更高的要求。通过密钥对信息进行加密是实现信息安全的重要手段。在通信系统中，用户设备（user equipment，UE）与网络相互认证后，UE可以与网络侧进行信息交互，为了确保信息的安全性，UE需要对待传输至网络侧的信息进行加密或完整性保护。例如，可以通过Kamf的衍生密钥对UE与接入与移动性管理功能（access and mobility management function，AMF）网元之间交互的信息进行加密或完整性保护。

Kamf可以由鉴权服务密钥Kausf推衍得到。为了实现UE与AMF网元之间的通信，UE与AMF网元各自生成的Kamf需要相同。因此，UE与网络侧各自生成的Kausf也需要相同。

在网络认证UE的过程中，可通过鉴权服务器功能（authentication server function，AUSF）网元作为认证设备对UE进行认证，或者，通过位于第三代合作伙伴计划（3rd generation partnership project，3GPP）网络外的认证凭证提供方（credentials provider、CdP）作为认证设备对UE进行认证。在AUSF网元作为认证设备的情况下，AUSF网元和UE均从扩展主会话密钥（extended master session key，EMSK）获得Kausf。在CdP作为认证设备的情况下，AUSF网元可根据来自CdP的密钥获得Kausf。因协议（RFC3748）规定EMSK不能被传输出CdP。因此，在CdP作为认证设备的情况下，用于获得Kausf的密钥不为EMSK。

这样，AUSF网元作为认证设备与CdP作为认证设备的情况下，用于获得Kausf的密钥不同。且现有技术中，UE无法感知网络侧采用AUSF网元还是CdP对UE进行认证。因此，UE也无法确定采用何种密钥获得Kausf。

发明内容

本申请实施例提供一种密钥推衍方法及其装置、系统，UE可以判断认证设备是否位于3GPP网络外，从而可以确定采用何种方式获得Kausf。

第一方面，本申请实施例提供一种密钥推衍方法，该方法包括：用户设备UE接收来自移动管理功能网元的认证成功消息；该认证成功消息用于指示该UE被认证设备成功认证；该UE根据该认证成功消息，生成主会话密钥MSK和扩展主会话密钥EMSK；并判断该认证设备是否位于第三代合作伙伴计划3GPP网络外；在该认证设备位于该3GPP网络外的情况下，该UE根据该MSK，生成鉴权服务密钥Kausf。

在该技术方案中，UE通过判断认证设备是否位于3GPP网络外，可以确定根据EMSK还是MSK获得Kausf，从而有利于使得UE与网络侧生成的Kausf相同，以确保UE与网络侧通信的顺利进行。

在一种实现方式中，该方法还包括：在认证设备位于3GPP网络内的情况下，该UE根据

EMSK, 生成Kausf。

在该技术方案中, 使得UE可以兼容认证设备位于3GPP网络外和认证设备位于3GPP网络内的网络架构。

在一种实现方式中, 该方法还包括: 该UE接收来自移动管理功能网元的第一指示信息, 该第一指示信息用于指示该认证设备位于该3GPP网络外或者该3GPP网络内; 该UE判断该认证设备是否位于3GPP网络外的具体实施方式可以为: 该UE根据该第一指示信息, 确定该认证设备是否位于3GPP网络外。

在该技术方案中, UE根据该第一指示信息即可确定采用EMSK还是MSK推衍Kausf。

在一种实现方式中, 该第一指示信息包括防止架构降级ABBA, 该ABBA的值为第一值的情况下, 该ABBA用于指示该认证设备位于该3GPP网络外; 该ABBA的值为第二值的情况下, 该ABBA用于指示该认证设备位于该3GPP网络内。例如, 第一值可以是非0值; 第二值可以为0。

在该技术方案中, 一方面, 通过采用现有信元ABBA作为第一指示信息, 可以减少对已有协议的改动。另一方面, 由于ABBA也是推衍Kamf的参数, 因此, 若ABBA被篡改, UE和移动管理功能网元生成的Kamf将不同, 这样可以发现攻击, 从而有利于提高通信的安全性。

在一种实现方式中, 该UE保存有第一配置信息, 该第一配置信息包括用于指示该认证设备是否位于该3GPP网络外的第二指示信息; 该UE判断该认证设备是否位于3GPP网络外的具体实施方式可以为: 该UE根据该第二指示信息, 确定该认证设备是否位于3GPP网络外。

在该技术方案中, UE根据预配置该UE中的第二指示信息判断认证设备是否位于3GPP网络外, 网络侧无需向UE发送指示信息(如移动管理功能网元无需向UE发送第一指示信息), 有利于减少网络侧设备的功耗。

在一种实现方式中, UE判断该认证设备是否位于3GPP网络外的具体实施方式可以为: 在UE获得该认证设备的标识的情况下, 该UE确定该认证设备位于3GPP网络外; 在该UE未获得该认证设备的标识的情况下, 该UE确定该认证设备位于3GPP网络内。

在一种实现方式中, UE根据MSK, 生成鉴权服务密钥Kausf的具体实施方式可以为: 该UE根据MSK和生成参数, 生成该Kausf; 其中, 该生成参数包括以下一项或多项: 该UE当前接入的服务网络的标识或该UE的标识。

在一种实现方式中, 该UE的标识包括该UE的第一标识, 该第一标识用于在该3GPP网络外的网络中标识该UE。

第二方面, 本申请实施例提供另一种密钥推衍方法, 该方法包括: 鉴权服务功能AUSF网元向认证设备发送第一触发指示, 该第一触发指示用于触发认证用户设备UE; 该AUSF网元接收来自该认证设备的认证成功消息和第一密钥; 该认证成功消息用于指示该UE被该认证设备成功认证; 该AUSF网元根据该第一密钥生成鉴权服务密钥Kausf; 并向移动管理功能网元发送该认证成功消息和第三指示信息, 该第三指示信息用于指示该认证设备位于第三代合作伙伴计划3GPP网络外或者该3GPP网络内。

在该技术方案中, AUSF网元通过向移动管理功能网元发送第三指示信息, 使得移动管理功能网元可以获知该认证设备是否位于3GPP网络外, 进而有利于移动管理功能网元告知

UE该认证设备是否位于3GPP网络外。或者，AUSF网元通过向移动管理功能网元发送第三指示信息，使得移动管理功能网元可以转发该第三指示信息至UE，以使UE获知该认证设备是否位于3GPP网络外。

在一种实现方式中，该AUSF网元根据该第一密钥生成鉴权服务密钥Kausf的具体实施方式可以为：该AUSF网元根据该第一密钥和生成参数，生成该Kausf；其中，该生成参数包括以下一项或多项：该UE当前接入的服务网络的标识或该UE的标识。

在一种实现方式中，该UE的标识包括该UE的第一标识，该第一标识用于在该3GPP网络外的网络中标识该UE。

在一种实现方式中，在AUSF网元向认证设备发送第一触发指示之前，该方法还包括：该AUSF网元确定该UE需要与该认证设备执行认证。

在一种实现方式中，AUSF网元确定UE需要与该认证设备执行认证的具体实施方式可以为：该AUSF网元接收来自该移动管理功能网元的该UE的第二标识；并根据该第二标识，确定该UE需要与该认证设备执行认证；第二标识为用户隐藏标识SUCI或用户永久标识SUPI。

在一种实现方式中，AUSF网元确定UE需要与该认证设备执行认证的具体实施方式可以为：该AUSF网元接收来自该移动管理功能网元的该UE的第二标识；该第二标识为用户隐藏标识SUCI或用户永久标识SUPI；该AUSF网元向统一数据管理UDM网元发送第一请求消息，该第一请求消息包括该SUCI或该SUPI；该AUSF网元接收来自该UDM网元的第一响应消息，该第一响应消息包括该认证设备的标识；该AUSF网元根据该认证设备的标识，确定该UE需要与该认证设备执行认证。

在一种实现方式中，该方法还包括：AUSF网元根据UE的第二标识，确定该UE的第一标识；该第一标识用于在该3GPP网络外的网络中标识该UE；该第二标识为SUCI或SUPI；该第二标识由该AUSF网元从该移动管理功能网元接收；该AUSF网元将该第一标识发送至该认证设备；前述第一触发指示具体用于触发根据该第一标识对应的认证凭证认证该UE。

在该技术方案中，可以避免将UE的第二标识（即SUCI或者SUPI）发给位于3GPP网络外的认证设备，即可以避免将UE的第二标识从3GPP网络内部传输到3GPP网络外部，从而避免了泄露用户的隐私。

第三方面，本申请实施例提供又一种密钥推衍方法，该方法包括：移动管理功能网元接收来自鉴权服务功能AUSF网元的认证成功消息和第三指示信息，该认证成功消息用于指示用户设备UE被认证设备成功认证；该第三指示信息用于指示该认证设备位于第三代合作伙伴计划3GPP网络外或者该3GPP网络内；该移动管理功能网元向该UE发送该认证成功消息和第一指示信息，该第一指示信息用于指示该认证设备位于该3GPP网络外或者该3GPP网络内；该第一指示信息根据该第三指示信息确定。

在该技术方案中，通过向UE发送该第一指示信息，使得UE可以根据该第一指示信息确定采用EMSK还是MSK推衍Kausf。

在一种实现方式中，该第一指示信息包括防止架构降级ABBA，该方法还包括：该移动管理功能网元将该ABBA的值确定为非零值；该ABBA的值为非零值的情况下，该ABBA用于指示该认证设备位于该3GPP网络外。

在该技术方案中，一方面，通过采用现有信元ABBA作为第一指示信息，可以减少对已有协议的改动。另一方面，由于ABBA也是推衍Kamf的参数，因此，若ABBA被篡改，UE和移动管理功能网元生成的Kamf将不同，这样可以发现攻击，从而有利于提高通信的安全性。

第四方面，本申请实施例提供又一种密钥推衍方法，该方法包括：协议转化网元接收来自鉴权服务功能AUSF网元的第二触发指示，该第二触发指示用于触发认证用户设备UE；该协议转化网元向认证设备发送第三触发指示，该第三触发指示用于触发认证该UE；该第三触发指示根据该第二触发指示得到；该协议转化网元接收来自该认证设备的认证成功消息和第一密钥；该认证成功消息用于指示该UE被该认证设备成功认证；该协议转化网元根据该第一密钥生成鉴权服务密钥Kausf；该协议转化网元向该AUSF网元发送该认证成功消息。

在一种实现方式中，该协议转化网元根据该第一密钥生成鉴权服务密钥Kausf的具体实施方式可以为：该协议转化网元根据该第一密钥和生成参数生成Kausf；其中，该生成参数包括以下一项或多项：服务网络的标识或该UE的标识。

在一种实现方式中，该UE的标识包括该UE的第一标识，该第一标识用于在第三代合作伙伴计划3GPP网络外的网络中标识该UE。

在一种实现方式中，该方法还包括：该协议转化网元将该UE的第一标识发送至该认证设备；该第三触发指示具体用于触发根据该第一标识对应的认证凭证认证该UE。

在该技术方案中，可以避免将UE的第二标识（即SUCI或者SUPI）发给位于3GPP网络外的认证设备，即可以避免将UE的第二标识从3GPP网络内部传输到3GPP网络外部，从而避免了泄露用户的隐私。

第五方面，本申请实施例提供了一种通信装置，该通信装置具有实现上述第一方面所述的方法示例中UE的部分或全部功能，比如通信装置的功能可具备本申请中的部分或全部实施例中的功能，也可以具备单独实施本申请中的任一个实施例的功能。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单元或模块。

在一种实现方式中，该通信装置的结构中可包括收发模块和处理模块。该处理模块被配置为支持通信装置执行上述方法中相应的功能。收发模块用于支持通信装置与其他设备之间的通信。该通信装置还可以包括存储模块，该存储模块用于与处理模块和收发模块耦合，其保存通信装置必要的计算机程序和数据。

在一种实现方式中，该通信装置包括：收发模块，用于接收来自移动管理功能网元的认证成功消息；该认证成功消息用于指示UE被认证设备成功认证；处理模块，用于根据该认证成功消息，生成MSK和EMSK；判断认证设备是否位于3GPP网络外；在认证设备位于3GPP网络外的情况下，根据MSK，生成Kausf。

作为示例，处理模块可以为处理器，收发模块可以为收发器，存储模块可以为存储器。

在一种实现方式中，所述通信装置包括：收发器，用于接收来自移动管理功能网元的认证成功消息；该认证成功消息用于指示UE被认证设备成功认证；处理器，用于根据该认证成功消息，生成MSK和EMSK；判断认证设备是否位于3GPP网络外；在认证设备位于3GPP

网络外的情况下，根据MSK，生成Kausf。

第六方面，本申请实施例提供了另一种通信装置，该通信装置具有实现上述第二方面所述的方法示例中AUSF网元的部分或全部功能，比如通信装置的功能可具备本申请中的部分或全部实施例中的功能，也可以具备单独实施本申请中的任一个实施例的功能。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单元或模块。

在一种实现方式中，该通信装置的结构中可包括处理模块和收发模块。该处理模块被配置为支持通信装置执行上述方法中相应的功能。收发模块用于支持通信装置与其他设备之间的通信。该通信装置还可以包括存储模块，该存储模块用于与处理模块和收发模块耦合，其保存通信装置必要的计算机程序和数据。

在一种实现方式中，该通信装置包括：收发模块，用于向认证设备发送第一触发指示，该第一触发指示用于触发认证UE；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证；处理模块，用于根据所述第一密钥生成Kausf；收发模块，还用于向移动管理功能网元发送认证成功消息和第三指示信息，第三指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内。

作为示例，处理模块可以为处理器，收发模块可以为收发器，存储模块可以为存储器。

在一种实现方式中，所述通信装置包括：收发器，用于向认证设备发送第一触发指示，该第一触发指示用于触发认证UE；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证；处理器，用于根据所述第一密钥生成Kausf；收发器，还用于向移动管理功能网元发送认证成功消息和第三指示信息，第三指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内。

第七方面，本申请实施例提供了又一种通信装置，该通信装置具有实现上述第三方面所述的方法示例中移动管理功能网元的部分或全部功能，比如通信装置的功能可具备本申请中的部分或全部实施例中的功能，也可以具备单独实施本申请中的任一个实施例的功能。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单元或模块。

在一种实现方式中，该通信装置的结构中可包括处理模块和收发模块。该处理模块被配置为支持通信装置执行上述方法中相应的功能。收发模块用于支持通信装置与其他设备之间的通信。该通信装置还可以包括存储模块，该存储模块用于与处理模块和收发模块耦合，其保存通信装置必要的计算机程序和数据。

在一种实现方式中，该通信装置包括：收发模块，用于接收来自AUSF网元的认证成功消息和第二指示信息，认证成功消息用于指示UE被认证设备成功认证；第二指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内；向所述UE发送认证成功消息和第一指示信息，第一指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内；第二指示信息根据第一指示信息确定。

作为示例，处理模块可以为处理器，收发模块可以为收发器，存储模块可以为存储器。

在一种实现方式中，所述通信装置包括：收发器，用于接收来自AUSF网元的认证成功消息和第二指示信息，认证成功消息用于指示UE被认证设备成功认证；第二指示信息用于

指示认证设备位于3GPP网络外或者3GPP网络内；向所述UE发送认证成功消息和第一指示信息，第一指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内；第二指示信息根据第一指示信息确定。

第八方面，本申请实施例提供了又一种通信装置，该通信装置具有实现上述第三方面所述的方法示例中协议转化功能网元的部分或全部功能，比如通信装置的功能可具备本申请中的部分或全部实施例中的功能，也可以具备单独实施本申请中的任一个实施例的功能。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单元或模块。

在一种实现方式中，该通信装置的结构中可包括处理模块和收发模块。该处理模块被配置为支持通信装置执行上述方法中相应的功能。收发模块用于支持通信装置与其他设备之间的通信。该通信装置还可以包括存储模块，该存储模块用于与处理模块和收发模块耦合，其保存通信装置必要的计算机程序和数据。

在一种实现方式中，该通信装置包括：收发模块，用于接收来自AUSF网元的第二触发指示，该第二触发指示用于触发认证UE；向认证设备发送第三触发指示，该第三触发指示用于触发认证UE；该第三触发指示根据第二触发指示得到；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证。

作为示例，处理模块可以为处理器，收发模块可以为收发器，存储模块可以为存储器。

在一种实现方式中，所述通信装置包括：收发器，用于接收来自AUSF网元的第二触发指示，该第二触发指示用于触发认证UE；向认证设备发送第三触发指示，该第三触发指示用于触发认证UE；该第三触发指示根据第二触发指示得到；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证。

第九方面，本申请实施例提供一种密钥推衍系统，该系统包括如第五方面至第八方面的一个或多个通信装置。

第十方面，本发明实施例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，所述计算机程序包括程序指令，所述程序指令被通信装置执行时使该通信装置执行上述第一方面的方法。

第十一方面，本发明实施例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，所述计算机程序包括程序指令，所述程序指令被通信装置执行时使该通信装置执行上述第二方面的方法。

第十二方面，本发明实施例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，所述计算机程序包括程序指令，所述程序指令被通信装置执行时使该通信装置执行上述第三方面的方法。

第十三方面，本发明实施例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，所述计算机程序包括程序指令，所述程序指令被通信装置执行时使该通信装置执行上述第四方面的方法。

第十四方面，本申请还提供了一种包括计算机程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

第十五方面，本申请还提供了一种包括计算机程序的计算机程序产品，当其在计算机

上运行时，使得计算机执行上述第二方面所述的方法。

第十六方面，本申请还提供了一种包括计算机程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第三方面所述的方法。

第十七方面，本申请还提供了一种包括计算机程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第四方面所述的方法。

附图说明

- 图 1a 是 5G 系统的网络架构的示意图；
- 图 1b 是现有的推衍 Kamf 的流程示意图；
- 图 1c 是本申请实施例适用的网络架构的示意图；
- 图 2 是本申请实施例提供的一种密钥推衍方法的流程示意图；
- 图 3 是本申请实施例提供的另一种密钥推衍方法的流程示意图；
- 图 4 是本申请实施例提供的又一种密钥推衍方法的流程示意图；
- 图 5 是本申请实施例提供的又一种密钥推衍方法的流程示意图；
- 图 6 为本申请实施例提供的一种通信装置的结构示意图；
- 图 7 为本申请实施例提供的另一种通信装置的结构示意图。

具体实施方式

为了更好地理解本申请实施例提供的技术方案，首先对本申请实施例涉及的技术术语进行介绍。

1、第五代通信（5th generation，5G）系统的网络架构

请参见图 1a，为 5G 系统的网络架构的示意图，该网络架构包括用户设备（user equipment，UE）、接入网（access network，AN）设备、核心网网元、数据网络（data network，DN）、协议转化网元和认证凭证提供方（credentials provider、CdP）。

其中，接入网设备也可以是无线接入网（radio access network，RAN）设备。接入网设备可以包括基站（base station，BS），可以是一种部署在无线接入网络中能够与终端设备进行无线通信的设备。其中，基站可能有多种形式，比如宏基站、微基站、中继站和接入点等。示例性地，本申请实施例涉及到的接入网设备可以是 5G 中的基站或长期演进（long term evolution，LTE）中的基站，其中，5G 中的基站还可以称为发送接收点（transmission reception point，TRP）或下一代基站节点（next generation Node B，gNB）。

其中，核心网网元可以包括：接入和移动性管理功能（access and mobility management function，AMF）、鉴权服务器功能（authentication server function，AUSF）、统一数据管理（unified data management，UDM）、会话管理功能（session management function，SMF）、策略控制功能（policy control function，PCF）、应用功能（application，AF）、用户面功能（user plane function，UPF）和网络切片选择功能（network slice selection function，NSSF）。

AMF 网元，非接入层（non-access stratum，NAS）信令的终结点，主要负责用户的接入认证和移动性管理。UE 与 AMF 可以通过 N1 NAS 消息进行通信，UE 与 AMF 之间的通信消息也可以通过 RAN 的 N2 消息进行中转。RAN 与 AMF 通过 N2 消息进行通信。

安全锚点功能 (security anchor function , SEAF) 网元 (图 1a 未示) , 具有认证 UE 的功能。可选的, AMF 网元可以具有 SEAF 网元的功能, 在此情况下, AMF 网元和 SEAF 网元可以合并设置于一个实体。

AUSF 网元: 具有鉴权服务功能, 用于处理第三代合作伙伴计划 (3rd generation partnership project , 3GPP) 接入和非 3GPP 接入的认证请求。

UDM 网元: 用于管理用户的签约信息, 完成用户认证与授权。

SMF 网元, 负责会话管理, 如用户的会话建立、删除, 维护协议数据单元 (protocol data unit , PDU) 会话上下文及用户面转发管道信息等。

PCF 网元, 用于生成、管理用户、会话、服务质量 (quality of service , QoS) 流处理策略。

AF 网元, 提供应用服务, 可以位于运营商网络内, 也可以位于运营商网络外。

UPF 网元, 用于对用户报文进行处理, 例如转发、计费等。

NSSF 网元, 用于支持基于用户请求的和签约的网络切片选择辅助信息 (network slice selection assistance information , NSSAI)、用户位置区域、切片容量、切片当前负荷等信息, 进行切片的灵活选择。

CdP: 存储有 UE 的第二认证凭证, 可提供对 UE 进行认证的服务。

UE 的认证凭证可以包括第一认证凭证、第二认证凭证, 其中, UE 的第一认证凭证是 UE 预配置于 UE 的认证凭证。UE 的第二认证凭证是预配置于认证设备中的认证凭证。

认证、授权和计费 (authentication、authorization、accounting , AAA) 服务器 (图 1a 未示) : 能够处理用户访问请求的服务器程序, 提供验证授权以及帐户服务, 主要目的是管理用户访问网络服务器, 对具有访问权的用户提供服务。

默认凭证服务器 (default credential server , DCS) (图 1a 未示) : 存储有 UE 的默认认证凭证 (即第一认证凭证) , 可提供对 UE 的认证服务。其中, 默认认证凭证是 UE 在出厂时预配置在 UE 上的认证凭证。

协议转化网元: 用于对 3GPP 内部网元与 3GPP 外部网元的交互进行协议转化。例如, 对于 AUSF 网元, 协议转化网元可以提供服务化接口 (service-based interface , SBI) 协议到 AAA 协议的底层协议转化; 对于 AAA 服务器, 协议转化网元可以提供 AAA 协议到 SBI 协议的底层协议转化。应用于本申请实施例中, 协议转化网元可以为 AAA 代理 (AAA-proxy , AAA-P)、AAA 互操作功能 (AAA-interworking function , AAA-IWF) 或首次认证功能 (primary authentication function , PAF)。可选的, AUSF 网元也可以具有上述协议转化网元所提供的功能, 即 AUSF 网元和协议转化网元可以合并为一个网元。在此情况下, 图 1a 所示网络架构中可以不包括协议转化网元。需要说明的是, 协议转化网元的名称用于举例, 并不构成对本申请实施例的限定, 例如协议转化网元还可以称为认证协议转化功能网元。

DN, 负责为 UE 提供服务, 包含运营商服务, 互联网服务, 第三方服务等, 如为 UE 提供上网功能、短信功能等。

图 1a 所示的网络架构示意图中, 还包括各个网元之间的接口, 例如 N2 表示 AMF 网元与 RAN 设备之间的接口。

2、非公共网络 (non-public network , NPN)

非公共网络(non-public network ,NPN)用于非公共目的建立的 3GPP 网络 ,例如工厂、学校、商业区搭建的内部网络。NPN 可以分为两种类型：独立的 NPN (standalone NPN , SNPN) 和公网集成的 NPN (public network integrated NPN , PNI-NPN)。其中, SNPN 不依赖于公网的功能, 而 PNI-NPN 需要依赖于公网的功能。

3、推衍 Kamf 的流程

请参见图 1b, 为 AUSF 网元作为认证设备时, 现有的推衍 Kamf 的流程示意图。该流程可以包括但不限于步骤 S101~步骤 S113。

步骤 S101: UE 向 AMF 网元发送注册请求, 以请求注册到网络。该注册请求包括该 UE 的用户隐藏标识 (subscription concealed identifier , SUCI)。

步骤 S102 :AMF 网元接收到该注册请求后 ,向 AUSF 网元发送认证请求 ,以请求 AUSF 网元对该 UE 进行认证。该认证请求包括 SUCI 以及服务网络的标识, SUCI 可以包括公共陆地移动网标识 (public land mobile network identity , PLMN ID) 和路由标识 (routing ID , RID)。SUCI 中包括的公共陆地移动网标识指示该 UE 的归属地网络, 服务网络指当前该 UE 的接入的网络, 如漫游地网络。

步骤 S103: AUSF 网元接收到该认证请求后, 根据该 SUCI 的 PLMN ID 和 routing ID 确定 UDM 网元。然后 ,请求该 UDM 网元从 SUCI 解析出该 UE 的用户永久标识(subscription permanent identifier , SUPI)。该 UDM 网元通知 AUSF 网元该 UE 的 SUPI 以及使用的认证方法 (如可扩展认证协议 (extensible authentication protocol , EAP) -传输层安全性协议 (transport layer security , TLS))。

步骤 S104: AUSF 网元根据该 SUPI 获得认证凭证。

例如, AUSF 网元本地存储有该 SUPI 对应的认证凭证, AUSF 根据该 SUPI 获得认证凭证。需要说明的是, 该认证凭证是预配置在 AUSF 网元中, 用于对 UE 进行认证的认证凭证。该认证凭证为该 UE 的第二认证凭证。

步骤 S105: AUSF 网元获得认证凭证后发起 EAP 的认证流程 (如 EAP-TLS 认证) , 认证完成后, UE 与 AUSF 网元都生成了主会话密钥 (master session key , MSK) 和扩展主会话密钥 (extended master session key , EMSK)。

需要说明的是, 认证流程包括 UE 认证网络和网络认证 UE 这两个子流程。可以先进行 UE 认证网络的流程, 再进行网络认证 UE 的流程。因此, UE 被网络成功认证后, 认证流程结束。在图 1b 中, 网络认证 UE 具体通过 AUSF 网元来认证 UE。

还需要说明的是, UE 和 AUSF 网元也可以在认证过程中生成 MSK 和 EMSK。例如, AUSF 网元可以在认证 UE 后, UE 认证 AUSF 网元前, 生成 MSK 和 EMSK。

UE 生成 MSK 和 EMSK 的方式为: 根据上述第一认证凭证生成 MSK 和 EMSK。认证设备生成 MSK 和 EMSK 的方式为: 根据上述第二认证凭证生成 MSK 和 EMSK。需要说明的是, UE 的第一认证凭证与第二认证凭证可以相同, 例如对称密钥。UE 的第一认证凭证与第二认证凭证也可以不同, 例如非对称密钥、证书等。当 UE 的第一认证凭证和第二认证凭证相同时, UE 与认证设备各自生成的 MSK 和 EMSK 均相同。当 UE 的第一认证凭证和第二认证凭证不同时, UE 根据该第一认证凭证生成 MSK 和 EMSK 的方式, 与认证设备根据第二认证凭证生成 MSK 和 EMSK 的方式不同, 以使能两者生成的 MSK 和 EMSK 均

相同，例如使用迪菲-赫尔曼（Diffie-Hellman，DH）密钥交换等方式。

步骤 S106：AUSF 网元从 EMSK 的最高 256 个比特位的值得到第一中间密钥（即鉴权服务密钥 Kausf）。

步骤 S107：AUSF 网元根据该 Kausf 以及服务网络的标识生成第二中间密钥（即安全锚点密钥 Kseaf）。

步骤 S108：AUSF 网元向 AMF 网元发送 EAP 成功消息、该 Kseaf 和 SUPI。该 EAP 成功消息用于指示该 UE 被该 AUSF 网元成功认证。

步骤 S109：AMF 网元接收到 EAP 成功消息、Kseaf 和 SUPI 后，根据该 Kseaf、防止架构降级（anti-bidding down between architectures，ABBA）和 SUPI 生成 Kamf。

步骤 S110：AMF 网元向 UE 发送 EAP success 消息、ABBA 和 SUPI。

步骤 S111：UE 接收到 EAP success 消息，获知 UE 被成功认证，从 EMSK 的最高 256 个比特位的值得到 Kausf。

步骤 S112：UE 根据该 Kausf 以及服务网络的标识生成 Kseaf。

步骤 S113：UE 根据该 Kseaf、ABBA 和 SUPI 生成 Kamf。

经过上述流程，AMF 网元和 UE 均生成了 Kamf。因此，后续 UE 与 AMF 网元可以使用 Kamf 推导的密钥或者 Kamf 进行通信的保护。为了实现 AMF 网元与 UE 之间的通信，AMF 网元和 UE 各自生成的 Kamf 需要相同。因此，AMF 网元和 UE 各自生成的 Kausf 也需要相同。

4、认证设备位于 3GPP 网络外；认证设备位于 3GPP 网络内

认证设备，存储有 UE 的认证凭证，认证设备用于对接入的 UE 进行认证。应用于本申请实施例，认证设备可以是 AAA 服务器、图 1a 中的 CdP、默认凭证服务器（default credential server，DCS）或图 1a 中的 AUSF 网元，或者其他具有对 UE 进行认证的功能的设备。认证设备可以位于 3GPP 网络内，也可以位于 3GPP 网络外。

UE 被认证设备成功认证后，该 UE 才能与 3GPP 网络内的网元（如 AMF）进行通信。为确保通信的安全性，在通信过程中需要通过密钥对通信信息进行加密。UE 被认证设备成功认证后，认证流程结束，UE 和认证设备两者均会生成 MSK 和 EMSK 这两个密钥。

3GPP 网络，可以指 3GPP 协议定义的网络，如移动通信网络、公共陆地移动网（public land mobile network，PLMN）、非公共网络（non-public network，NPN）等包含接入网、核心网和 UE 的网络，可以是 5G 网络或者未来演进的移动通信网络。其中，PLMN 是由政府或它所批准的经营者，为公众提供陆地移动通信业务目的而建立和经营的网络。

认证设备位于 3GPP 网络内，表示 3GPP 网络内部的网元对 UE 进行认证。换言之，认证 UE 的认证凭证保存在 3GPP 网络内部的网元中。认证设备位于 3GPP 网络内的情况下，该认证设备具体可以为图 1a 中的 AUSF 网元。结合上述可知，在此情况下，UE 被 AUSF 网元（即认证设备）基于 EAP 方法成功认证后，UE 和 AUSF 网元两者均会生成 MSK 和 EMSK。认证设备位于 3GPP 网络内，例如 3GPP 网络内的 AUSF 网元作为认证设备对 UE 进行认证的情况下，AUSF 网元和 UE 获得 Kausf 的方式为：从 EMSK 获得 Kausf。

认证设备位于 3GPP 网络外，表示 3GPP 网络外部的实体对 UE 进行认证。换言之，认证 UE 的认证凭证保存在 3GPP 网络外部的实体中。该实体可以为 3GPP 网络的网元以外的

实体，3GPP 网络内部的网元信任该实体对 UE 的认证结果。认证设备位于 3GPP 网络外的情况下，该认证设备具体可以为 DCS、AAA 服务器或图 1a 中的 CdP。结合上述可知，在此情况下，UE 被（位于 3GPP 网络外的）认证设备基于 EAP 方法成功认证后，UE 和该认证设备两者均会生成 MSK 和 EMSK。认证设备位于 3GPP 网络外，例如 3GPP 网络外的 CdP 作为认证设备对 UE 进行认证的情况下，AUSF 网元和 UE 获得 Kausf 的方式为：根据来自 CdP 的密钥获得 Kausf。

但是，现有协议（RFC3748）规定，CdP 和 AAA 服务器均无法将 EMSK 或 EMSK 的最高 256 个比特位的值传输给其他网元。因此，在 CdP 作为认证设备的情况下，用于获得 Kausf 的密钥不为 EMSK。这样，AUSF 网元作为认证设备与 CdP 作为认证设备（即认证设备位于 3GPP 网络内与认证设备位于 3GPP 网络外）的情况下，用于获得 Kausf 的密钥不同。且现有技术中，UE 无法感知网络侧采用 AUSF 网元还是 CdP 对 UE 进行认证。因此，UE 也无法确定采用何种密钥获得 Kausf。

5、推衍方式 1；推衍方式 2；第一密钥

为了适应认证设备位于不同位置的情况，本申请实施例提供了两种推衍方式用于获得 Kausf。其中，推衍方式 1 是为适应认证设备位于 3GPP 网络内，所采用的推衍方式。推衍方式 2 是为适应认证设备位于 3GPP 网络外，所采用的推衍方式。

推衍方式 1 为：从 EMSK 获得 Kausf。例如，将 EMSK 的部分比特位（如最高 256 比特位）的值作为 Kausf。

推衍方式 2 为：从 MSK 获得 Kausf。例如，将 MSK 的部分比特位（如最高 256 比特位）的值作为 Kausf。可选的，推衍方式 2 具体可以为：从 MSK 获得第一密钥，然后从该第一密钥获得 Kausf。例如，将第一密钥的部分比特位（如最高 256 比特位）的值作为 Kausf。其中，该第一密钥可以为该 MSK，也可以为 MSK 的部分比特位。或者，该第一密钥可以从该 MSK 推衍得到，即第一密钥是对该 MSK 进行运算或处理等操作得到的。本申请对第一密钥的名称不做限定，例如，第一密钥还可以称为 AAA-key。

需要说明的是，UE 侧（即 UE）与网络侧采用的推衍方式需要相同，或者说，UE 侧与网络侧需要采用相同的密钥推衍 Kausf，才能确保 UE 侧与网络侧生成的 Kausf 相同。其中，网络侧可以包括多个网元，例如网络侧可以包括但不限于 AUSF 网元、协议转化网元和位于 3G 网络外的网元中的一个或多个网元。“网络侧采用的推衍方式”可以指：通过网络侧的一个或多个网元参与推衍过程，进而得到 Kausf。

例如，认证设备位于 3GPP 网络外的情况下，在网络侧，生成 EMSK 和 MSK 的设备为位于 3GPP 网络外的认证设备，获得 Kausf 的设备为 AUSF 网元。该认证设备可以向 AUSF 网元提供第一密钥，AUSF 网元进而从该第一密钥获得 Kausf。

上述举例为网络侧通过（位于 3GPP 网络外的）认证设备和 AUSF 网元参与推衍过程，得到 Kausf 的情况。由于该第一密钥从 MSK 获得，因此，对网络侧而言，推衍 Kausf 的方式实际上为上述推衍方式 2。

上述可知，推衍方式不同，用于生成 Kausf 的密钥不同。推衍方式 1，与用于生成 Kausf 的密钥为 EMSK 相对应。推衍方式 2，与用于生成 Kausf 的密钥为 MSK（或第一密钥）相对应。需要说明的是，在本申请实施例中，对于 UE 而言，若确定采用推衍方式 2，即表示

该 UE 从 MSK 获得 Kausf。对于网络侧中用于获得 Kausf 的网元（如 AUSF 网元或者协议转化网元）而言，若确定采用推衍方式 2，即表示该网元从（认证设备提供的）第一密钥获得 Kausf。

请参见图 1c，为本申请实施例适用的网络架构的示意图。图 1c 包括 UE101、移动管理功能网元 102、AUSF 网元 103 和认证设备 104。

其中，本申请实施例涉及的 UE101，可以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、气球和人造卫星上等）。UE 包括具有无线通信功能的手持式设备、车载设备、穿戴式设备或计算设备。示例性地，UE 可以是手机（mobile phone）、平板电脑或带无线收发功能的电脑。终端设备还可以是虚拟现实（virtual reality，VR）终端设备、增强现实（augmented reality，AR）终端设备、智能汽车（smart vehicle）终端设备、工业控制中的无线终端、无人驾驶中的无线终端、无人机、无人机控制器、远程医疗中的无线终端、智能电网中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端、等等。本申请的实施例对 UE 所采用的具体技术和具体设备形态不做限定。

其中，移动管理功能网元 102 可以是图 1a 中的 AMF 网元，也可以是安全锚点功能（security anchor function，SEAF）网元。

AUSF 网元 103，可以用于为移动管理功能网元 102 提供 UE 认证服务。

认证设备网元 104，用于对 UE 进行认证。认证设备 104 可以为 AUSF 网元、AAA 服务器、DCS 或图 1a 中的 CdP。在一种实现方式中，AUSF 网元 103 可以自行对 UE 进行认证，此时，AUSF 网元 103 与认证设备 104 合并设置与一个实体中。在另一种实现方式中，AUSF 网元可以触发位于 3GPP 网络外的认证设备 104 对 UE 进行认证。

可选的，图 1c 所示的网络架构还可以包括协议转化网元 105，用于为实现 AUSF 网元 103 与（处于 3GPP 网络外的）认证设备 104 之间的通信提供协议转化功能。

需要说明的是，移动管理功能网元 102、认证设备 104 和协议转化网元 105 的名称用于举例，并不构成对本申请实施例的限定。

在本申请中，AUSF 网元 103 向位于 3GPP 网络外的认证设备 104 发送第一触发指示，该第一触发指示用于触发认证 UE101；认证设备 104 接收到第一触发指示后，对 UE101 进行认证。认证设备 104 成功认证 UE101 后，生成 MSK 和 EMSK，并从 MSK 获得第一密钥，然后向 AUSF 网元 103 发送认证成功消息和第一密钥，该认证成功消息用于指示 UE101 被认证设备 104 成功认证。

AUSF 网元 103 接收到认证成功消息和第一密钥后，根据该第一密钥生成 Kausf，并向通过移动管理功能网元 102 向 UE101 发送该认证成功消息（即认证成功消息经由移动管理功能网元 102 传输至 UE101）。相应的，UE101 根据认证成功消息，生成 MSK 以及 EMSK；并判断认证设备 104 是否位于 3GPP 网络外；在认证设备 104 位于该 3GPP 网络外的情况下，根据该 MSK 生成 Kausf（即采用推衍方式 2 获得 Kausf）。

UE101 通过判断认证设备 104 是否位于 3GPP 网络外，可以确定认证设备 104 位于 3GPP 网络外的情况下，采用 MSK 生成 Kausf。另外，在网络侧，AUSF 网元用于生成 Kausf 的

第一密钥是由认证设备 104 从 MSK 获得的。UE101 与网络侧均采用 MSK 生成 Kausf，因此，UE101 与网络侧生成的 Kausf 相同，从而有利于确保通信的安全性。

在本申请实施例中，UE101 可以通过如下三种方式判断认证设备 104 是否位于 3GPP 网络外：

判断方式一，UE101 根据来自网络侧的第一指示信息确定认证设备 104 是否位于 3GPP 网络外。具体过程如下：

在上述过程中，AUSF 网元 103 除了向移动管理功能网元 102 发送认证成功消息以外，还向其发送第三指示信息，该第三指示信息用于指示认证设备 104 位于 3GPP 网络外或者位于该 3GPP 网络内。移动管理功能网元 102 可以根据接收到的第三指示信息得到第一指示信息，并向 UE101 发送该第一指示信息以及前述认证成功消息，该第一指示信息用于指示认证设备 104 位于 3GPP 网络外或者位于该 3GPP 网络内。相应的，UE101 接收到该第一指示信息，即可判断认证设备 104 是否位于 3GPP 网络外。关于判断方式一的具体描述可以详见图 4 实施例中的描述。

判断方式二，UE101 根据第一配置信息中的第二指示信息确定认证设备 104 是否位于 3GPP 网络外，该第二指示信息用于指示认证设备 104 是否位于 3GPP 网络外。该第一配置信息可以预配置于该 UE 中。关于判断方式二的具体描述可以详见图 5 实施例中的描述。

判断方式三，UE101 根据认证设备的标识判断认证设备 104 是否位于 3GPP 网络外。例如，若 UE 获得认证设备的标识，则 UE 确定认证设备 104 位于 3GPP 网络外。关于判断方式三的具体描述可以详见图 5 实施例中的描述。

需要说明的是，UE101 通过判断认证设备 104 是否位于 3GPP 网络外，目的在于使得 UE101 与网络侧采用相同推衍方式（即推衍方式 1 或推衍方式 2）生成 Kausf，以使得 UE 与网络侧生成的 Kausf 相同。

需要说明的是，在本申请实施例中提及的“认证设备是否位于 3GPP 网络外”用于举例，在具体实现中，可以使得网络侧（如 AUSF 网元、协议转化网元、位于 3GPP 网络外的认证设备）与 UE 采用相同推衍方式生成 Kausf 的方式均在本申请保护范围内。例如，“认证设备是否位于 3GPP 网络外”可以描述为“是否采用 MSK 推衍 Kausf”、“是否采用第一密钥推衍 Kausf”、“是否采用 EMSK 推衍 Kausf”、“是否采用推衍方式 1 推衍 Kausf”、“是否采用推衍方式 2 推衍 Kausf”。可以理解的是，若确定不采用第一密钥或 MSK 推衍 Kausf，则表示可以采用 EMSK 推衍 Kausf。同理，若确定不采用 EMSK 推衍 Kausf，则表示可以采用第一密钥或者 MSK 推衍 Kausf。

“认证设备是否位于 3GPP 网络外”还可以描述为“用于推衍 Kausf 的密钥是否从外部网络获得”、“用于推衍 Kausf 的密钥是否从内部网络获得”、“用于推衍 Kausf 的密钥是否从 3GPP 网络外获得”、“用于推衍 Kausf 的密钥是否从 3GPP 网络内获得”、“用于推衍 Kausf 的密钥是否从内部网络中的网元获得”、“用于推衍 Kausf 的密钥是否从外部网络中的网元获得”、“用于推衍 Kausf 的密钥是否从 3GPP 网络内的网元获得”、“用于推衍 Kausf 的密钥是否从 3GPP 网络外的网元获得”。其中，“用于推衍 Kausf 的密钥”可以指第一密钥、MSK 或者 EMSK。若确定用于推衍 Kausf 的密钥是从外部网络获得的，那么“用于推衍 Kausf 的密钥”指第一密钥或 MSK。若确定用于推衍 Kausf 的密钥不是从外部网络获得的，那么“用

于推衍 Kausf 的密钥”指 EMSK。

“认证设备是否位于 3GPP 网络外”还可以描述为“正在执行认证凭证位于独立于 SNPN 的第三方的认证”、“正在执行外部认证”、“正在执行 3GPP 外部认证”、“认证凭证位于独立于 SNPN 的第三方的认证已完成”、“外部认证已完成”、“3GPP 外部认证已完成”、“即将执行认证凭证位于独立于 SNPN 的第三方的认证”、“即将执行外部认证”、“即将执行 3GPP 外部认证”等。可以理解的是，若确定正在执行外部认证，则表示可以采用第一密钥或 MSK 推衍 Kausf。若无法确定正在执行外部认证，或者确定正在执行内部认证（即由内部网络中的网元对 UE 进行认证），则表示可以采用 EMSK 推衍 Kausf。

需要说明的是，本申请实施例中提及的“内部网络”与“外部网络”与相对应的概念。“内部网络”可以指由 3GPP 定义的网络，可以理解的是，“外部网络”可以理解为“内部网络”以外的网络。本申请实施例中提及的“内部认证”与“外部认证”与相对应的概念。“内部认证”可以指由 3GPP 定义的网络中的网元对 UE 进行认证，可以理解的是，“外部认证”可以理解由 3GPP 定义的网络以外的网络，中的网元对 UE 进行认证。

本申请实施例描述的技术可用于各种通信系统，例如第四代（4th generation，4G）通信系统，4.5G 通信系统，5G 通信系统，多种通信系统融合的系统，或者未来演进的通信系统。

可以理解的是，本申请实施例描述的通信系统是为了更加清楚的说明本申请实施例的技术方案，并不构成对本申请实施例提供的技术方案的限定，本领域技术人员可知，随着系统架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

下面将对本申请实施例提供的密钥推衍方法进行具体阐述。需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体限定。还需要说明的是，在本申请实施例的附图中，各个实施例所示的步骤，以及步骤之间的先后顺序用于举例，并不构成对本申请实施例的限定。应理解，执行图示中的部分步骤或调整步骤的顺序进行具体实施，均落在本申请的保护范围内。

请参见图 2，图 2 是本申请实施例提供的一种密钥推衍方法的流程示意图。其中，步骤 S201、步骤 S210~步骤 S212 的执行主体为 UE，或者为 UE 中的芯片。步骤 S202 和步骤 S209 的执行主体为移动管理功能网元，或者为移动管理功能网元中的芯片。步骤 S203、步骤 S207~步骤 S208 的执行主体为 AUSF 网元，或者为 AUSF 网元中的芯片。步骤 S204~步骤 S206 的执行主体为认证设备，或者为认证设备中的芯片。以下以 UE、移动管理功能网元、AUSF 网元、认证设备为密钥推衍方法的执行主体为例进行说明。该方法可以包括但不限于如下步骤：

步骤 S201：UE 向移动管理功能网元发送注册请求。

UE 发送该注册请求以请求注册到网络。该注册请求可以包括该 UE 的第二标识，第二标识可以是 SUCI 或 SUPI。

步骤 S202：移动管理功能网元接收到该注册请求后，向 AUSF 网元发送认证请求。

该认证请求用于请求 AUSF 网元对该 UE 进行认证。该认证请求可以包括 UE 的第二标识。移动管理功能网元可以调用 AUSF 网元提供的 UE 认证服务(Nausf_UEAuthentication), 向 AUSF 网元发送该注册请求 (Nausf_UEAuthentication_Authenticate Request)。

步骤 S203: AUSF 网元向认证设备发送第一触发指示, 该第一触发指示用于触发认证 UE。

在本申请实施例中, 在 AUSF 网元向位于 3GPP 网络外的认证设备发送第一触发指示之前, 该 AUSF 网元可以确定 UE 是否需要与该认证设备执行认证。若 AUSF 网元确定 UE 需要与该认证设备执行认证, 可以表示认证该 UE 的认证设备处于 3GPP 网络外, 或者可以表示该 AUSF 网元无法对 UE 进行认证。所以, 该 AUSF 网元可以向认证设备发送第一触发指示, 以触发位于 3GPP 网络外的认证设备认证 UE。该第一触发指示可以包括触发 EAP 认证的消息, 例如 EAP 开始 (EAP-start) 消息, EAP 身份回复消息等, 第一触发指示还可以包含该 UE 的第二标识。

可以理解的是 若 AUSF 网元确定 UE 不需要与该认证设备执行认证, 可以表示该 AUSF 网元可以自行对 UE 进行认证, 或者可以表示认证该 UE 的认证设备处于 3GPP 网络内。所以该 AUSF 网元可以不向认证设备发送第一触发指示。例如, 此时, 该 AUSF 网元作为认证 UE 的认证设备。

在一种实现方式中, AUSF 网元可以通过如下方式确定 UE 需要与处于 3GPP 网络外的认证设备执行认证:

第一种方式, AUSF 网元接收来自移动管理功能网元的 UE 的第二标识, 并根据该第二标识, 确定该 UE 需要与该认证设备执行认证。该第二标识包括路由标识 RID, 该 RID 可以指示认证 UE 的认证设备的标识。若认证设备的标识与该 AUSF 网元的标识不同, 则表示认证设备并非该 AUSF 网元, 因此, AUSF 网元可以确定该 UE 需要与该认证设备执行认证。

其中, 认证设备的标识用于唯一标识该认证设备, AUSF 网元的标识用于唯一标识该 AUSF 网元。可选的, 标识可以指域名或 IP 地址。AUSF 网元可通过如下方式确定认证设备的标识: 第二标识为 SUCI, AUSF 网元根据 SUCI 中的 PLMN ID 和 RID 获得认证设备的 IP 地址。又如, 该第二标识是网络访问标识(network access identifier, NAI)格式, AUSF 网元根据 NAI 格式的第二标识确定认证设备的域名。采用 NAI 格式的第二标识包含用户部分和域名部分 (即第二标识的形式为: <用户部分>@<域名部分>, 例如 1234@abcd)。其中, 域名部分可以包括认证设备的域名。

若认证设备的标识与 AUSF 网元的标识不同可以包括但不限于如下情况: 1、认证设备的域名与该 AUSF 网元的域名不同, 表示认证设备并非该 AUSF 网元。2、认证设备的 IP 地址与该 AUSF 网元的 IP 地址不同, 则表示认证设备并非该 AUSF 网元, 因此, AUSF 网元可以确定该 UE 需要与该认证设备执行认证。3、认证设备的 IP 地址与该 AUSF 网元的 IP 地址不属于同一网段, 则可以表示认证设备与该 AUSF 网元不位于同一局域网内, 因此可以认为认证设备与该 AUSF 网元位于不同的网络内。又因 AUSF 网元位于 3GPP 网络内, 因此可以认为认证设备位于 3GPP 网络内外。所以, AUSF 网元可以确定该 UE 需要与该认证设备执行认证。

可选的，若认证设备的标识与该 AUSF 网元的标识相同，则表示 UE 需要与该 AUSF 网元执行认证。此时，AUSF 网元无需发送上述第一触发指示。上述第二标识可以为该 UE 的 SUCI 或 SUPI。需要说明的是，AUSF 网元所接收到的该第二标识可以携带于上述注册请求中。

第二种方式，AUSF 网元接收来自移动管理功能网元的 UE 的第二标识，该第二标识为 SUCI 或 SUPI；该 AUSF 网元向统一数据管理 UDM 网元发送第一请求消息，该第一请求消息包括该 SUCI 或该 SUPI；该 AUSF 网元接收来自该 UDM 网元的第一响应消息，该第一响应消息包括认证设备的标识；该 AUSF 网元根据该认证设备的标识，确定该 UE 需要与该认证设备执行认证。

认证 UE 的认证设备的标识可以保存于 UDM 网元中。AUSF 网元向该 UDM 网元发送第一请求消息，以请求获取认证 UE 的认证设备的标识。若认证设备的标识与该 AUSF 网元的标识不同，则表示认证设备并非该 AUSF 网元，因此，AUSF 网元可以确定该 UE 需要与该认证设备执行认证。

UDM 网元可以根据 UE 的 SUCI 或 SUPI 获得认证该 UE 的认证设备的标识。例如，UDM 网元存储有 UE 的 SUCI 与认证该 UE 的认证设备的标识之间的第一对应关系，UDM 网元接收到第一请求消息后，可以根据该第一请求消息携带的 SUCI，以及该第一对应关系获取认证该 UE 的认证设备的标识。又如，UDM 网元存储有 UE 的 SUPI 与认证该 UE 的认证设备的标识之间的第二对应关系，UDM 网元接收到第一请求消息后，可以根据该第一请求消息携带的 SUPI，以及该第二对应关系获取认证该 UE 的认证设备的标识。或者，UDM 网元接收到第一请求消息后，可以根据该第一请求消息携带的 SUCI，确定 UE 的 SUPI；然后根据该 SUPI 以及该第二对应关系获取认证该 UE 的认证设备的标识。

需要说明的是，AUSF 网元发送的第一请求消息包括 SUCI 的情况下，该 SUCI 可以是 AUSF 网元从移动管理功能网元接收到的。AUSF 网元发送的第一请求消息包括 SUPI 的情况下，该 SUPI 可以是 AUSF 网元从移动管理功能网元接收到的；或者，该 SUPI 可以是 AUSF 网元从移动管理功能网元接收到的 SUCI 确定的。还需要说明的是，AUSF 网元从移动管理功能网元接收到的该第二标识可以携带于上述注册请求中。

在一种实现方式中，AUSF 网元可以根据 UE 的第二标识，确定该 UE 的第一标识；并将该第一标识发送至认证设备；该第一触发指示具体用于触发根据该第一标识对应的认证凭证（即前述第二认证凭证）认证该 UE。其中，该第一标识用于在 3GPP 网络外的网络中标识该 UE，例如用于在位于 3GPP 网络外的认证设备内标识 UE。第一标识也可以称为外部标识。第一标识可以是一般公共订阅标识符（generic public subscription identifier，GPSI）。第二标识为 SUCI 或 SUPI；该第二标识由该 AUSF 网元从移动管理功能网元接收，例如，该第二标识携带于上述注册请求中。

通过这种方式，可以避免将 UE 的第二标识（即 SUCI 或者 SUPI）发给位于 3GPP 网络外的认证设备，即可以避免将 UE 的第二标识从 3GPP 网络内部传输到 3GPP 网络外部，从而避免了泄露用户的隐私。可选的，第一标识可以与第一触发指示分开发送，或者一起发送，本申请实施例对此不做限定。

可选的，不同 UE 的第一标识对应的认证凭证可以相同，也可以不同。不同 UE 的第一

标识对应的认证凭证相同，使得认证设备可以使用一个认证凭证对多个 UE 进行认证。在一种实现方式中，不同 UE 的第一标识可以相同，也可以不同。不同 UE 的第一标识相同的情况下，不同 UE 的第一标识可以对应同一认证凭证。

可选的，AUSF 网元可以自行确定 UE 的第一标识，或者，向 UDM 网元请求获取 UE 的第一标识。若 AUSF 网元存储有 UE 的第一标识，AUSF 网元可以根据 UE 的第二标识自行确定该 UE 的第一标识。UE 的第一标识和第二标识可以相同，也可以不相同。AUSF 网元向 UDM 网元发送请求，以请求获取 UE 的第一标识，该请求中包括 UE 的第二标识。UDM 网元存储有 UE 的第一标识，UDM 网元根据 UE 的第二标识，确定与该第二标识对应的第一标识，并将该第一标识发送给 AUSF 网元。例如，UDM 网元从 UE 的第二标识（如 SUCI）解析出 SUPI，然后根据 SUPI 获得该 SUPI 对应的 GPSI（即第二标识），向 AUSF 返回该 GPSI。上述 AUSF 网元向该 UDM 网元发送的请求可以携带于 UE 认证获得服务请求（Nudm_UEAuthentication_Get Request）消息中。

需要说明的是，AUSF 网元可以确定认证设备的标识，和/或，UE 的第一标识。其中，UE 的第一标识可以用于确定认证设备的标识，也可以发送给认证设备以触发认证设备根据该第一标识对应的认证凭证认证该 UE。认证设备的标识可以通过 UE 的第二标识确定的，也可以通过 UE 的第一标识确定的。

步骤 S204：认证设备对该 UE 进行认证。

认证设备接收到第一触发指示后，开始对 UE 进行认证。本申请实施例对认证设备所采用的认证方法不做限定。认证方法可以包括但不限于 EAP 认证方法、EAP-TLS 认证方法、EAP-AKA 认证方法、5G AKA 认证方法、使用证书的认证方法或协议（如 RFC3748、RFC5216、RFC5281、3GPP TS 33.501 等）中规定的认证方法等。

其中，UE 存储有 UE 的第一认证凭证，认证设备存储有 UE 的第二认证凭证，该 UE 与该认证设备可以根据该 UE 的第一认证凭证和该 UE 的第二认证凭证进行相互认证。例如，认证设备根据该 UE 的第二认证凭证对该 UE 进行认证。UE 根据该 UE 的第一认证凭证对该认证设备进行认证。可选的，认证设备可以根据 UE 的第二标识或第一标识获取该 UE 的第二认证凭证。

在本申请实施例中，认证设备可以自行决定采用何种认证方法对 UE 进行认证；或者，AUSF 网元可以指示认证设备采用何种认证方法对 UE 进行认证。AUSF 网元可以自行决定，指示认证设备采用何种认证方法对 UE 进行认证；或者，根据来自 UDM 网元的通知信息确定，指示认证设备采用何种认证方法对 UE 进行认证。

步骤 S205：在该 UE 被成功认证的情况下，认证设备生成 MSK 和 EMSK。

认证设备根据 UE 的第二认证凭证生成 MSK 和 EMSK。

步骤 S206：认证设备向 AUSF 网元发送认证成功消息和第一密钥，该认证成功消息用于指示 UE 被认证设备成功认证。

需要说明的是，认证成功消息和第一密钥可以同时发送，也可以分开发送。分开发送的情况下，可以先发送认证成功消息，也可以先发送第一密钥。由图 2 可知，认证成功消息从认证设备发出，先后经由 AUSF 网元、移动管理功能网元中转，以传输至 UE。需要说明的是，在一种实现方式中，当实施本申请实施例所述的密钥推衍方式的网络架构中部署

有协议转化网元的情况下，该认证成功消息也可以经由 AUSF 网元、协议转化网元、移动管理功能网元中转以传输至 UE。

第一密钥的生成可以参考推衍方式 2。

步骤 S207：AUSF 网元根据第一密钥生成鉴权服务密钥 Kausf。

AUSF 网元接收到来自认证设备的认证成功消息和第一密钥后，可以从该第一密钥中获取部分比特位作为 Kausf。例如，取第一密钥的最高 256 个比特位的值作为 Kausf。

在一种实现方式中，AUSF 网元可以根据该第一密钥和生成参数生成 Kausf。其中，生成参数可以包括但不限于以下一项或多项：UE 当前接入的服务网络的标识或该 UE 的标识。其中，UE 当前接入的服务网络可以为该 UE 的归属地网络或者漫游地网络。UE 的标识可以包括前述第一标识或第二标识。

可选的，该生成参数可以包括但不限于以下一项或多项：UE 当前接入的服务网络的标识、该 UE 的标识或推衍方式参数。AUSF 网元根据该第一密钥和生成参数生成 Kausf 的情况下，该生成参数中推衍方式参数的取值，与 AUSF 网元根据 EMSK 和生成参数生成 Kausf 的情况下，该生成参数中推衍方式参数的取值不同。对于 AUSF 网元而言，该 AUSF 网元确定 UE 需要与位于 3GPP 网络外的认证设备执行认证的情况下，AUSF 网元可以根据第一密钥和生成参数生成 Kausf。该 AUSF 网元确定 UE 不需要与位于 3GPP 网络外的认证设备执行认证的情况下，AUSF 网元可以根据 EMSK 和生成参数生成 Kausf。因此，AUSF 网元可以确定 UE 是否需要与位于 3GPP 网络外的认证设备执行认证，确定推衍方式参数的取值。通过将推衍方式参数作为确定 Kausf 的其中一个参数，有利于使得在 3GPP 网络外对 UE 进行认证的情况下生成的 Kausf，与在 3GPP 网络内对 UE 进行认证的情况生成的 Kausf 不同，从而实现密钥隔离。推衍方式参数可以为 1 比特的二进制位（表示为 0 或 1）、密钥衍生功能（Key Derivation Function, KDF）算法的输入值（如 FC 值）或者其他值，本申请实施例对此不做限定。

需要说明的是，AUSF 网元生成 Kausf 之后，从 Kausf 推衍 Kseaf，以及从 Kseaf 推衍 Kamf 的过程可参见图 1b 中相应流程的描述，此处不再赘述。

若 AUSF 网元确定 UE 不需要与该认证设备执行认证，可以表示该 AUSF 网元可以自行对 UE 进行认证，或者可以表示认证该 UE 的认证设备处于 3GPP 网络内。此时，AUSF 网元可以采用推衍方式 1 生成 Kausf，即 AUSF 网元根据 EMSK 生成 Kausf。可选的，AUSF 网元可以根据 EMSK 和生成参数生成 Kausf。其中，生成参数参见前文描述，此处不再赘述。

步骤 S208：AUSF 网元向移动管理功能网元发送该认证成功消息。

需要说明的是，步骤 S207 和步骤 S208 的执行顺序不分先后，既可以同时执行，也可以先后执行。

步骤 S209：移动管理功能网元接收来自 AUSF 网元的认证成功消息后，向所述 UE 发送该认证成功消息。

步骤 S210：UE 根据该认证成功消息，生成 MSK 以及 EMSK。

UE 接收到来自移动管理功能网元的认证成功消息后，生成 MSK 以及 EMSK。需要说明的是，步骤 S210 的执行过程可参见图 1b 中步骤 S105 的具体描述，此处不再赘述。

步骤 S211：UE 判断认证设备是否位于 3GPP 网络外。

UE 接收到来自移动管理功能网元的认证成功消息后，通过判断认证设备是否位于 3GPP 网络外，以确定采用哪种推衍方式获得 Kausf。UE 判断认证设备是否位于 3GPP 网络外的具体实施方式可参见图 4 和图 5 所示实施例。

需要说明的是，UE 判断的内容为“认证设备是否位于 3GPP 网络外”仅用于举例，其中，“认证设备是否位于 3GPP 网络外”，还可以描述为“是否采用 MSK 推衍 Kausf”、“是否采用第一密钥推衍 Kausf”、“是否采用 EMSK 推衍 Kausf”、“是否采用推衍方式 1 推衍 Kausf”、“是否采用推衍方式 2 推衍 Kausf”等等。具体可以参见前文描述，此处不再赘述。

步骤 S212：在该认证设备位于该 3GPP 网络外的情况下，该 UE 根据 MSK，生成鉴权服务密钥 Kausf。

在确定认证设备位于 3GPP 网络外的情况下，该 UE 可以采用推衍方式 2 生成 Kausf，即根据 MSK 生成 Kausf。可选的，UE 可以从 MSK 获得第一密钥，然后根据第一密钥生成 Kausf。第一密钥参见前文描述，此处不再赘述。

需要说明的是，网络侧和 UE 各自生成的 MSK 相同，网络侧和 UE 从 MSK 各自获得的第一密钥也相同，因此，网络侧和 UE 各自生成的 Kausf 也相同。从而使得 UE 与网络侧各自生成的 Kseaf、Kamf 也相同，这样有利于确保 UE 与移动管理功能网元之间顺利进行通信。另外，在网络侧，AUSF 网元从位于 3GPP 网络外的认证设备接收到的第一密钥，是从 MSK 获得的，所以不会违背协议规定（即 CdP 和 AAA 服务器均无法将 EMSK 或 EMSK 的最高 256 个比特位的值传输给其他网元）。

在一种实现方式中，UE 可以根据第一密钥和生成参数，生成 Kausf；其中，该生成参数包括但不限于以下一项或多项：该 UE 当前接入的服务网络的标识或该 UE 的标识。该 UE 当前接入的服务网络可以为该 UE 归属地网络或者漫游地网络。可选的，该生成参数包括但不限于以下一项或多项：该 UE 当前接入的服务网络的标识、该 UE 的标识或推衍方式参数。需要说明的是，UE 根据第一密钥和生成参数生成 Kausf 的执行过程，与 AUSF 网元根据第一密钥和生成参数生成 Kausf 的执行过程相同，具体可参见步骤 S207 中的描述。

在一种实现方式中，UE 通过判断，确定认证设备位于 3GPP 网络内的情况下，该 UE 可以采用推衍方式 1 生成 Kausf，即可以根据 EMSK 生成 Kausf。例如，从该 EMSK 中获取部分比特位作为 Kausf。例如，取 EMSK 的最高 256 个比特位的值作为 Kausf。

在本申请实施例中，在认证设备位于 3GPP 网络外的情况下，UE 根据 MSK 生成 Kausf；在认证设备位于 3GPP 网络内的情况下，该 UE 根据 EMSK 生成 Kausf。通过这种方式，使得 UE 可以兼容认证设备位于 3GPP 网络外所采用的密钥推衍方式（即推衍方式 2），和认证设备位于 3GPP 网络内所采用的密钥推衍方式（即推衍方式 1）。

由于认证设备位于 3GPP 网络外或者位于 3GPP 网络内的情况下，用于生成 Kausf 的密钥（即 MSK 或 EMSK）不同，可以使得生成的 Kausf 不同，从而实现密钥隔离。认证设备位于 3GPP 网络外或者位于 3GPP 网络内的情况下，推衍方式参数均作为确定 Kausf 的其中一个参数，且在认证设备位于 3GPP 网络外和位于 3GPP 网络内的情况下，推衍方式参数的取值不同，可以使得认证设备位于 3GPP 网络外的情况下生成的 Kausf，与认证设备位于 3GPP 网络内的情况生成的 Kausf 不同，从而进一步实现密钥隔离。

需要说明的是，结合步骤 S211 中的描述：UE 判断的内容为“认证设备是否位于 3GPP 网络外”仅用于举例，“认证设备是否位于 3GPP 网络外”，还可以描述为“是否采用 MSK 推衍 Kausf”、“是否采用第一密钥推衍 Kausf”、“是否采用 EMSK 推衍 Kausf”、“是否采用推衍方式 1 推衍 Kausf”、“是否采用推衍方式 2 推衍 Kausf”等等。可以理解的是，UE 判断的内容不同时，该 UE 所确定的内容相应变化。例如，UE 判断的内容为“是否采用推衍方式 2 推衍 Kausf”时，UE 所确定的内容是：确定采用推衍方式 2 推衍 Kausf，或者，确定不采用推衍方式 2 推衍 Kausf。对于 UE 判断的内容的其他描述，该 UE 所确定的内容，此处不再一一举例。

在实施本申请实施例中，UE 通过判断认证设备是否位于 3GPP 网络外，以确定根据 EMSK 还是 MSK 获得 Kausf，使得 UE 可以兼容认证设备位于 3GPP 网络外所采用的密钥推衍方式（即推衍方式 2），和认证设备位于 3GPP 网络内所采用的密钥推衍方式（即推衍方式 1）。

请参见图 3，图 3 是本申请实施例提供的另一种密钥推衍方法的流程示意图，该方法详细描述了在图 1c 所示的网络架构中包括协议转化网元的情况下，密钥推衍方法的流程。其中，步骤 S301、步骤 S312~步骤 S314 的执行主体为 UE，或者为 UE 中的芯片。步骤 S302 和步骤 S311 的执行主体为移动管理功能网元，或者为移动管理功能网元中的芯片。步骤 S303 和步骤 S310 的执行主体为 AUSF 网元，或者为 AUSF 网元中的芯片。步骤 S304、步骤 S308~步骤 S309 的执行主体为协议转化设备，或者为协议转化设备中的芯片。步骤 S305~步骤 S307 的执行主体为认证设备，或者为认证设备中的芯片。以下以 UE、移动管理功能网元、AUSF 网元、协议转化设备、认证设备为密钥推衍方法的执行主体为例进行说明。

该方法可以包括但不限于如下步骤：

步骤 S301：UE 向移动管理功能网元发送注册请求。

步骤 S302：移动管理功能网元接收到该注册请求后，向 AUSF 网元发送认证请求。

需要说明的是，步骤 S301~步骤 S302 的执行过程可参见图 2 中步骤 S201~步骤 S202 的具体描述，此处不再赘述。

步骤 S303：AUSF 网元向协议转化网元发送第二触发指示，该第二触发指示用于触发认证 UE。第二触发指示可以包含触发 EAP 认证的消息，例如 EAP 开始（EAP-start）消息，EAP 身份回复消息等。第二触发指示还可以包含一个显式的指示信息以及 UE 的标识，例如该指示信息为 1 时代表触发认证 UE，该指示信息为 0 时代表不触发认证 UE。第二触发指示还可以包含一个隐式的指示信息，例如，第二触发指示包含 UE 的标识时可以表示该第二触发指示包含该隐式的指示信息。当第二触发指示包含隐式的指示信息时，代表触发认证 UE。UE 的标识可以是 UE 的第一标识，也可以是 UE 的第二标识。

AUSF 网元向协议转化网元发送第二触发指示，以触发协议转化网元向认证设备发送第三触发指示，进而触发认证设备认证 UE。AUSF 网元发送第二触发指示的内容可以参见图 2 实施例中步骤 S203 的相关描述，此处不再赘述。

步骤 S304：协议转化网元接收到该第二触发指示后，向认证设备发送第三触发指示，该第三触发指示用于触发认证该 UE；该第三触发指示根据该第二触发指示得到。

第三触发指示可以用于触发认证设备认证该 UE。可选的,第三触发指示可以是第二触发指示,即协议转化网元将接收到第二触发指示转发给认证设备。或者,第三触发指示由协议转化网元根据第二触发指示构造得到。其中,第三触发指示的内容可参见图 2 实施例中步骤 S203 中第一触发指示的相关描述,此处不再赘述。不同点在于,步骤 S203 中,第一触发指示由 AUSF 网元发送给认证设备。步骤 S304 中,第一触发指示由协议转化网元发送给认证设备。例如,协议转化网元从 AUSF 网元获得第二触发指示(显式指示),若第二触发指示中显式的指示信息的值为 1 时,协议转化网元生成第三触发指示(EAP 开始消息)。

步骤 S305:认证设备对该 UE 进行认证。

步骤 S306:在该 UE 被成功认证的情况下,认证设备生成 MSK 和 EMSK。

需要说明的是,步骤 S305~步骤 S306 的执行过程可参见图 2 中步骤 S204~步骤 S205 的具体描述,此处不再赘述。

步骤 S307:认证设备向协议转化网元发送认证成功消息和第一密钥,该认证成功消息用于指示 UE 被认证设备成功认证。

需要说明的是,步骤 S307 的执行过程可参见图 2 中步骤 S206 的具体描述,此处不再赘述。区别在于:步骤 S206 中,认证成功消息和第一密钥由认证设备向 AUSF 网元发送;步骤 S307 中,由认证设备向协议转化网元发送。

步骤 S308:协议转化网元根据第一密钥生成鉴权服务密钥 Kausf。

需要说明的是,步骤 S308 中,协议转化网元接收到来自认证设备的认证成功消息和第一密钥后,生成 Kausf 仅用于举例,并不构成对本申请实施例的限定。在其他可行的实现方式中,协议转化网元在接收到来自认证设备的认证成功消息和第一密钥后,可以将该认证成功消息和第一密钥发送给 AUSF 网元。相应的,AUSF 网元可以根据来自协议转化网元的第一密钥生成 Kausf。换言之,在网络侧,生成 Kausf 的网元可以为协议转化网元也可以为 AUSF 网元。当生成 Kausf 的网元为协议转化网元时,协议转化网元可以将生成的 Kausf 发送给 AUSF 网元,由 AUSF 网元从 Kausf 推衍 Kseaf。后续从 Kseaf 推衍 Kamf 的过程可参见图 1b 中相应流程的描述,此处不再赘述。

密钥的推衍是基于单向函数(哈希函数)实现的,因此,AUSF 网元虽然接收到了 Kausf,但是无法获知用于推衍 Kausf 的第一密钥,从而能实现协议转化网元与 AUSF 网元的密钥隔离。其中,协议转化网元与 AUSF 网元的密钥隔离指:AUSF 网元无法获知协议转化网元所使用的密钥(即第一密钥)。在 AUSF 网元接收到的 Kausf 来自认证设备的情况下,可以实现 AUSF 网元与认证设备的密钥隔离。

需要说明的是,协议转化网元根据第一密钥生成 Kausf 的过程可以与 AUSF 网元根据第一密钥生成 Kausf 的过程相同,具体可参见图 2 中步骤 S207 的具体描述,此处不再赘述。

步骤 S309:协议转化网元向 AUSF 网元发送该认证成功消息。

需要说明的是,步骤 S308 和步骤 S309 的执行顺序不分先后,既可以同时执行,也可以先后执行。

步骤 S310:AUSF 网元接收到来自协议转化网元的认证成功消息后,向移动管理功能网元发送该认证成功消息。

步骤 S311：移动管理功能网元接收来自 AUSF 网元的认证成功消息后，向前述 UE 发送该认证成功消息。

步骤 S312：UE 根据该认证成功消息，生成 MSK 以及 EMSK。

步骤 S313：UE 判断认证设备是否位于 3GPP 网络外。

步骤 S314：在该认证设备位于该 3GPP 网络外的情况下，该 UE 根据 MSK，生成鉴权服务密钥 Kausf。

需要说明的是，步骤 S311~步骤 S314 的执行过程可参见图 2 中步骤 S209~步骤 S212 的具体描述，此处不再赘述。

在本申请实施例中，通过协议转化网元推衍 Kausf，使得 AUSF 网元即使接收到 Kausf，也无法获知用于推衍 Kausf 的第一密钥，从而能实现协议转化网元与 AUSF 网元的密钥隔离，以提高通信的安全性。

需要说明的是，图 4、图 5 实施例以实施密钥推衍方法的网络架构不包括协议转化网元为例，并不构成对本申请实施例的限定。用于实施图 4 或图 5 实施例中的密钥推衍方法的网络架构可以部署有协议转化网元，部署有协议转化网元的情况下，密钥推衍方法的流程可参照图 3 实施例中的描述。

请参见图 4，图 4 是本申请实施例提供的又一种密钥推衍方法的流程示意图，该方法详细描述了 UE 根据第一指示信息确定认证设备是否位于 3GPP 网络外。其中，步骤 S401、步骤 S410~步骤 S412 的执行主体为 UE，或者为 UE 中的芯片。步骤 S402 和步骤 S409 的执行主体为移动管理功能网元，或者为移动管理功能网元中的芯片。步骤 S403、步骤 S407~步骤 S408 的执行主体为 AUSF 网元，或者为 AUSF 网元中的芯片。步骤 S404~步骤 S406 的执行主体为认证设备，或者为认证设备中的芯片。以下以 UE、移动管理功能网元、AUSF 网元、认证设备为密钥推衍方法的执行主体为例进行说明。该方法可以包括但不限于如下步骤：

步骤 S401：UE 向移动管理功能网元发送注册请求。

步骤 S402：移动管理功能网元接收到该注册请求后，向 AUSF 网元发送认证请求。

步骤 S403：AUSF 网元向认证设备发送第一触发指示，该第一触发指示用于触发认证 UE。

步骤 S404：认证设备对该 UE 进行认证。

步骤 S405：在该 UE 被成功认证的情况下，认证设备生成 MSK 和 EMSK。

步骤 S406：认证设备向 AUSF 网元发送认证成功消息和第一密钥，该认证成功消息用于指示 UE 被认证设备成功认证。

步骤 S407：AUSF 网元根据第一密钥生成鉴权服务密钥 Kausf。

需要说明的是，步骤 S401~步骤 S407 的执行过程可分别参见图 2 中步骤 S201~步骤 S207 的具体描述，此处不再赘述。

步骤 S408：AUSF 网元向移动管理功能网元发送该认证成功消息和第三指示信息。

该第三指示信息用于指示该认证设备位于 3GPP 网络外或者该 3GPP 网络内；或者，该第三指示信息可以用于指示采用 MSK（或者第一密钥）推衍 Kausf；或者，该第三指示信

息可以用于指示采用 EMSK 推衍 Kausf；或者，该第三指示信息可以用于指示采用推衍方式 1 推衍 Kausf；或者，该第三指示信息可以用于指示采用推衍方式 2 推衍 Kausf。

或者，该第三指示信息可以用于指示用于推衍 Kausf 的密钥从外部网络（或 3GPP 网络外）获得；或者，该第三指示信息可以用于指示用于推衍 Kausf 的密钥从内部网络（或 3GPP 网络内）获得；或者，该第三指示信息可以用于指示用于推衍 Kausf 的密钥从外部网络（或 3GPP 网络外）中的网元获得；或者，该第三指示信息可以用于指示用于推衍 Kausf 的密钥从内部网络（或 3GPP 网络内）中的网元获得。

或者，该第三指示信息可以用于指示正在执行认证凭证位于独立于 SNPN 的第三方的认证；或者，该第三指示信息可以用于指示正在执行外部（或 3GPP 外部）认证。或者，该第三指示信息可以用于指示认证凭证位于独立于 SNPN 的第三方的认证已完成；或者，该第三指示信息可以用于指示外部（或 3GPP 外部）认证已完成。或者，该第三指示信息可以用于指示即将执行认证凭证位于独立于 SNPN 的第三方的认证；或者，该第三指示信息可以用于指示即将执行外部（或 3GPP 外部）认证”。需要说明的是，本申请实施例中提及的该第三指示信息的作用仅用于举例，在具体实现中，UE 根据来自网络侧的指示信息以使得生成的 Kausf 与网络侧生成的 Kausf 相同的方式，均在本申请保护范围内。该第三指示信息还可以称为第二推衍指示。

AUSF 网元通过向移动管理功能网元发送第三指示信息，使得移动管理功能网元可以获知该认证设备是否位于 3GPP 网络外，进而有利于移动管理功能网元（通过第一指示信息）告知 UE 该认证设备是否位于 3GPP 网络外。或者，AUSF 网元通过向移动管理功能网元发送第三指示信息，使得移动管理功能网元可以转发该第三指示信息至 UE，以使 UE 获知该认证设备是否位于 3GPP 网络外。此时，第三指示信息与第一指示信息相同。

需要说明的是，AUSF 网元可以在认证过程中发送第三指示信息，也可以在认证完成后发送第三指示信息。还需要说明的是，本申请对 AUSF 网元发送认证成功消息与发送第三指示信息的顺序不做限定。

在本申请实施例中，AUSF 网元可以在确定 UE 需要与认证设备执行认证的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在向认证设备发送第一触发指示的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在接收到来自认证设备的认证成功消息的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在向认证设备发送第一触发指示，并接收到来自认证设备的认证成功消息的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在向协议转化网元发送第二触发指示的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在接收到来自协议转化网元的认证成功消息的情况下，向移动管理功能网元发送第三指示信息。可选的，AUSF 网元可以在向协议转化网元发送第二触发指示，并接收到来自该协议转化网元的认证成功消息的情况下，向移动管理功能网元发送第三指示信息。

步骤 S409 移动管理功能网元接收来自 AUSF 网元的认证成功消息和第三指示信息后，向前述 UE 发送该认证成功消息和第一指示信息。

第一指示信息可以用于指示该认证设备位于 3GPP 网络外或者该 3GPP 网络内，该第三

指示信息根据该第一指示信息确定。需要说明的是，第一指示信息和第三指示信息所指示的内容相同，关于第一指示信息的内容，可以参见步骤 S408 中的描述。

在一种实现方式中，第一指示信息可以通过已有信元指示。此时，第一指示信息为隐式指示，即并未生成新的消息或在现有消息中增加新的消息元素。例如，上述信元为 ABBA 时，第一指示信息包括 ABBA，移动管理功能网元接收到第三指示信息，且第三指示信息用于指示认证设备位于 3GPP 网络外的情况下，移动管理功能网元可以将 ABBA 的值确定为非零值，ABBA 的值为非零值的情况下该 ABBA 用于指示认证设备位于 3GPP 网络外。可以理解的是，第三指示信息用于指示认证设备位于 3GPP 网络内的情况下，该移动管理功能网元可以将 ABBA 的值确定为 0，ABBA 的值为 0 的情况下该 ABBA 用于指示认证设备位于 3GPP 网络内。需要说明的是，上述 ABBA 的值所代表的含义用于举例，并不构成本申请实施例的限定。例如，ABBA 的值为 0 的情况下该 ABBA 可以用于指示认证设备位于 3GPP 网络外，ABBA 的值为非零值的情况下该 ABBA 可以用于指示认证设备位于 3GPP 网络内。采用现有信元以指示第一指示信息，可以减少对已有协议的改动。

在另一种实现方式中，第一指示信息可以包括一个标志位 1 (flag) 或指示字段 1，该标志位 1 (或指示字段 1) 可以用于指示认证设备位于 3GPP 网络外或者 3GPP 网络内。例如，若第一指示信息包括该标志位 1 (或指示字段 1)，则该第一指示信息可以用于指示认证设备位于 3GPP 网络外。可以理解的是，若第一指示信息不包括标志位 1 (或指示字段 1)，则该第一指示信息可以用于指示认证设备位于 3GPP 网络内。或者，若第一指示信息包括该标志位 1 (或指示字段 1)，则该第一指示信息可以用于指示认证设备位于 3GPP 网络内。若第一指示信息不包括标志位 1 (或指示字段 1)，则该第一指示信息可以用于指示认证设备位于 3GPP 网络外。移动管理功能网元可以根据第三指示信息所指示的内容，确定构造的第一指示信息中是否包括该标志位 1 (或指示字段 1)。

在又一种实现方式中，移动管理功能网元可以将接收到的第三指示信息转发给 UE，此时，第三指示信息与第一指示信息相同，第三指示信息与第一指示信息均为显式指示。

步骤 S410：UE 根据该认证成功消息，生成 MSK 以及 EMSK。

需要说明的是，步骤 S410 的执行过程可参见图 2 中步骤 S210 的具体描述，此处不再赘述。

步骤 S411：UE 根据该第一指示信息，确定认证设备是否位于 3GPP 网络外。

UE 接收到来自移动管理功能网元的第一指示信息后，可以根据该第一指示信息，判断认证设备是否位于 3GPP 网络外。

具体的，UE 可以根据第一指示信息所指示的内容，确定认证设备是否位于 3GPP 网络外。例如，第一指示信息可以用于指示该认证设备位于 3GPP 网络外，则 UE 确定认证设备是否位于 3GPP 网络外。

在一种实现方式中，第一指示信息和第三指示信息可以通过携带的指示参数指示认证设备是否位于 3GPP 网络外或者 3GPP 网络外。例如，第三指示信息包括指示参数，在该指示参数的值为非 0 的情况下，该第三指示信息可以用于指示认证设备位于 3GPP 网络外。在该指示参数的值为 0 的情况下，该第三指示信息可以用于指示认证设备位于 3GPP 网络内。移动管理功能网元接收到第三指示信息后，若转发该第三指示信息，此时第一指示信

息与第三指示信息相同，即第一指示信息中也包括指示参数。UE 可以根据第一指示信息中指示参数的取值，确定认证设备是否位于 3GPP 网络外。

可选的，UE 可以根据是否接收到第一指示信息，确定认证设备是否位于 3GPP 网络外。例如，第一指示信息用于指示该认证设备位于 3GPP 网络外的情况下，若 UE 接收到来自移动管理功能网元的认证成功消息的情况下，未接收到该第一指示信息，则该 UE 可以确定认证设备是否位于 3GPP 网络内。同理，第一指示信息用于指示该认证设备位于 3GPP 网络内的情况下，若 UE 接收到来自移动管理功能网元的认证成功消息的情况下，未接收到该第一指示信息，则该 UE 可以确定认证设备是否位于 3GPP 网络外。可选的，移动管理功能网元确定认证设备位于 3GPP 网络内的情况下，可以不向 UE 发送第一指示信息。

可以理解的是，对于第三指示信息，移动管理功能网元也可以根据是否接收到第三指示信息，确定认证设备是否位于 3GPP 网络外。例如，第三指示信息用于指示该认证设备位于 3GPP 网络外的情况下，若移动管理功能网元在接收到认证成功消息的情况下，未接收到该第三指示信息，则该移动管理功能网元可以确定认证设备是否位于 3GPP 网络内。同理，第三指示信息用于指示该认证设备位于 3GPP 网络内的情况下，若移动管理功能网元在接收到认证成功消息的情况下，未接收到该第三指示信息，则该移动管理功能网元可以确定认证设备位于 3GPP 网络外。

步骤 S412：在该认证设备位于该 3GPP 网络外的情况下，该 UE 根据 MSK，生成鉴权服务密钥 Kausf。

需要说明的是，步骤 S412 的执行过程可参见图 2 中 S212 的具体描述，此处不再赘述。

在本申请实施例中，Kamf 可以是根据 Kseaf、ABBA 以及 SUPI 推衍得到的。通过采用现有信元 ABBA 作为第一指示信息，一方面可以减少对已有协议的改动；另一方面，由于 ABBA 也是推衍 Kamf 的参数，因此，若 ABBA 被篡改，UE 和移动管理功能网元生成的 Kamf 将不同，这样可以发现攻击，从而有利于提高通信的安全性。

在一种实现方式中，在认证设备位于该 3GPP 网络内的情况下，UE 可以根据 EMSK 生成 Kausf。UE 根据 EMSK 生成 Kausf 的相关内容，可参见步骤 S211 中的具体描述，此处不再赘述。

在本申请实施例中，第一指示信息用于指示认证设备位于 3GPP 网络外或者 3GPP 网络内，UE 根据该第一指示信息即可确定采用何种推衍方式（或者采用 EMSK 还是 MSK）推衍 Kausf。

请参见图 5，图 5 是本申请实施例提供的又一种密钥推衍方法的流程示意图。图 5 所示实施例详细描述了 UE 如何根据预配置该 UE 中的第一配置信息判断认证设备是否位于 3GPP 网络外。其中，步骤 S501、步骤 S510~步骤 S512 的执行主体为 UE，或者为 UE 中的芯片。步骤 S502 和步骤 S509 的执行主体为移动管理功能网元，或者为移动管理功能网元中的芯片。步骤 S503、步骤 S507~步骤 S508 的执行主体为 AUSF 网元，或者为 AUSF 网元中的芯片。步骤 S504~步骤 S506 的执行主体为认证设备，或者为认证设备中的芯片。以下以 UE、移动管理功能网元、AUSF 网元、认证设备为密钥推衍方法的执行主体为例进行说明。该方法可以包括但不限于如下步骤：

步骤 S501：UE 向移动管理功能网元发送注册请求。

步骤 S502：移动管理功能网元接收到该注册请求后，向 AUSF 网元发送认证请求。

步骤 S503：AUSF 网元向认证设备发送第一触发指示，该第一触发指示用于触发认证 UE。

步骤 S504：认证设备对该 UE 进行认证。

步骤 S505：在该 UE 被成功认证的情况下，认证设备生成 MSK 和 EMSK。

步骤 S506：认证设备向 AUSF 网元发送认证成功消息和第一密钥，该认证成功消息用于指示 UE 被认证设备成功认证。

步骤 S507：AUSF 网元根据第一密钥生成鉴权服务密钥 Kausf。

步骤 S508：AUSF 网元向移动管理功能网元发送该认证成功消息。

步骤 S509：移动管理功能网元接收来自 AUSF 网元的认证成功消息后，向前述 UE 发送该认证成功消息。

步骤 S510：UE 根据该认证成功消息，生成 MSK 以及 EMSK。

其中，步骤 S501~步骤 S510 的执行过程可分别参见图 2 中步骤 S201~步骤 S210 的具体描述，此处不再赘述。

步骤 S511：UE 根据第二指示信息，确定认证设备是否位于 3GPP 网络外。

在本申请实施例中，UE 可以根据以下方式判断认证设备是否位于 3GPP 网络外。

一种实现方式为，UE 根据第二指示信息，确定认证设备是否位于 3GPP 网络外。该第二指示信息用于指示该认证设备是否位于 3GPP 网络外，该第二指示信息包括于第一配置信息中，UE 可以预先配置有该第一配置信息和第一认证凭证。

具体的，当 UE 确定使用该第一认证凭证进行 EAP 认证的情况下，UE 获得该第一认证凭证，并根据该第一认证凭证生成 MSK 和 EMSK。UE 获得该第一认证凭证的同时，可以获得与该第一认证凭证对应的第一配置信息，进而根据该第一配置信息中的第二指示信息，判断认证设备是否位于 3GPP 网络外。可选的，UE 根据网络广播的标识选择第一网络，然后确定第一网络对应的第一认证凭证。

需要说明的是，该第二指示信息可以为显式的指示信息，或者隐式的指示信息。第二指示信息为显式的指示信息的示例如下：该第二指示信息为 1 比特的二进制位（表示为 0 或 1），该第二指示信息的值为 1 的情况下，该第二指示信息用于指示该认证设备位于 3GPP 网络外，该第二指示信息的值为 0 的情况下，该第二指示信息用于指示该认证设备位于 3GPP 网络内。或者，该第二指示信息的值为 0 的情况下，该第二指示信息用于指示该认证设备位于 3GPP 网络外；该第二指示信息的值为 1 的情况下，该第二指示信息用于指示该认证设备位于 3GPP 网络内。

第二指示信息为隐式的指示信息的示例如下：该第二指示信息包括一个标志位 2 或指示字段 2，该标志位 2（或指示字段 2）用于指示认证设备位于 3GPP 网络外或者 3GPP 网络内。例如，若该标志位 2（或指示字段 2）用于指示认证设备位于 3GPP 网络外，且第二指示信息包括该标志位 2（或指示字段 2），则该第二指示信息用于指示认证设备位于 3GPP 网络外。可以理解的是，若第二指示信息不包括标志位 2（或指示字段 2），则该第二指示信息可以用于指示认证设备位于 3GPP 网络内。或者，若该标志位 2（或指示字段 2）用于

指示认证设备位于 3GPP 网络内，且第二指示信息包括该标志位 2（或指示字段 2），则该第二指示信息可以用于指示认证设备位于 3GPP 网络内。若第二指示信息不包括标志位 2（或指示字段 2），则该第二指示信息可以用于指示认证设备位于 3GPP 网络外。

需要说明的是，第二指示信息用于指示认证设备是否位于 3GPP 网络外，用于举例，并不构成对本申请实施例的限定。例如，该第二指示信息可以用于指示认证 UE 的认证凭证是否位于 3GPP 网络外；或者，该第二指示信息可以用于指示采用 MSK（或者第一密钥）推衍 Kausf；或者，该第二指示信息可以用于指示采用 EMSK 推衍 Kausf；或者，该第二指示信息可以用于指示采用推衍方式 1 推衍 Kausf；或者，该第二指示信息可以用于指示采用推衍方式 2 推衍 Kausf。第二指示信息所指示的内容可以与第一指示信息（或者第三指示信息）所指示的内容相同，具体可以参见步骤 S408~步骤 S409 中的描述，此处不再赘述。

另一种实现方式为，UE 根据认证设备的标识判断认证设备是否位于 3GPP 网络外。可选的，若 UE 获得认证设备的标识，则 UE 确定认证设备位于 3GPP 网络外。可选的，若 UE 未获得认证设备的标识，则 UE 确定认证设备位于 3GPP 网络内。该认证设备的标识可以是服务提供方标识（service provider identity, SP ID），PLMN ID，SNPN ID 等。

UE 可以根据以下方式获得认证设备的标识：

1. UE 从接入网设备的广播消息中获得一个或多个认证设备的标识，UE 选择了第一认证设备的标识。例如，UE 向用户展示从广播消息中获得的所有认证设备的标识，用户手动选择该第一认证设备的标识。

2. UE 预配置了接入网络的标识和认证设备的标识的对应关系。UE 从接入网设备的广播消息中获得一个或多个接入网络的标识，UE 选择了第一接入网络的标识。UE 根据预配置的该对应关系，可以获得与该第一接入网络的标识对应的认证设备的标识。例如，UE 根据网络优先级列表选择了第一接入网络的标识，并根据预配置的第一接入网络的标识与第一认证设备的标识的对应关系，获得第一认证设备的标识。

3. UE 从接入网设备的广播消息中获得一个或多个接入网络的标识，UE 选择了第一接入网络的标识，并从第一接入网络接入，然后从第一接入网络接收到认证设备的标识。

在认证设备对 UE 进行认证（如 EAP 认证）前，UE 可以通过上述任一方式获得该认证设备的标识。然后，在该 UE 被认证设备成功认证后，该 UE 可以采用推衍方式 2 生成 Kausf；可选的，当 UE 无法获得该认证设备的标识的情况下，该 UE 可以采用推衍方式 1 生成 Kausf。

步骤 S512：在该认证设备位于该 3GPP 网络外的情况下，该 UE 根据 MSK，生成鉴权服务密钥 Kausf。

需要说明的是，步骤 S512 的执行过程可参见图 2 中步骤 S212 的具体描述，此处不再赘述。

在本申请实施例中，UE 根据预配置于该 UE 中的第二指示信息判断认证设备是否位于 3GPP 网络外，网络侧无需向 UE 发送指示信息（即 AUSF 网元无需向移动管理功能网元发送第三指示信息，移动管理功能网元也无需向 UE 发送第一指示信息），有利于减少网络侧设备的功耗。

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相应的装置，包括用于执行上述实施例相应的模块。所述模块可以是软件，也可以是硬件，或者是软件和硬件结合。

请参见图6，为本申请提供的一种通信装置的结构示意图。图6所示的通信装置600包括收发模块601和处理模块602。

在一种设计中，装置600为UE：

示例性的，收发模块601，用于接收来自移动管理功能网元的认证成功消息；该认证成功消息用于指示UE被认证设备成功认证；

处理模块602，用于根据该认证成功消息，生成MSK和EMSK；判断认证设备是否位于3GPP网络外；在认证设备位于3GPP网络外的情况下，根据MSK，生成Kausf。

装置600为UE时，用于实现图2~图5所示实施例中UE的功能。

在一种设计中，装置600为AUSF网元：

示例性的，收发模块601，用于向认证设备发送第一触发指示，该第一触发指示用于触发认证UE；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证；

处理模块602，用于根据该第一密钥生成Kausf；

收发模块601，还用于向移动管理功能网元发送认证成功消息和第三指示信息，第三指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内。

装置600为AUSF网元时，用于实现图2~图5所示实施例中AUSF网元的功能。

在一种设计中，装置600为移动管理功能网元：

示例性的，收发模块601，用于接收来自AUSF网元的认证成功消息和第二指示信息，认证成功消息用于指示UE被认证设备成功认证，第二指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内；向该UE发送认证成功消息和第一指示信息，第一指示信息用于指示认证设备位于3GPP网络外或者3GPP网络内；第二指示信息根据第一指示信息确定。

装置600为移动管理功能网元时，用于实现图2~图5所示实施例中移动管理功能网元的功能。

在一种设计中，装置600为协议转化网元：

示例性的，收发模块601，用于接收来自AUSF网元的第二触发指示，该第二触发指示用于触发认证UE；向认证设备发送第三触发指示，该第三触发指示用于触发认证UE；该第三触发指示根据第二触发指示得到；接收来自认证设备的认证成功消息和第一密钥；认证成功消息用于指示UE被认证设备成功认证；

处理模块602，用于根据第一密钥生成Kausf；

收发模块601，还用于向该AUSF网元发送认证成功消息。

装置600为协议转化网元时，用于实现图3所示实施例中协议转化网元的功能。

请参见图7，为本申请提供的另一种通信装置的结构示意图。图7所示的通信装置700包括至少一个处理器701、存储器702，可选的，还可包括通信接口703。

存储器702可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘（hard disk drive，HDD）或固态硬盘（solid-state

drive, SSD)、或者存储器702是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702可以是上述存储器的组合。

本申请实施例中不限定上述处理器701以及存储器702之间的具体连接介质。本申请实施例在图中以存储器702和处理器701之间通过总线704连接,总线704在图中以粗线表示,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。该总线704可以分为地址总线、数据总线、控制总线等。为便于表示,图7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。

处理器701可以具有数据收发功能,能够与其他设备进行通信,在如图7装置中,也可以设置独立的数据收发模块,例如通信接口703,用于收发数据;处理器701在与其他设备进行通信时,可以通过通信接口703进行数据传输。

一种示例中,当UE采用图7所示的形式时,图7中的处理器可以通过调用存储器702中存储的计算机执行指令,使得UE执行上述任一方法实施例中的UE执行的方法。

一种示例中,当AUSF网元采用图7所示的形式时,图7中的处理器可以通过调用存储器702中存储的计算机执行指令,使得AUSF网元执行上述任一方法实施例中的AUSF网元执行的方法。

一种示例中,当移动管理功能网元采用图7所示的形式时,图7中的处理器可以通过调用存储器702中存储的计算机执行指令,使得移动管理功能网元执行上述任一方法实施例中的移动管理功能网元执行的方法。

一种示例中,当协议转化网元采用图7所示的形式时,图7中的处理器可以通过调用存储器702中存储的计算机执行指令,使得协议转化网元执行上述任一方法实施例中的协议转化网元执行的方法。

具体的,图6的处理模块和收发模块的功能/实现过程均可以通过图7中的处理器701调用存储器702中存储的计算机执行指令来实现。或者,图6的处理模块的功能/实现过程可以通过图7中的处理器701调用存储器702中存储的计算机执行指令来实现,图6的收发模块的功能/实现过程可以通过图7中的通信接口703来实现。

本申请实施例还提供一种密钥推导系统,该系统可以包括图2~图5中的移动管理功能网元和AUSF网元。可选的,还包括图2~图5中的UE。可选的,还包括图3中的协议转化网元。

可以理解的是,本申请实施例中的一些可选的特征,在某些场景下,可以不依赖于其他特征,比如其当前所基于的方案,而独立实施,解决相应的技术问题,达到相应的效果,也可以在某些场景下,依据需求与其他特征进行结合。相应的,本申请实施例中给出的装置也可以相应的实现这些特征或功能,在此不予赘述。

本领域技术人员还可以理解到本申请实施例列出的各种说明性逻辑块(illustrative logical block)和步骤(step)可以通过电子硬件、电脑软件,或两者的结合进行实现。这样的功能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员对于相应的应用,可以使用各种方法实现所述的功能,但这种实现不应被理解为超出本申请实施例保护的范围。

本申请所描述的方案可通过各种方式来实现。例如,这些技术可以用硬件、软件或者

硬件结合的方式来实现。对于硬件实现,用于在通信装置(例如,基站,终端、网络实体、核心网网元或芯片)处执行这些技术的处理模块,可以实现在一个或多个通用处理器、数字信号处理器(digital signal processor ,DSP)、数字信号处理器件、专用集成电路(application specific integrated circuit ,ASIC)、可编程逻辑器件、现场可编程门阵列(field programmable gate array ,FPGA)、或其它可编程逻辑装置,离散门或晶体管逻辑,离散硬件部件,或上述任何组合中。通用处理器可以为微处理器,可选地,该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现,例如数字信号处理器和微处理器,多个微处理器,一个或多个微处理器联合一个数字信号处理器核,或任何其它类似的配置来实现。

可以理解,本申请实施例中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。

本申请还提供了一种计算机可读介质,其上存储有计算机程序,该计算机程序被计算机执行时实现上述任一方法实施例的功能。

本申请还提供了一种计算机程序产品,该计算机程序产品被计算机执行时实现上述任一方法实施例的功能。

在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(digital subscriber line ,DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包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,高密度数字视频光盘(digital video disc ,DVD))、或者半导体介质(例如,固态硬盘(solid state disk ,SSD))等。

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，并非是限定时间，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。

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，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。

本申请中各个实施例之间相同或相似的部分可以互相参考。在本申请中各个实施例、以及各实施例中的各个实施方式/实施方法/实现方法中，如果没有特殊说明以及逻辑冲突，不同的实施例之间、以及各实施例中的各个实施方式/实施方法/实现方法之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例、以及各实施例中的各个实施方式/实施方法/实现方法中的技术特征根据其内在的逻辑关系可以组合形成新的实施例、实施方式、实施方法、或实现方法。以上所述的本申请实施方式并不构成对本申请保护范围的限定。

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。

权利要求

1、一种密钥推衍方法，其特征在于，所述方法包括：

用户设备 UE 接收来自移动管理功能网元的认证成功消息；所述认证成功消息用于指示所述 UE 被认证设备成功认证；

所述 UE 根据所述认证成功消息，生成主会话密钥 MSK 和扩展主会话密钥 EMSK；

所述 UE 判断所述认证设备是否位于第三代合作伙伴计划 3GPP 网络外；

在所述认证设备位于所述 3GPP 网络外的情况下，所述 UE 根据所述 MSK，生成鉴权服务密钥 Kausf。

2、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述认证设备位于所述 3GPP 网络内的情况下，所述 UE 根据所述 EMSK，生成 Kausf。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述方法还包括：

所述 UE 接收来自所述移动管理功能网元的第一指示信息，所述第一指示信息用于指示所述认证设备位于所述 3GPP 网络外或者所述 3GPP 网络内；

所述 UE 判断所述认证设备是否位于 3GPP 网络外，包括：

所述 UE 根据所述第一指示信息，确定所述认证设备是否位于 3GPP 网络外。

4、如权利要求 3 所述的方法，其特征在于，所述第一指示信息包括防止架构降级 ABBA，所述 ABBA 的值为非零值的情况下，所述 ABBA 用于指示所述认证设备位于所述 3GPP 网络外。

5、如权利要求 1 或 2 所述的方法，其特征在于，所述 UE 保存有第一配置信息，所述第一配置信息包括用于指示所述认证设备是否位于所述 3GPP 网络外的第二指示信息；

所述 UE 判断所述认证设备是否位于 3GPP 网络外，包括：

所述 UE 根据所述第二指示信息，确定所述认证设备是否位于 3GPP 网络外。

6、如权利要求 1 或 2 所述的方法，其特征在于，所述 UE 判断所述认证设备是否位于 3GPP 网络外，包括：

在所述 UE 获得所述认证设备的标识的情况下，所述 UE 确定所述认证设备位于 3GPP 网络外；

在所述 UE 未获得所述认证设备的标识的情况下，所述 UE 确定所述认证设备位于 3GPP 网络内。

7、如权利要求 1~6 中任一项所述的方法，其特征在于，所述 UE 根据所述 MSK，生成鉴权服务密钥 Kausf，包括：

所述 UE 根据所述 MSK 和生成参数，生成所述 Kausf；

其中，所述生成参数包括以下一项或多项：所述 UE 当前接入的服务网络的标识或所述 UE 的标识。

8、如权利要求 7 所述的方法，其特征在于，所述 UE 的标识包括所述 UE 的第一标识，所述第一标识用于在所述 3GPP 网络外的网络中标识所述 UE。

9、一种密钥推衍方法，其特征在于，所述方法包括：

鉴权服务功能 AUSF 网元向认证设备发送第一触发指示，所述第一触发指示用于触发

认证用户设备 UE；

所述 AUSF 网元接收来自所述认证设备的认证成功消息和第一密钥；所述认证成功消息用于指示所述 UE 被所述认证设备成功认证；

所述 AUSF 网元根据所述第一密钥生成鉴权服务密钥 Kausf；

所述 AUSF 网元向移动管理功能网元发送所述认证成功消息和第三指示信息，所述第三指示信息用于指示所述认证设备位于第三代合作伙伴计划 3GPP 网络外或者所述 3GPP 网络内。

10、如权利要求 9 所述的方法，其特征在于，所述 AUSF 网元根据所述第一密钥生成鉴权服务密钥 Kausf，包括：

所述 AUSF 网元根据所述第一密钥和生成参数，生成所述 Kausf；

其中，所述生成参数包括以下一项或多项：所述 UE 当前接入的服务网络的标识或所述 UE 的标识。

11、如权利要求 10 所述的方法，其特征在于，所述 UE 的标识包括所述 UE 的第一标识，所述第一标识用于在所述 3GPP 网络外的网络中标识所述 UE。

12、如权利要求 9~11 中任一项所述的方法，其特征在于，在所述 AUSF 网元向认证设备发送第一触发指示之前，所述方法还包括：

所述 AUSF 网元确定所述 UE 需要与所述认证设备执行认证。

13、如权利要求 12 所述的方法，其特征在于，所述 AUSF 网元确定所述 UE 需要与所述认证设备执行认证，包括：

所述 AUSF 网元接收来自所述移动管理功能网元的所述 UE 的第二标识；所述第二标识为用户隐藏标识 SUCI 或用户永久标识 SUPI；

所述 AUSF 网元根据所述第二标识，确定所述 UE 需要与所述认证设备执行认证。

14、如权利要求 12 所述的方法，其特征在于，所述 AUSF 网元确定所述 UE 需要与所述认证设备执行认证，包括：

所述 AUSF 网元接收来自所述移动管理功能网元的所述 UE 的第二标识；所述第二标识为用户隐藏标识 SUCI 或用户永久标识 SUPI；

所述 AUSF 网元向统一数据管理 UDM 网元发送第一请求消息，所述第一请求消息包括所述 SUCI 或所述 SUPI；

所述 AUSF 网元接收来自所述 UDM 网元的第一响应消息，所述第一响应消息包括所述认证设备的标识；

所述 AUSF 网元根据所述认证设备的标识，确定所述 UE 需要与所述认证设备执行认证。

15、如权利要求 9~14 中任一项所述的方法，其特征在于，所述方法还包括：

所述 AUSF 网元根据所述 UE 的第二标识，确定所述 UE 的第一标识；所述第一标识用于在所述 3GPP 网络外的网络中标识所述 UE；所述第二标识为 SUCI 或 SUPI；所述第二标识由所述 AUSF 网元从所述移动管理功能网元接收；

所述 AUSF 网元将所述第一标识发送至所述认证设备；所述第一触发指示具体用于触发根据所述第一标识对应的认证凭证认证所述 UE。

16、一种密钥推导方法，其特征在于，所述方法包括：

移动管理功能网元接收来自鉴权服务功能 AUSF 网元的认证成功消息和第三指示信息，所述认证成功消息用于指示用户设备 UE 被认证设备成功认证；所述第三指示信息用于指示所述认证设备位于第三代合作伙伴计划 3GPP 网络外或者所述 3GPP 网络内；

所述移动管理功能网元向所述 UE 发送所述认证成功消息和第一指示信息，所述第一指示信息用于指示所述认证设备位于所述 3GPP 网络外或者所述 3GPP 网络内；所述第一指示信息根据所述第三指示信息确定。

17、如权利要求 16 所述的方法，其特征在于，所述第一指示信息包括防止架构降级 ABBA，所述方法还包括：

所述移动管理功能网元将所述 ABBA 的值确定为非零值；所述 ABBA 的值为非零值的情况下，所述 ABBA 用于指示所述认证设备位于所述 3GPP 网络外。

18、一种密钥推导系统，其特征在于，所述系统包括鉴权服务功能 AUSF 网元和移动管理功能网元；

所述 AUSF 网元，用于向认证设备发送第一触发指示，所述第一触发指示用于触发认证所述 UE；接收来自所述认证设备的认证成功消息和第一密钥；所述认证成功消息用于指示所述 UE 被所述认证设备成功认证；根据所述第一密钥生成鉴权服务密钥 Kausf；向移动管理功能网元发送所述认证成功消息和第三指示信息，所述第三指示信息用于指示所述认证设备位于第三合作伙伴计划 3GPP 网络外或者所述 3GPP 网络内；

移动管理功能网元，用于接收来自所述 AUSF 网元的所述认证成功消息和所述第三指示信息；向所述 UE 发送所述认证成功消息和第一指示信息，所述第一指示信息用于指示所述认证设备位于所述 3GPP 网络外或者所述 3GPP 网络内；所述第一指示信息根据所述第三指示信息确定。

19、如权利要求 18 所述的系统，其特征在于，所述第一指示信息包括防止架构降级 ABBA，所述 ABBA 的值为非零值的情况下，所述 ABBA 用于指示所述认证设备位于所述 3GPP 网络外。

20、如权利要求 18 或 19 所述的系统，其特征在于，

所述 AUSF 网元，具体用于根据所述第一密钥和生成参数，生成所述 Kausf；

其中，所述生成参数包括以下一项或多项：所述 UE 当前接入的服务网络的标识或所述 UE 的标识。

21、如权利要求 20 所述的系统，其特征在于，所述 UE 的标识包括所述 UE 的第一标识，所述第一标识用于在所述 3GPP 网络外的网络中标识所述 UE。

22、如权利要求 18~21 中任一项所述的系统，其特征在于，

所述 AUSF 网元，还用于确定所述 UE 需要与所述认证设备执行认证。

23、如权利要求 22 所述的系统，其特征在于，

所述 AUSF 网元，具体用于接收来自所述移动管理功能网元的所述 UE 的第二标识；所述第二标识为用户隐藏标识 SUCI 或用户永久标识 SUPI；根据所述第二标识，确定所述 UE 需要与所述认证设备执行认证。

24、如权利要求 22 所述的系统，其特征在于，

所述 AUSF 网元，具体用于接收来自所述移动管理功能网元的所述 UE 的第二标识；所述第二标识为用户隐藏标识 SUCI 或用户永久标识 SUPI；向统一数据管理 UDM 网元发送第一请求消息，所述第一请求消息包括所述 SUCI 或所述 SUPI；接收来自所述 UDM 网元的第一响应消息，所述第一响应消息包括所述认证设备的标识；根据所述认证设备的标识，确定所述 UE 需要与所述认证设备执行认证。

25、如权利要求 18~24 中任一项所述的系统，其特征在于，

所述 AUSF 网元，还用于根据所述 UE 的第二标识，确定所述 UE 的第一标识；将所述第一标识发送至所述认证设备；所述第一标识用于在所述 3GPP 网络外的网络中标识所述 UE；所述第二标识为 SUCI 或 SUPI；所述第二标识由所述 AUSF 网元从所述移动管理功能网元接收；所述第一触发指示具体用于触发根据所述第一标识对应的认证凭证认证所述 UE。

26、一种通信装置，其特征在于，所述装置包括处理模块和收发模块，所述处理模块和所述收发模块用于所述装置执行权利要求 1~17 中任一项所述的方法。

27、一种通信装置，其特征在于，所述装置包括：处理器，所述处理器与存储器耦合，所述存储器用于存储程序，当所述程序被所述处理器执行时，使得所述装置执行如权利要求 1~17 中任一项所述的方法。

28、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被执行时使得计算机执行如权利要求 1~17 中任一项所述的方法。