(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 9 月 10 日 (10.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/177768 A1

(51) 国际专利分类号：
H04L 9/32 (2006.01)

(21) 国际申请号： PCT/CN2020/078309

(22) 国际申请日： 2020 年 3 月 6 日 (06.03.2020)

(25) 申请语言： 中文

(26) 公布语言： 中文

(30) 优先权：
201910170883.3 2019年3月7日 (07.03.2019) CN

(71) 申请人：华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]；中国广东省深圳市龙岗区坂田华为总部办公楼，Guangdong 518129 (CN)。

(72) 发明人：胡伟华 (HU, Weihua)；中国广东省深圳市龙岗区坂田华为总部办公楼，Guangdong 518129 (CN)。洪佳楠 (HONG, Jianan)；中国广东省深圳市龙岗区坂田华为总部办公楼，Guangdong 518129 (CN)。

(74) 代理人：北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS)；中国北京市西城区裕民路18号北环中心A座2002，Beijing 100029 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title** NETWORK VERIFICATION METHOD, APPARATUS, AND SYSTEM

(54) **发明名称**：一种网络验证方法、装置及系统

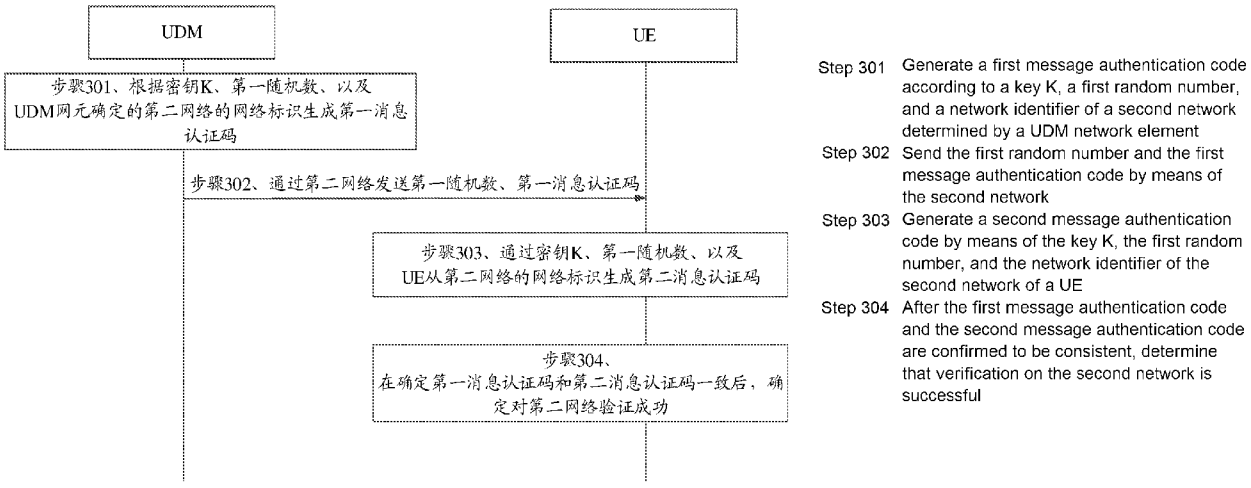

图 3

(57) **Abstract:** **A network verification method, apparatus, and system, used for solving the problem that a terminal device cannot verify a service network while performing two-way authentication with a home network. In the present application, a unified data management network element in a first network generates a first message authentication code according to a key K of the terminal device, a first random number, and a network identifier of a second network; the first random number and the first message authentication code are sentto the terminal device by means of the second network. After receiving the first random number and the first message authentication code, the terminal device generates a second message authentication code by means of a local stored key K, the first random number, and the network identifier of the second network; after the first message authentication code and the second message authentication code are confirmed to be consistent, verification on the second network is successful. The terminal device also completes the verification on the second network while verifying the first network according to the first message authentication code.**

WO 2020/177768 A1

[见续页]

ST ,SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ ,VC, VN, WS ,ZA ,ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护）:ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW ,SD ,SL ,ST ,SZ ,TZ, UG, ZM, ZW) ,欧亚 (AM , AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE ,DK ,EE, ES, FI, FR, GB, GR, HR, HU, IE ,IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT , RO, RS ,SE ,SI ,SK ,SM ,TR) ,OAPI (BF ,BJ ,CF ,CG, Cl, CM ,GA ,GN ,GQ, GW, KM, ML, MR, NE ,SN ,TD ,TG)。

本国际公布 :

- 包括国际检索报告 (条约第21条 (3))。

(57) 摘要 ：一种网络验证方法、装置及系统，用以终端设备在与家乡网络双向认证时，无法对服务网络验证的问题。本申请中，第一网络中的统一数据管理网元根据终端设备的密钥K、第一随机数、以及第二网络的网络标识生成第一消息认证码；并向通过第二网络向终端设备发送第一随机数、第一消息认证码。终端设备接收第一随机数、第一消息认证码之后，通过本地存储的密钥K、第一随机数、以及第二网络的网络标识生成第二消息认证码；在确定第一消息认证码和第二消息认证码一致后，对第二网络验证成功。终端设备在根据第一消息认证码对第一网络进行认证的过程中，同时可以完成对第二网络验证。

一种网络验证方法、装置及系统

相关申请的交叉引用

本申请要求在2019年03月07日提交中国专利局、申请号为201910170883.3、申请名称为“一种网络验证方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种网络验证方法、装置及系统。

背景技术

在移动通信系统中，当终端设备和第一网络签约后，第一网络即为终端设备的家乡网络，家乡网络中保存有终端设备的签约信息，若终端设备移动到第一网络的服务范围之外，例如当前终端设备处于第二网络的服务范围内，此时第二网络就成为服务网络，需要为终端设备提供网络服务。

在第二网络为终端设备提供网络服务之前，第二网络需要获知终端设备的签约信息，为了获取终端设备的签约信息，终端设备需要先与第一网络通过第二网络作为中介进行双向认证，双向认证通过后，第一网络会将终端设备的签约信息发送给第二网络。

但是在上述验证过程中，终端设备并不会对第二网络进行验证，也就是无法识别出第二网络是否为欺骗网络，在双向验证之后，第二网络会获取终端设备的签约信息，导致终端设备的信息泄露。

发明内容

本申请提供一种网络验证方法、装置及系统，用以解决现有技术中终端设备在与家乡网络双向认证时，无法对服务网络验证的问题。

第一方面，本申请实施例提供了一种网络验证方法，该方法可由统一数据管理网元或统一数据管理网元的芯片执行，所述方法包括：第一网络中的统一数据管理网元根据终端设备的密钥K、第一随机数、以及第二网络的网络标识生成第一消息认证码；然后，所述统一数据管理网元向通过第二网络向所述终端设备发送随机数、第一消息认证码。

通过上述方法，所述统一数据管理网元在生成所述第一消息认证码时，采用所述第二网络的网络标识，可以使得所述终端设备在根据所述第一消息认证码对所述第一网络进行认证的过程中，同时可以完成对所述第二网络验证。

在一种可能的设计中，所述第一消息认证码携带在认证令牌中的。

通过上述方法，将所述第一消息认证码携带在认证令牌中，可以保证所述第一消息认证码的安全性。

在一种可能的设计中，所述统一数据管理网元可以直接根据终端设备的密钥K、第一随机数、以及第二网络的网络标识生成第一消息认证码（第一种方式），示例性的，如可以通过预设的运算，根据所述终端设备的密钥K、所述第一随机数、以及所述第二网络的

网络标识生成第一消息认证码；也可以采用其他方式生成第一消息认证码，示例性的，所述统一数据管理网元可以先根据所述第一随机数和所述第二网络的网络标识生成的第二随机数；之后，再根据所述终端设备的密钥 K、所述第二随机数生成第一消息认证码 (第二种方式 X

通过上述方法，所述统一数据管理网元可以采用不同的方式生成所述第一消息认证码，其中第一种方式较为直接，运算简单，可以较好的节省效率；第二种方式能够在不更改现有标准中消息认证码生成算法的前提下，可以实现终端设备对服务网络的验证。

在一种可能的设计中，在所述根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码之前，统一数据管理网元可以接收来自所述第二网络中的网元的终端认证获取请求，所述终端认证获取请求包括力P密后的用户标识；之后，解密所述加密后的用户标识，获得解密后的用户标识；可以根据所述解密后的用户标识，获取所述终端设备的签约数据，其中，所述终端的签约数据中包括所述终端设备的密钥 K。

通过上述方法，所述统一数据管理网元可以通过所述终端设备的用户标识查询到所述终端设备的密钥 K，使得之后可以成功生成所述第一消息认证码，进一步的，保证可以实现所述终端设备对所述第二网络的验证。

第二方面，本申请实施例提供了一种网络验证方法，该方法可由终端设备或终端设备的芯片执行所述方法包括：终端设备通过第二网络接收来自第一网络中的统一数据管理网元的第一随机数、第一消息认证码；之后，所述终端设备根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码；然后，所述终端设备在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

通过上述方法，所述终端设备在生成所述第二消息认证码时，采用所述第二网络的网络标识，可以使得所述终端设备在根据所述第一消息认证码和所述第二消息认证码对所述第一网络进行认证的过程中，同时可以完成对所述第二网络验证。

在一种可能的设计中，所述第一消息认证码携带在认证令牌中的。

通过上述方法，将所述第一消息认证码携带在认证令牌中，可以保证所述第一消息认证码的安全性。

在一种可能的设计中，所述终端设备可以直接根据本地存储的密钥 K、第一随机数、以及第二网络的网络标识生成第二消息认证码 (第一种方式)，示例性的，如可以通过预设的运算，所述本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第一消息认证码；也可以采用其他方式生成第一消息认证码，示例性的，所述终端设备可以先根据第一随机数和所述第二网络的网络标识生成的第二随机数；之后，再根据所述本地存储的密钥 K、所述第二随机数生成第二消息认证码 (第二种方式 X

通过上述方法，所述终端设备可以采用不同的方式生成所述第二消息认证码，其中第一种方式较为直接，运算简单，可以较好的节省效率；第二种方式并不需要更改现有标准中消息认证码生成算法，还保证可以实现终端设备对第二网络的验证。

在一种可能的设计中，所述终端设备通过第二网络接收来自第一网络的随机数、第一消息认证码时，可以从所述第二网络的安全锚功能网元接收携带有所述随机数、第一消息认证码的认证请求，获取所述随机数、第一消息认证码。

通过上述方法，所述终端设备可以方便的获取所述随机数和第一消息认证码，可以保证后续完成对所述第二网络的验证。

第三方面，本申请实施例还提供了一种通信装置，所述通信装置应用于第一网络中的统一数据管理网元，有益效果可以参见第一方面的描述此处不再赘述。该装置具有实现上述第一方面的方法实例中行为的功能。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，所述装置的结构中包括接收单元、处理单元和发送单元，这些单元可以执行上述第一方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不你:赘述。

第四方面，本申请实施例还提供了一种通信装置，所述通信装置应用于终端设备，有益效果可以参见第二方面的描述此处不再赘述。该装置具有实现上述第二方面的方法实例中行为的功能。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，所述装置的结构中包括接收单元、生成单元和验证单元，这些单元可以执行上述第二方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不你:赘述。

第五方面，本申请实施例还提供了一种通信装置，所述通信装置应用于第一网络中的统一数据管理网元，有益效果可以参见第一方面的描述此处不再赘述。所述通信装置的结构中包括处理器和存储器，所述处理器被配置为支持所述基站执行上述第一方面方法中相应的功能。所述存储器与所述处理器耦合，其保存所述通信装置必要的程序指令和数据。所述通信装置的结构中还包括通信接口，用于与其他设备进行通信。

第六方面，本申请实施例还提供了一种通信装置，所述通信装置应用于终端设备，有益效果可以参见第二方面的描述此处不再赘述。所述通信装置的结构中包括处理器和存储器，所述处理器被配置为支持所述基站执行上述第二方面方法中相应的功能。所述存储器与所述处理器耦合，其保存所述通信装置必要的程序指令和数据。所述通信装置的结构中还包括收发机，用于与其他设备进行通信。

第七方面，本申请实施例还提供了一种通信系统，有益效果可以参见第一方面和第二方面的描述此处不再赘述。所述系统包括第一网络中的统一数据管理网元和第一网络中的认证服务功能网元；

其中，所述认证服务功能网元，用于接收来自第二网络中安全锚功能网元的认证鉴定请求；所述认证鉴定请求中包括来自终端设备的加密后的用户标识；向所述统一数据管理网元发送终端认证获取请求，所述终端认证获取请求包括所述加密后的用户标识；

所述统一数据管理网元，用于接收所述终端认证获取请求；解密所述加密后的用户标识，得到解密后的用户标识；根据所述解密后的用户标识，获取所述终端设备对应的签约数据，其中，所述终端设备对应的签约数据中包括所述终端设备的密钥K；根据所述终端设备的密钥K、第一随机数、以及所述第二网络的网络标识生成第一消息认证码；以及通过所述第二网络向所述终端设备发送所述第一随机数和所述第一消息认证码。

在一种可能的设计中，所述第一消息认证码携带在认证令牌中。

在一种可能的设计中，所述统一数据管理网元在根据终端设备的密钥K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码时，可以直接根据所述终端设备的密钥K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码，也可以采用其他方式生成所述第一消息认证码，示例性的，可以先根据所述第一随机数和所述第二网络的网络标识生成第二随机数；之后根据所述终端设备的密钥K和所述第二随机数生成所述第一消息认证码。

在一种可能的设计中，所述系统还可以包括所述第二网络的安全锚功能网元；所述安全锚功能网元可以从所述终端设备接收注册请求，所述注册请求中包括所述加密的用户标识；还可以向所述认证服务功能网元发送所述认证鉴定请求；还可以通过所述认证服务功能网元接收来自所述统一数据管理网元的所述第一随机数和所述第一消息认证码，以及向所述终端设备发送认证请求，所述认证请求中包括所述第一随机数和所述第一消息认证码。

第八方面，本申请还提供一种计算机可读存储介质，所述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，使得计算机执行上述各方面所述的方法。

第九方面，本申请还提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述各方面所述的方法。

第十方面，本申请还提供一种计算机芯片，所述芯片与存储器相连，所述芯片用于读取并执行所述存储器中存储的软件程序，执行上述各方面所述的方法。

附图说明

图 1A 为本申请提供的一种网络系统架构示意图；

图 1B 为本申请提供的一种终端设备的结构示意图；

图 2 为现有技术中 UE 与家乡网络双向认证的方法示意图；

图 3 为本申请提供的一种网络验证方法的示意图；

图 4 为本申请提供的一种网络验证方法的示意图；

图 5 为本申请提供的一种网络验证方法的示意图；

图 6 为本申请提供的一种网络验证方法的示意图；

图 7~10 为本申请提供的一种通信装置的结构示意图。

具体实施方式

为了使本申请实施例的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施例作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。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。

参阅图 1A 所示，为本申请适用的一种可能的网络架构示意图。该网络架构为 5G 网络架构。该 5G 架构中的网元包括用户设备，图 1A 中以终端设备为 UE 为例。网络架构还包括无线接入网（radio access network，RAN）、接入和移动性控制功能（access and mobility function，AMF）、统一数据管理（unified data management，UDM）、认证服务功能（authentication server function，AUSF）、安全锚功能（security anchor function，SEAF）等。

所述 RAN 的主要功能是控制用户通过无线接入到移动通信网络。RAN 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，或任何远程控制机），并提供与其核心网的连接。

所述 AMF 网元负责终端的接入管理和移动性管理，如注册管理，连接管理，移动管理，可达性管理等；在实际应用中，其包括了 LTE 中网络框架中移动性管理实体（mobility management entity，MME）里的移动性管理功能，并加入了接入管理功能。

所述 SEAF 网元用于完成对 UE 的认证 ,在 5G 中 ,SEAF 的功能可以合并到 AMF 中。

所述 AUSF 网元具有鉴权服务功能，用于终结所述 SEAF 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 SEAF。

所述 UDM 网元可存储用户的签约信息，生成认证参数等。

所述 ARPF 网元具有认证凭证存储和处理功能，用于存储用户的长期认证凭证，如永久密钥 K 等。在 5G 中，所述 ARPF 网元的功能可以合并到 UDM 网元中。

本申请中的终端设备，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。

如图 1B 所示，为本申请实施例提供的一种 UE 的结构示意图，其中，UE 包括两种模块，分别为通用用户身份模块（universal subscriber identity module，USIM）和移动设备（mobile equipment，ME）模块。

所述 USIM 可以是 UE 中的 SIM 卡，可以存储一些较为重要的 UE 的签约信息，如在本申请实施例中所述 UE 与所述家乡网络签约所约定的密钥 K，所述 USIM 还可以执行一些参数计算，在本申请实施例中可以实现第一消息认证码生成。

所述 ME 模块可以统指所述 UE 中除所述 USIM 外的硬件构成以及软件程序。所述 ME 模块中通常不会存储安全要求高的 UE 的签约信息 ,所述 ME 模块可以提供一些辅助功能，其中包括 :实现所述 UISM 与网络侧之间的信息转发、利用所述 USIM 输出的参数生成 RES*、生成 K_{AUSF}，在本申请实施例中，所述 ME 还可以实现第二随机数的生成。

其中，图 1A 的架构中，与本申请有关的网元主要是：所述 UE、所述 AUSF 网元、所述 UDM 网元以及所述 SEAF 网元。

在本申请实施例中，所述 SEAF 网元和所述 AUSF 网元位于不同的网络中，例如，所述 SEAF 网元位于服务网络（serving network）中，在漫游场景下，所述 SEAF 网元位于拜访公共陆地移动网（visited public land mobile network，VPLMN）中，所述 AUSF 网元位于家乡网络（home network）中，若所述 UE 在所述家乡网络的覆盖范围之外则无法直接接入所述家乡网络获取服务。

若所述 UE 在家乡网络的覆盖范围之外，在所述服务网络的覆盖范围之内，所述 UE 为了能够获取所述服务网络提供的网络服务，则需要接入所述服务网络；由于所述服务网络并未与所述 UE 签约，所述 UE 为了可以获取所述服务网络的网络服务，所述服务网络需要对所述 UE 进行验证，所述家乡网络和所述 UE 需要进行双向认证。

如图 2 所示为基于如图 1A 所示的系统框架中，现有的双向认证的方法示意图。

步骤 201: 所述 UE 将加密后的用户标识携带在注册请求中发送给所述 SEAF 网元。

示例性的，所述 UE 可以对签约固定标识（subscription permanent identifier，SUPI）进行加密生成签约隐藏标识（subscription concealed identifier，SUCI），所述 UE 将 SUCI 携带

在注册请求中发送给所述 SEAF 网元。

一种可能的实现方式中，所述 UE 使用配置的公钥对用户标识进行加密，得到加密后的用户标识。可选的，当网络存在多个公私钥对时，所述 UE 在加密用户标识时，可以指示网络自己使用了哪一个公钥对用户标识进行了加密，以便于网络根据所述 UE 的指示选择对应的私钥进行解密。例如所述 UE 还将用于解密该加密后的用户标识的密钥标识符和所述加密后的用户标识一起携带在注册请求中发送给所述 SEAF 网元。

步骤 202: 为了从家乡网络中获取所述 UE 的认证向量和用户标识，所述 SEAF 网元将加密后的用户标识携带在认证鉴定请求中，发送给所述家乡网络中的 AUSF 网元。

可选的，所述认证鉴定请求中还携带有所述密钥标识符。

步骤 203: 所述 AUSF 网元将加密后的用户标识携带在 UE 认证获取请求中，发送给所述 UDM 网元。

可选的，所述 UE 认证获取请求中还携带有所述密钥标识符。

步骤 204: 所述 UDM 网元对加密后的用户标识进行解密获取用户标识，所述 UDM 网元才根据用户标识查询该用户标识对应的 UE 的签约信息。

可选的，当所述 UE 认证获取请求中携带有密钥标识符时，所述 UDM 网元根据所述密钥标识符获取解密密钥，并使用所述解密密钥解密所述加密后的用户标识，得到解密后用户标识。

步骤 205: 所述 UDM 网元根据所述 UE 的签约信息生成认证向量，其中所述认证向量包括多个参数，其中包括消息认证码（message authentication code, MAC），RAND, 期望的挑战回复（eXpected RESponse，XRES*）、K_{AUSF}。

示例性的，MAC 可以携带在认证令牌（authentication token, AUTN），也就是说，所述认证向量可以包括 RAND、携带有 MAC 的 AUTN、XRES*、K_{AUSF}; AUTN 携带 MAC 的方式可参见现有 AUTN 的生成方式。

所述认证向量中的 RAND 是所述 UDM 网元随机生成的；对于所述认证向量中的其他参数，所述 UDM 网元可以根据所述 UE 签约信息中所述 UE 的密钥 K 以及 RAND, 通过不同运算生成 MAC、XRES* 以及 K_{ausf}。

也就是说，所述 UDM 网元在生成 MAC、XRES* 以及 K_{AUS} 均需要基于所述 UE 的密钥 K 和 RAND, 但运算方式不同。

例如，所述 UDM 网元根据所述 UE 的密钥 K、所述 RAND 以及消息认证码生成算法，确定消息认证码 MAC。

MAC 用于所述 UE 对所述家乡网络的认证，XRES* 用于家乡网络对 UE 的认证，K_{AUSF} 是所述 UE 和所述 AUSF 网元之间同步的派生密钥，用于派生锚点密钥 K_{seaf}。

步骤 206: 所述 UDM 网元向所述 AUSF 网元发送认证获取响应，所述认证获取响应中包括所述认证向量和所述用户标识。

步骤 207: 所述 AUSF 网元对所述认证向量进行进一步处理，例如对 XRES* 进行哈希运算，生成 HXRES*，根据 K_{AUSF} 进行推演生成 K_{SEAF}，处理后的认证向量包括 RAND、MAC、HXRES*，其中，MAC 可以携带在 AUTN, 也就是说，所述处理后的认证向量包括 RAND、携带有 MAC 的 AUTN。

步骤 208: 所述 AUSF 网元向所述 SEAF 网元发送认证鉴定响应，所述认证鉴定响应

中携带有所述处理后的认证向量。

步骤 209: 所述 SEAF 网元向所述 UE 发送认证请求，其中，所述认证请求中携带处理后的认证向量中的部分参数，该部分参数包括 RAND、MAC, 其中，MAC 可以携带在 AUTN 中。

步骤 210: 所述 UE 根据所述 UE 中的 USIM 中存储的密钥 K 与从所述 SEAF 网元接收的 RAND 生成 XMAC, 这里所述 UE 生成 XMAC 所采用的运算方式与所述 UDM 网元生成 MAC 所采用的运算方式相同。

所述 UE 对 XMAC 和 AUTN 中携带的 MAC 的比对实现所述 UE 对所述家乡网络的认证。若 XMAC 和 AUTN 中的 MAC 一致，则认证成功，否则认证失败。

在认证成功后，所述 UE 根据 RAND 和 K 生成 RES*，这里所述 UE 生成 RES*所采用的运算方式与所述 UDM 网元生成 XRES*所采用的运算方式相同。

步骤 211: 所述 UE 将 RES* 包含在认证响应中，发送给所述 SEAF 网元。

步骤 212: 所述 SEAF 网元对所述认证响应中包括的 RES*进行哈希运算，生成 HRES*，将 HRES*与所述 AUSF 网元发送的认证向量中的 HXRES*进行比对，通过 HRES*与的 HXRES* 的比对完成所述服务网络对所述 UE 的认证，若 HRES*与的 HXRES*一致，则所述服务网络对所述 UE 认证成功，否则认证失败。

步骤 213: 在所述服务网络对所述 UE 认证成功之后，所述 SEAF 网元将所述 UE 返回的 RES*转发给所述 AUSF 网元，由所述 AUSF 网元进行下一步的认证。

步骤 214: 所述 AUSF 网元接收到 RES*后，将 RES*与所述认证向量中的 XRES*进行比对，结果若一致，则完成所述家乡网络对所述 UE 的认证。

步骤 215: 所述 AUSF 网元在认证成功之后，会将用户标识和 K_{SEAF} 发送给所述 SEAF 网元。

由上述内容可以才看出，所述 UE 在接入所述服务网络后，仅是所述 UE 与所述家乡网络之间存在双向认证，也即所述 UE 对所述家乡网络的认证和所述家乡网络对所述 UE 的认证，而所述 UE 并不会对服务网络进行验证，也无法识别所述服务网络是否为欺骗网络。

为了在所述 UE 与所述家乡网络进行双向认证的过程中同时完成对所述服务网络的验证，本申请提出了一种网络验证方法，在本申请实施例中，所述家乡网络中的统一数据管理网元在生成认证向量时，认证向量中的消息认证码 (在本申请实施例中对应了第一消息认证码) 的生成过程中利用所述统一数据管理网元确定的服务网络的网络标识；所述 UE 在对所述家乡网络认证时，也需要结合所述服务网络发送给所述 UE 的网络标识生成消息认证码 (在本申请实施例中对应了第二消息认证码), 与来自所述家乡网络中的统一数据管理网元的消息认证码进行比对，以完成所述 UE 对所述家乡网络的验证，也就是说，在所述 UE 对所述家乡网络认证的过程中，涉及到所述服务网络的网络标识的验证，采用本申请实施例的方式既可以实现对所述家乡网络的验证，同时也可以验证所述服务网络是否为欺骗网络。

具体的，本申请实施例提供的网络验证方法，以可以分为两种方式：

方式一、所述家乡网络中的统一数据管理网元在生成第一消息认证码时直接利用了所述统一数据管理网元确定的服务网络的网络标识，相应的，所述 UE 在生成第二消息认证码时直接利用了所述 UE 从所述服务网络接收的服务网络的网络标识。

方式二、所述家乡网络中的统一数据管理网元在生成第一消息认证码时，先基于第一随机数和所述统一数据管理网元确定的服务网络的网络标识生成第二随机数，之后，根据所述第二随机数生成所述第一消息认证码，相应的，所述 UE 在生成第二消息认证码时，先基于第一随机数和所述 UE 从服务网络接收的网络标识生成第二随机数，之后，根据所述第二随机数生成所述第二消息认证码。

上述两种实现方式，相比于现有技术，本申请实施例中，所述 UDM 网元或者所述 UE 在生成消息认证码 MAC 时，都引入了服务网络的网络标识这一新的输入参数，使得所述 UE 在验证家乡网络的时候，也能够同步实现对服务网络的验证。

下面对这两种方式分别进行介绍：

方式一、消息认证码是直接基于服务网络的网络标识生成的。

如图 3 所示，以第一网络为 UE 的家乡网络，第二网络是 UE 当前所连接的服务网络，统一数据管理网元为 UDM 网元、认证服务功能网元为 AUSF 网元、安全锚功能网元为 SEAF 网元为例，对本申请实施例提供的一种网络验证方法中的方式一进行介绍，该方法包括：

步骤 301: 所述第一网络中的 UDM 网元根据所述 UE 的密钥 K、第一随机数、以及第二网络的网络标识生成第一消息认证码。

示例性的，所述 UDM 网元可以基于第一运算，根据所述 UE 的密钥 K、第一随机数、以及第二网络的网络标识生成第一消息认证码。

作为一种可能的实施方式，在步骤 301 之前，所述 UDM 网元可以接收来自所述第一网络中的 AUSF 网元的 UE 认证获取请求之后，可以生成所述第一随机数。

所述 AUSF 网元在接收到所述第二网络中的 SEAF 发送的携带所述 UE 用户标识的认证鉴定请求后，所述 AUSF 网元向所述 UDM 网元发送携带有所述加密后的用户标识的 UE 认证获取请求，以请求所述 UDM 网元生成的认证向量；所述 UDM 网元在接收到所述 UE 认证获取请求确定后续需要对 UE 进行认证，采用随机生成的方式生成所述随机数。

需要说明的是，所述 UE 认证获取请求中可以携带加密后的用户标识，也可以携带不加密后的用户标识 (本申请中用所述 UE 的用户标识表示不加密的用户标识或解密后的用户标识)，如在所述 UE 首次接入所述第二网络的情况下，可以携带加密后的用户标识，在所述 UE 非首次接入所述第二网络的情况下，可以携带不加密的用户标识，在本申请实施例中以所述 UE 认证获取请求中携带有加密后的用户标识为例进行说明。对于所述 UE 认证获取请求中携带所述 UE 的用户标识的情况，所述 UDM 网元可以省略解密过程，执行之后的操作。

一种可能的实现方式中，所述 UE 认证获取请求中包括加密后的用户标识。所述 UDM 获取默认的私钥对所述加密后的用户标识进行解密，获得解密后的用户标识。

另一种可能的实现方式中，所述 UE 认证获取请求中包括加密后的用户标识和用于解密所述加密后的用户标识的密钥对应的密钥标识符。所述 UDM 网元根据所述密钥标识符获取解密密钥，并使用所述解密密钥对所述加密后的用户标识进行解密，获得解密后的用户标识。

所述 UDM 网元在获取所述 UE 的用户标识后，可以根据所述 UE 的用户标识获取所述 UE 的签约信息，并从所述 UE 的签约信息中确定与所述 UE 在签约时约定的密钥 K，执行步骤 301。

在步骤 301 中，区别于现有技术，所述 UDM 网元在生成消息认证码时，会结合所述

第二网络的网络标识。

所述 UDM 网元获取所述第二网络的网络标识的方式本申请实施例并不限定，所述第二网络的网络标识可以是所述第二网络中的核心网网元，如所述 SEAF 网元发送给所述 UDM 网元的，也可以是所述 AUSF 网元在获取了所述第二网络的网络标识之后，发送给所述 UDM 网元的。

所述 AUSF 网元可以将所述第二网络的网络标识携带在需要发送给所述 UDM 网元的信息中，将所述第二网络的网络标识发送给所述 UDM 网元，所述需要发送给所述 UDM 网元的信息可以是所述 UE 认证获取请求，也可以其他信息，本申请实施例并不限定。

需要说明的是，所述 AUSF 网元获取所述第二网络的网络标识的方式本申请实施例并不限定，所述第二网络的网络标识可以是所述第二网络中的核心网网元，如所述 SEAF 网元发送给所述 AUSF 网元，也可以是所述 AUSF 网元通过与所述第二网络中的核心网网元，如所述 SEAF 网元通信的信息通道确定所述第二网络，进而确定所述第二网络的网络标识。

所述第二网络的网络标识用于标识所述第二网络，具体的，所述第二网络的网络标识可以是统一分配的序列号，也可以是可路由网络地址，还可以是如域名形式标识的网络名，本申请实施例并不限定所述第二网络的网络标识的形式，凡是可以标识所述第二网络的标识均适用于本申请实施例。

在步骤 301 中，所述 UDM 网元生成所述第一消息认证码时，所采用的第一运算可以是将所述 UE 的密钥 K、所述第一随机数、以及所述第二网络的网络标识作为输入参数获取消息验证码的运算方式，该第一运算相比于现有的消息认证码生成算法（如步骤 205 所述的消息认证码算法），至少多了一个输入参数“第二网络的网络标识”，本申请实施例中并不限定所述第一运算的具体类型，且在基于所述第一运算生成所述第一消息认证码时，还可以结合其他参数，例如可以结合匿名化序列号（sequence number, SQN），认证管理域（authentication management field, AMF）等，本申请实施例并不限定。

在生成了所述第一消息认证码后，可以将所述第一消息认证码携带在认证令牌中，也就是说，所述 UDM 网元在构造所述认证令牌时，将所述第一消息认证码作为所述认证令牌中的一部分。

步骤 302: 所述 UDM 网元通过第二网络向所述 UE 发送所述第一随机数、第一消息认证码。

所述 UDM 网元在生成了所述第一消息认证码之后，可以将所述第一随机数和所述第一消息认证码发送给所述 UE, 示例性的，所述 UDM 网元可以生成认证向量，所述认证向量中包括所述第一随机数和所述认证令牌，所述认证令牌中携带所述第一消息认证码，所述 UDM 网元将所述认证向量中的第一随机数和认证令牌通过所述第二网络中的 SEAF 网元发送给所述 UE。

作为一种可能的实施方式，所述 UDM 网元可以通过所述第二网络的 SEAF 网元将所述认证向量中的第一随机数和认证令牌发送给所述 UE; 具体的，所述 UDM 网元可以先将所述认证向量发送给所述第一网络中的 AUSF 网元中，之后，再由所述第一网络中的 AUSF 网元将所述第一随机数和所述第一消息认证码发送给所述第二网络的 SEAF 网元。

当所述 SEAF 网元接收到所述认证向量后，可以获取所述认证向量中的第一随机数和认证令牌，将所述第一随机数和所述认证令牌发送给所述 UE。

应需理解的是，所述认证向量还可以包括其他参数，如 XRES* 、K_{ausf} ，所述第一网

络中的AUSF网元在接收到所述认证向量后，可以对所述认证向量进一步处理，具体可以参见步骤207中的相关描述，此处不再赘述。

步骤303：所述UE通过第二网络接收所述第一随机数、所述第一消息认证码后，根据本地存储的密钥K、第一随机数、以及所述第二网络的网络标识生成第二消息认证码。

示例性的，所述UE可以采用与所述UDM网元侧相同的方式生成所述第二消息认证码，所述UE基于所述第一运算，通过本地存储的密钥K、第一随机数、以及所述第二网络的网络标识生成第二消息认证码。

所述UE在生成所述第二消息认证码之前，需要先确定所述第二网络的网络标识，所述UE确定所述第二网络的网络标识的方式本申请实施例并不限定，例如可以是基站通过广播消息，将所述第二网络的网络标识发送给所述UE的，又例如所述第二网络的网络标识可以是所述第二网络中的SEAF网元发送给所述UE的。

所述UE与所述第一网络签约时，会约定密钥K，所述密钥K保存在所述UE的签约信息中，同时所述密钥K也会存储在所述UE本地。

所述UE采用与所述UDM网元中生成所述第一消息认证码相同的方式生成所述第二消息认证码，所述UE基于相同的所述第一运算，通过本地存储的密钥K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码。

步骤304：所述UE在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

所述UE在生成所述第二消息认证码后，可以与接收到所述第一消息认证码进行比对。若所述第一消息认证码和所述第二消息认证码一致，则说明所述UDM网元在生成所述第一消息认证码采用的第二网络的网络标识与所述UE在生成所述第二消息认证码采用的第二网络的网络标识相同，所述UE接收到所述第二网络的网络标识为真实的网络标识，所述第二网络不是欺骗网络，对所述第二网络验证成功。

若所述第一消息认证码和所述第二消息认证码不一致，则对所述第一网络或者是说第二网络验证不成功。

方式二、消息认证码是基于由服务网络的网络标识确定的随机数生成的。

如图4所示，以所述第一网络为所述UE的家乡网络，所述第二网络是所述UE当前所连接的服务网络，统一数据管理网元为UDM网元、认证服务功能网元为AUSF网元、安全锚功能网元为SEAF网元为例，对本申请实施例提供的一种网络验证方法中的方式二进行介绍，该方法包括：

步骤401：所述UDM网元根据所述第一随机数和所述第二网络的网络标识生成第二随机数。

示例性的，所述UDM网元可以基于第二运算，根据所述第一随机数、以及第二网络的网络标识生成第一消息认证码。

在如图4所示的实施例中，所述第二运算为将所述第一随机数、以及所述第二网络的网络标识作为输入参数的以获取一个新的随机数的运算方式，本申请实施例中并不限定所述第一运算的具体类型，所述UDM网元确定所述第二网络的网络标识的方式与如图3所示的实施例中所述UDM网元确定所述第二网络的网络标识的方法相同，具体可参见如图3所示的实施例中的相关描述，此处不再赘述。

作为一种可能的实施方式，在步骤401之前，所述UDM网元可以接收来自所述第一

网络中的 AUSF 网元的 UE 认证获取请求之后，可以生成所述第一随机数。关于所述 UE 认证获取请求的说明、以及所述 UDM 网元对所述加密后的用户标识，进行解密，并获取所述 UE 的密钥 K 的说明可以参见步骤 301 中的相关描述，此处不再赘述。

步骤 402: 所述 UDM 网元根据所述 UE 的密钥 K、所述第二随机数生成第一消息认证码。

示例性的，所述 UDM 网元可以基于第三运算，根据所述 UE 的密钥 K、所述第二随机数生成第一消息认证码。

所述 UDM 网元在生成所述第二随机数后，基于所述第二运算生成所述第一消息认证码，在步骤 402 中，所述 UDM 网元生成所述第一消息认证码时，所采用的所述第二运算可以是将所述 UE 的密钥 K、所述第二随机数、以及所述 UDM 网元确定的所述第二网络的网络标识作为输入参数获取消息认证码的运算方式，该第三运算可以和现有的消息认证码生成算法相同。本申请实施例中并不限定所述第三运算的具体类型，且在基于所述第三运算生成所述第一消息认证码时，还可以结合其他参数，例如可以结合 SQN、AMF 等，本申请实施例并不限定。在生成了所述第一消息认证码后，可以将所述第一消息认证码携带在认证令牌中，也就是说，所述 UDM 网元在构造所述认证令牌时，将所述第一消息认证码作为所述认证令牌中的一那分。

步骤 403: 所述 UDM 网元通过第二网络向所述 UE 发送所述第一随机数、所述第一消息认证码。

所述 UDM 网元通过第二网络向所述 UE 发送第一随机数、第一消息认证码与如图 3 所述的实施例中所述 UDM 网元向通过第二网络向所述 UE 发送随机数、第一消息认证码的方式相同，此处不再赘述。

步骤 404: 所述 UE 通过第二网络接收所述第一随机数、第一消息认证码后，根据所述第一随机数和所述第二网络的网络标识生成第二随机数，示例性的，所述 UE 可以基于所述第一运算，生成第二随机数。

步骤 405: 所述 UE 根据本地存储的密钥 K、第二随机数生成第二消息认证码，示例性的，所述 UE 可以基于所述第三运算，生成第二消息认证码。

所述 UE 在生成所述第二消息认证码之前，需要先确定所述第二网络的网络标识，所述 UE 确定所述第二网络的网络标识可参见如图 3 所示的实施例中的相关描述，此处不再赘述。

所述 UE 在接收到所述第一随机数后，可以采用与所述第一网络中的 UDM 网元中生成所述第一消息认证码相同的方式生成所述第二消息认证码，所述 UE 首先基于相同的所述第一运算，通过所述第一随机数、以及所述 UE 从所述第二网络接收的所述第二网络的网络标识生成所述第二随机数；之后基于相同的所述第二运算，通过本地存储的密钥 K、第二随机数生成第二消息认证码。

所述密钥 K 的描述可参见如图 3 所示的实施例中的相关描述，此处不再赘述。

步骤 406: 所述 UE 在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

所述 UE 在生成所述第二消息认证码后，可以与接收到所述第一消息认证码进行比对。

若所述第一消息认证码和所述第二消息认证码一致，则说明所述 UDM 网元在生成所述第一消息认证码采用的第二随机数与所述 UE 在生成所述第二消息认证码采用的第二随

机数相同，进一步的可以说明，所述 UDM 网元在生成所述第二随机数采用的第二网络的网络标识与所述 UE 在生成所述第二随机数采用的第二网络的网络标识相同，所述 UE 接收到所述第二网络的网络标识为真实的网络标识，所述第二网络不是欺骗网络，对所述第二网络验证成功。

若所述第一消息认证码和所述第二消息认证码不一致，则说明所述 UDM 网元在生成所述第一消息认证码采用的第二随机数与所述 UE 在生成所述第二消息认证码采用的第二随机数不同，进一步的可以说明，所述 UDM 网元在生成所述第二随机数采用的第二网络的网络标识与所述 UE 在生成所述第二随机数采用的第二网络的网络标识不同，所述 UE 接收到所述第二网络的网络标识不是真实的网络标识，所述第二网络是欺骗网络，对所述第二网络验证不成功。

相比于图 3 所示实施例，本申请实施例可以在不更改现有标准中消息认证码生成算法的前提下，实现 UE 对服务网络的验证；从图 2 所示的实施例，可以看出现有的消息认证码是根据所述 UE 的密钥 K 和 RAND 生成的，当采用如图 4 所示的实施例中，可以不更改生成消息认证码 (对应图 4 中的第一消息认证码和第二消息认证码) 的生成算法，不需要更改用于生成消息认证码的参数数量，只需将现有的消息认证码生成方式中的 RAND 更新为第二随机数即可，也就是说，仍可以沿用现有的消息认证码的生成算法，使得生成消息认证码的方式更为方便、高效。

下面将如图 3、4 所示的实施例应用于具体场景，对本申请实施例提供的网络认证方法，进行进一步介绍：

在本申请实施例中涉及两种服务网络的网络标识 (serving network name，SNN)，分别为所述家乡网络确定的服务网络的网络标识 (如所述家乡网络中的 UDM 网元确定的服务网络的网络标识) 和所述 UE 从服务网络接收的服务网络的网络标识，为了便于说明，用第一 SNN 和第二 SNN 进行区分，其中，所述第一 SNN 为所述家乡网络确定的服务网络的网络标识，所述第二 SNN 为所述 UE 从所述服务网络接收的服务网络的网络标识。

一般来说，第一 SNN 为所述服务网络的真实的网络标识，而所述服务网络发送给终端设备的第二 SNN，并不一定是真实网络标识，所述服务网络有可能通过发送假的网络标识给终端设备，欺骗所述终端设备，获取所述终端设备的相关信息，在本申请实施例中可以通过第一 SNN 和第二 SNN 是否一致来验证所述服务网络是否为欺骗网络。

如图 5 所示，为本申请实施例提供的一种网络认证方法，该方法包括：

步骤 501: 同步骤 201~204，具体可参见如图 2 所示的步骤 201~204 的相关说明，此处不再赘述。

需要说明的是，本申请实施例中并不限定所述家乡网络中的 UDM 网元确定所述第一 SNN 的方式，例在所述服务网络中的 SEAF 网元在所述家乡网络中的 AUSF 网元发送加密后的用户标识时，所述网元可以同时发送所述第一 SNN，所述 AUSF 网元获取所述第一 SNN；所述 AUSF 网元在转发加密后的用户标识时，也会将所述第一 SNN 发送给所述 UDM 网元；又例如，所述 AUSF 网元可以根据与所述 SEAF 网元交互的通道，确定该通道对应的服务网络，进而确定第一 SNN，之后，在向所述 UDM 网元发送加密后的用户标识时，同时发送所述第一 SNN，在本申请实施例中，凡是可以使所述 UDM 网元接收到所述第一 SNN 的方式均适用于本申请实施例。

步骤 502: 所述 UDM 网元生成第一认证向量，其中所述第一认证向量包括 RAND、

XRES*、K_{AUSF}、第一消息认证码 MAC*，其中 MAC 携带在 AUTN 中。

其中，RAND、XRES*、K_{AUSF}可以采用现有的生成方式，此处不再详述。

对于 MAC*，所述 UDM 网元基于所述第一运算，根据所述 UE 签约信息中的密钥 K、RAND、第一 SNN 生成 MAC*。

下面列举一种第一认证向量中各个参数的生成方式：

所述 UDM 网元生成 RAND 后，通过如下方式生成 MAC*、XRES*、K_{AUSF}：

MAC* = f_1(K，RAND，第一 SNN)，XRES* = f_2(K，RAND，第一 SNN)，K_{AUSF} = f_3(K，RAND)，其中，f_1、f_2、f_3分别表示一种运算方式。

步骤 503：所述 UDM 网元在生成了所述第一认证向量之后，将所述第一认证向量发送给所述 AUSF 网元，示例性的，所述 UDM 网元将携带有所述第一认证向量携带在认证获取响应发送给所述 AUSF 网元。

步骤 504：所述 AUSF 网元在接收到所述第一认证向量后，对所述第一认证向量进行进一步处理，生成第二认证向量。

其中，所述第二认证向量中包括 RAND、HXRES*、MAC*，MAC*携带在 AUTN 中。

HXRES*的生成方式参见步骤 207 中的相关描述，此处不再赘述。

可选的，所述 AUSF 网元还可以根据 K_{AUSF}进行推演生成 K_{seaf}，并在本地保存 KSEAF 以便后续发送给所述 SEAF 网元。

步骤 505：所述 AUSF 网元向所述服务网络中的 SEAF 网元发送所述第二认证向量。

所述 AUSF 可以向所述服务网络中的 SEAF 网元发送携带有所述第二认证向量的认证鉴定响应。

步骤 506：所述 SEAF 网元在接收到所述第二认证向量后，向所述 UE 发送非接入层(non-access stratum,NAS)消息(如认证请求)，所述 NAS 消息中包括 RAND，MAC*，MAC*可以携带在 AUTN 中。

步骤 507：所述 UE 接收到所述 NAS 消息后，基于所述第一运算，通过所述 USIM 中存储的密钥 K、RAND、所述第二 SNN 生成第二消息认证码 XMAC*。

其中，所述第二 SNN 是所述 UE 在接入服务网络后，所述服务网络发送给所述 UE 的服务网络的网络标识，本申请实施例并不限定所述第二 SNN 发送给 UE 的方式，凡是可以使所述 UE 接收到所述第二 SNN 的方式均适用于本申请实施例。

步骤 508：所述 UE 在确定 XMAC*与 AUTN 中携带的 MAC*一致后，向所述 SEAF 网元发送携带有 RES*的认证响应。

其中，RES*的生成方式可以参见步骤 210 中的相关描述，此处不再赘述。

需要说明的是，所述 UE 进行 XMAC*和 MAC*的对比的操作可以是 UE 中的 USIM 模块执行的，可以是 ME 模块本申请实施例并不限定。

若所述 UDM 网元在生成认证令牌时采用如步骤 502 中列举的方式，下面对所述 UE 进行 XMAC*和 MAC*的对比的方式进行详细介绍：

首先，所述 UE 采用与所述 UDM 网元生成 MAC*的相同的方式生成 XMAC*，也即 XMAC* = f_1(K，RAND,第二 SNN)。

所述 UE 可以采用与所述 UDM 网元生成 XRES*的相同的方式生成 RES*，也即 RES* = f_2(K，RAND，第二 SNN)。

所述 UE 在生成 XMAC*后，对 XMAC*和 AUTN*中的 MAC*进行对比，若一致，则

说明在所述 UE 生成 XMAC* 时使用的所述第一 SNN 和所述 UDM 网元生成 MAC* 时使用的所述第二 SNN 相同，所述服务网络不是欺骗网络，所述 UE 对服务网络验证成功；若不一致，则说明所述服务网络为欺骗网络，所述 UE 对所述服务网络验证失败。

若所述 UE 对服务网络验证失败，所述 UE 可以向 SEAF 网元发送用于指示验证失败的消息。

步骤 509: 同步骤 212～步骤 215，此处不再赘述，实现所述服务网络对 UE 进行认证，所述家乡网络对 UE 进行认证。

如图 6 所示，为本申请实施例提供的另一种网络认证方法，该方法包括：

步骤 601: 同步骤 501。

步骤 602: 所述 UDM 网元生成第一认证向量，其中所述第一认证向量包括第一 RAND、XRES*、K_{AUSF}、第一消息认证码 (MAC* X

其中，MAC* 可以携带在 AUTN 中，第一 RAND 是所述 UDM 网元随机生成的随机数。

所述 UDM 网元生成 MAC* 的过程如下：所述 UDM 网元先基于所述第二运算，根据所述第一 RAND 和所述第一 SNN 生成第二 RAND，之后，再基于所述第三运算，根据所述 UE 签约信息中的密钥 K 与所述第二 RAND 生成 MAC*。

XRES*、K_{AUSF} 的生成方式可以与现有的生成方式相同，也即通过对应的运算方式，根据第一 RAND 和密钥 K 生成，也可以通过对应的运算方式，根据所述第二 RAND 和密钥 K 生成，本申请实施例并不限定。

下面列举一种第一认证向量中各个参数的生成方式：

通过如下方式生成 MAC*、XRES* 、KAUSF：

第二 RAND=H (第一 RAND，第一 SNN)，MAC* = f_1(K, 第二 RAND,)，XRES*=f_2 (K, 第二 RAND，第一 SNN)，K_{AUSF} =f_3 (K，第二 RAND)，其中，H、f_1 、f_2 、f_3 分别表示一种运算方式。

步骤 603: 所述 UDM 网元在生成了所述第一认证向量之后，将所述第一认证向量发送给所述 AUSF 网元，示例性的，所述 UDM 网元将携带有所述第一认证向量携带在认证获取响应发送给所述 AUSF 网元。

步骤 604: 所述 AUSF 网元在接收到所述第一认证向量后，对所述第一认证向量进行进一步处理，生成第二认证向量。

其中，所述第二认证向量中包括第一 RAND、HXRES*、MAC*，其中，MAC* 可以携带在 AUTN 中。

HXRES* 的生成方式参见步骤 207 中的相关描述，此处不再赘述。

可选的，所述 AUSF 网元还可以根据 K_{AUSF} 进行推演生成 K_{SEAF}，并在本地保存 KSEAF 以便后续发送给 SEAF 网元。

步骤 605: 所述 AUSF 网元向所述 SEAF 网元发送所述第二认证向量。

所述 AUSF 可以向所述服务网络中的 SEAF 网元发送携带有所述第二认证向量的认证鉴定响应。

步骤 606: 所述 SEAF 网元在接收到所述第二认证向量后，向所述 UE 发送 NAS 消息 (如认证请求)，所述 NAS 消息中包括第一 RAND，MAC*，其中，MAC* 可以携带在 AUTN 中。所述 NAS 消息还可以包括其他信息，本申请实施例并不限定。

步骤 607: 所述 UE 接收到所述 NAS 消息后，基于所述第二运算，通过所述第一 RAND、第二 SNN 生成第二 RAND，之后再基于第三运算，根据第二 RAND 和 USIM 中存储的密钥 K 生成第二消息认证码 XMAC*。

需要说明的是，步骤 607 中的第二 RAND 与步骤 602 中的第二 RAND 不同，步骤 607 中的第二 RAND 是所述 UE 生成的，步骤 602 中的第二 RAND 是所述 UDM 网元生成的，步骤 607 中的第二 RAND 与步骤 602 中的第二 RAND 的数值是否相同，取决于所述第一 SNN 和所述第二 SNN 是否相同，若所述第一 SNN 和所述第二 SNN 不同，则步骤 607 中的第二 RAND 与步骤 602 中的第二 RAND 的数值不同，所述第一 SNN 和所述第二 SNN 相同，则步骤 607 中的第二 RAND 与步骤 602 中的第二 RAND 的数值相同。

步骤 608: 所述 UE 在确定 XMAC* 与认证令牌中的 MAC* 一致后，向所述 SEAF 网元发送 RES*。

所述 UE 根据第二 RAND 和密钥 K 生成 RES*，这里所述 UE 生成 RES* 所采用的运算方式与所述 UDM 网元生成 XRES* 所采用的运算方式相同。

需要说明的是，所述 UE 进行 XMAC* 和 MAC* 的对比的操作可以是所述 UE 中的 USIM 模块执行的，可以是其他模块 (如 ME 模块)本申请实施例并不限定。

若所述 UDM 网元在生成认证令牌时采用如步骤 602 中列举的方式，下面对 UE 进行 XMAC* 和 MAC* 的对比的方式进行介绍：

首先，所述 UE 采用与所述 UDM 网元生成 MAC* 的相同的方式生成 XMAC*，也即第二 RAND=H(第一 RAND，第二 SNN)，$XMAC^* = f_1(K, SQN, 第二\ RAND, 第二\ SNN)$。

所述 UE 可以采用与所述 UDM 网元生成 XRES* 的相同的方式生成 RES*，也即 $RES^* = f_2(K, 第二\ RAND, 第二\ SNN)$。

所述 UE 在生成 XMAC* 后，对 XMAC* 和 AUTN* 中的 MAC* 进行对比，若一致，则说明在所述 UE 生成 XMAC* 时使用的第二 RAND 和所述 UDM 网元生成 MAC* 时使用的第二 RAND 相同，进一步可以说明所述 UE 生成第二 RAND 使用的第二 SNN 和 UDM 网元生成第二 RAND 使用的第一 SNN 相同，所述服务网络不是欺骗网络，所述 UE 对所述服务网络验证成功；若不一致，则说明所述服务网络为欺骗网络，所述 UE 对所述服务网络验证失败。

若所述 UE 对服务网络验证失败，所述 UE 向所述 SEAF 网元发送用于指示验证失败的消息。

步骤 609: 同步骤 509，此处不再赘述。

基于与方法实施例同一发明构思，本申请实施例还提供了一种通信装置，用于执行上述如图 3~6 所示的方法实施例中所述 UDM 网元执行的方法，相关特征可参见上述方法实施例，此处不再赘述，如图 7 所示，所述装置包括处理单元 701 和发送单元 702:

所述处理单元 701，用于根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码；

所述发送单元 702，用于通过所述第二网络向所述终端设备发送所述第一随机数和所述第一消息认证码。

作为一种可能的实施方式，所述第一消息认证码携带在认证令牌中。

作为一种可能的实施方式，所述处理单元 701 在根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码时，可以直接根据所述终端设备的密

钥 K、所述第一随机数、以及所述第二网络的网络标识生成第一消息认证码，也可以采用其他方式，示例性的，所述处理单元 701 可以先根据所述第一随机数和所述第二网络的网络标识生成第二随机数；之后，根据所述终端设备的密钥 K 和所述第二随机数生成所述第一消息认证码。

作为一种可能的实施方式，所述装置还包括接收单元 703，所述接收单元 703 在所述处理单元 701 根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码之前，可以接收来自所述第二网络中的认证服务功能网元发送的终端认证获取请求，所述终端认证获取请求包括加密后的用户标识；所述处理单元 701 则可以解密所述加密后的用户标识，得到解密后的用户标识；以及根据所述解密后的用户标识，获取所述终端设备的签约数据，其中，所述终端的签约数据中包括所述终端设备的密钥 K。

基于与方法实施例同一发明构思，本申请实施例还提供了一种通信装置，用于执行上述如图 3~6 所示的方法实施例中所述终端设备执行的方法，相关特征可参见上述方法实施例，此处不再赘述，如图 8 所示，该装置包括接收单元 801、生成单元 802 以及验证单元 803:

所述接收单元 801，用于通过第二网络接收来自第一网络的随机数、第一消息认证码；以及从所述第二网络接收所述第二网络的网络标识；

所述生成单元 802，用于根据本地存储的密钥 K、第一随机数、以及所述第二网络的网络标识生成第二消息认证码；

所述验证单元 803，用于在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

作为一种可能的实施方式，所述第一消息认证码携带在认证令牌中。

作为一种可能的实施方式，所述生成单元 802 在根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码，可以直接根据所述本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成所述第二消息认证码，也可以采用其他方式，示例性的，所述生成单元 802 可以先根据所述第一随机数和所述第二网络的网络标识生成第二随机数；之后，根据所述本地存储的密钥 K 和所述第二随机数生成所述第二消息认证码。

作为一种可能的实施方式，所述接收单元 801 在通过第二网络接收来自第一网络的随机数、第一消息认证码时，所述随机数、第一消息认证码可以携带在一些信令中，示例性的，所述接收单元 801 可以从所述第二网络的安全锚功能网元接收认证请求，所述认证请求中包括所述第一随机数、第一消息认证码。

本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，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器中，也可以是单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

该集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台终端设备（可以是个人计算机，手机，或者网络设备等）或处理器（processor）执行本申请各个实施例

该方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(read-only memory, ROM)、随机存取存储器(random access memory, RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

在本申请实施例中,所述统一数据管理网元和所述终端设备均可以采用集成的方式划分各个功能模块的形式来呈现。这里的"模块"可以指特定ASIC, 电路,执行一个或多个软件或固件程序的处理器和存储器,集成逻辑电路,和成其他可以提供上述功能的器件。

在一个简单的实施例中,本领域的技术人员可以想到所述统一数据管理网元可采用图9所示的形式。

如图9所示的通信装置900,包括至少一个处理器901、存储器902,可选的,还可以包括通信接口903。

存储器902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902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902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901以及存储器902之间的具体连接介质。本申请实施例在图中以存储器902和处理器901之间通过总线904连接,总线904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904可以分为地址总线、数据总线、控制总线等。为便于表示,图9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901可以具有数据收发功能,能够与其他设备进行通信,在如图9装置中,也可以设置独立的数据收发模块,例如通信接口903,用于收发数据;处理器901在与其他设备进行通信时,可以通过通信接口903进行数据传输。

当所述统一数据管理网元采用图9所示的形式时,图9中的处理器901可以通过调用存储器1402中存储的计算机执行指令,使得所述基站可以执行上述任一方法实施例中的所述基站执行的方法。

具体的,图7的发送单元、接收单元和处理单元的功能/实现过程均可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现。或者,图7中的处理单元的功能/实现过程可以通过图9中的处理器901调用存储器902中存储的计算机执行指令来实现,图7的发送单元和接收单元的功能/实现过程可以通过图9中的通信接口903来实现。

在一个简单的实施例中,本领域的技术人员可以想到所述终端设备可采用图10所示的形式。

如图10所示的通信装置1000,包括至少一个处理器1001、存储器1002,可选的,还可以包括收发器1003。

存储器1002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1002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1002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1001以及存储器1002之间的具体连接介质。本申

请实施例在图中以存储器 1002 和处理器 1001 之间通过总线 1004 连接，总线 1004 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 1004 可以分为地址总线、数据总线、控制总线等。为便于表示，图 10 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 1001 可以具有数据收发功能，能够与其他设备进行通信，在如图 10 装置中，也可以设置独立的数据收发模块，例如收发器 1003，用于收发数据；处理器 1001 在与其他设备进行通信时，可以通过收发器 1003 进行数据传输。

当终端设备采用图 10 所示的形式时，图 10 中的处理器 1001 可以通过调用存储器 1002 中存储的计算机执行指令，使得所述终端设备可以执行上述任一方法实施例中的终端设备执行的方法。

具体的，图 8 中的接收单元、生成单元以及验证单元的功能/实现过程均可以通过图 10 中的处理器 1001 调用存储器 1002 中存储的计算机执行指令来实现。或者，图 8 中的生成单元以及验证单元的功能/实现过程可以通过图 10 中的处理器 1001 调用存储器 1002 中存储的计算机执行指令来实现，图 8 中的接收单元的功能/实现过程可以通过图 10 中的收发器 1003 来实现。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

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精神和范围。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

1、一种网络验证方法，其特征在于，所述方法包括：

统一数据管理网元根据终端设备的密钥 K、第一随机数、以及第二网络的网络标识生成第一消息认证码；

通过所述第二网络向所述终端设备发送所述第一随机数和所述第一消息认证码。

2、如权利要求 1所述的方法，其特征在于，所述第一消息认证码携带在认证令牌中。

3、如权利要求 1或 2所述的方法，其特征在于，所述统一数据管理网元根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码，包括：

所述统一数据管理网元根据所述第一随机数和所述第二网络的网络标识生成第二随机数；

所述统一数据管理网元根据所述终端设备的密钥 K和所述第二随机数生成所述第一消息认证码。

4、如权利要求 1~3 任一所述的方法，其特征在于，所述统一数据管理网元在所述根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码之前，所述方法还包括：

所述统一数据管理网元接收来自所述第二网络中的认证服务功能网元发送的终端认证获取请求，所述终端认证获取请求包括力P密后的用户标识；

所述统一数据管理网元解密所述加密后的用户标识，得到解密后的用户标识；

所述统一数据管理网元根据所述解密后的用户标识，获取所述终端设备对应的签约数据，其中，所述终端设备对应的签约数据中包括所述终端设备的密钥 K。

5、一种网络验证方法，其特征在于，所述方法包括：

通过第二网络接收来自第一网络中统一数据管理网元的第一随机数和第一消息认证码；

根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码；

在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

6、如权利要求 5所述的方法，其特征在于，所述第一消息认证码携带在认证令牌中。

7、如权利要求 5或 6所述的方法，其特征在于，所述根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码，包括：

根据所述第一随机数和所述第二网络的网络标识生成第二随机数；

根据所述本地存储的密钥 K和所述第二随机数生成所述第二消息认证码。

8、如权利要求 5~7 任一所述的方法，其特征在于，所述通过第二网络接收来自第一网络中统一数据管理网元的第一随机数和第一消息认证码，包括：

从所述第二网络的安全锚功能网元接收认证请求，所述认证请求中包括所述第一随机数和所述第一消息认证码。

9、一种通信装置，其特征在于，所述装置包括处理单元和发送单元：

所述处理单元，用于根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码；

所述发送单元，用于通过所述第二网络向所述终端设备发送所述第一随机数和所述第一消息认证码。

10、如权利要求 9 所述的装置，其特征在于，所述第一消息认证码携带在认证令牌中。

11、如权利要求 9 或 10 所述的装置，其特征在于，所述处理单元在根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码，具体用于：

根据所述第一随机数和所述第二网络的网络标识生成第二随机数；

根据所述终端设备的密钥 K 和所述第二随机数生成所述第一消息认证码。

12、如权利要求 9~11 任一所述的装置，其特征在于，所述装置还包括接收单元，所述接收单元在所述处理单元根据终端设备的密钥 K、所述第一随机数、以及第二网络的网络标识生成第一消息认证码之前，用于：

接收来自所述第二网络中的认证服务功能的终端认证获取请求，所述终端认证获取请求包括加密后的用户标识；

所述处理单元，还用于解密所述加密后的用户标识，得到解密后的用户标识；以及根据所述解密后的用户标识，获取所述终端设备的签约数据，其中，所述终端的签约数据中包括所述终端设备的密钥 K。

13、一种通信装置，其特征在于，所述装置包括接收单元、生成单元以及验证单元：

所述接收单元，用于通过第二网络接收来自第一网络中统一数据管理网元的第一随机数和第一消息认证码；

所述生成单元，用于根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码；

所述验证单元，用于在确定所述第一消息认证码和所述第二消息认证码一致后，确定对所述第二网络验证成功。

14、如权利要求 13 所述的装置，其特征在于，所述第一消息认证码携带在认证令牌中。

15、如权利要求 13 或 14 所述的装置，其特征在于，所述生成单元在根据本地存储的密钥 K、所述第一随机数、以及所述第二网络的网络标识生成第二消息认证码，具体用于：

根据所述第一随机数和所述第二网络的网络标识生成第二随机数；

根据所述本地存储的密钥 K 和所述第二随机数生成所述第二消息认证码。

16、如权利要求 13~15 任一所述的装置，其特征在于，所述接收单元在通过第二网络接收来自第一网络中统一数据管理网元的第一随机数和第一消息认证码，具体用于：

从所述第二网络的安全锚功能网元接收认证请求，所述认证请求中包括所述第一随机数和所述第一消息认证码。

17、一种通信系统，其特征在于，所述系统包括第一网络中的统一数据管理网元和第一网络中的认证服务功能网元；

所述认证服务功能网元，用于接收来自第二网络中安全锚功能网元的认证鉴定请求；所述认证鉴定请求中包括来自终端设备的加密后的用户标识；向所述统一数据管理网元发送终端认证获取请求，所述终端认证获取请求包括所述加密后的用户标识；

所述统一数据管理网元，用于接收所述终端认证获取请求；解密所述加密后的用户标识，得到解密后的用户标识；根据所述解密后的用户标识，获取所述终端设备对应的签约数据，其中，所述终端设备对应的签约数据中包括所述终端设备的密钥 K；根据所述终端

设备的密钥 K、第一随机数、以及所述第二网络的网络标识生成第一消息认证码；以及通过所述第二网络向所述终端设备发送所述第一随机数和所述第一消息认证码。

18、如权利要求 17 所述的系统，其特征在于，所述第一消息认证码携带在认证令牌中。

19、如权利要求 17 或 18 所述的系统，其特征在于，所述统一数据管理网元在根据终端设备的密钥 K、第一随机数、以及第二网络的网络标识生成第一消息认证码，具体用于：

根据所述第一随机数和所述第二网络的网络标识生成第二随机数；根据所述终端设备的密钥 K 和所述第二随机数生成所述第一消息认证码。

20、如权利要求 17-19 任一所述的系统，其特征在于，所述系统还包括所述第二网络中的安全锚功能网元；

所述安全锚功能网元，用于从所述终端设备接收注册请求，所述注册请求中包括所述加密的用户标识；向所述认证服务功能网元发送所述认证鉴定请求；通过所述认证服务功能网元接收来自所述统一数据管理网元的所述第一随机数和所述第一消息认证码，以及向所述终端设备发送认证请求，所述认证请求中包括所述第一随机数和所述第一消息认证码。

21、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执行指令，当所述通信装置运行时，所述处理器执行所述存储器存储的所述计算机执行指令，以使所述通信装置执行如权利要求 1-4 任一所述的方法。

22、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执行指令，当所述通信装置运行时，所述处理器执行所述存储器存储的所述计算机执行指令，以使所述通信装置执行如权利要求 5-8 任一所述的方法。

23、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中存储有指令，当其在计算机上运行时，使得计算机执行如权利要求 1 至 4 中任一项所述的方法。

24、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中存储有指令，当其在计算机上运行时，使得计算机执行如权利要求 5 至 8 中任一项所述的方法。

25、一种计算机芯片，其特征在于，所述芯片与存储器相连，所述芯片用于读取并执行所述存储器中存储的软件程序，执行如权利要求 1 到 8 任一项所述的方法。

26、一种包含指令的计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1 到 8 任一项所述的方法。

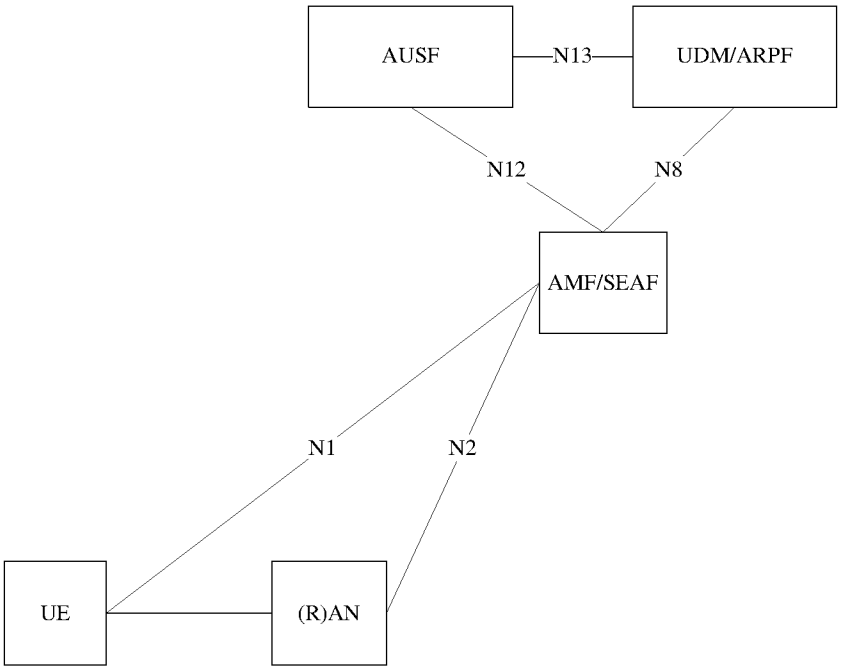

图 1A

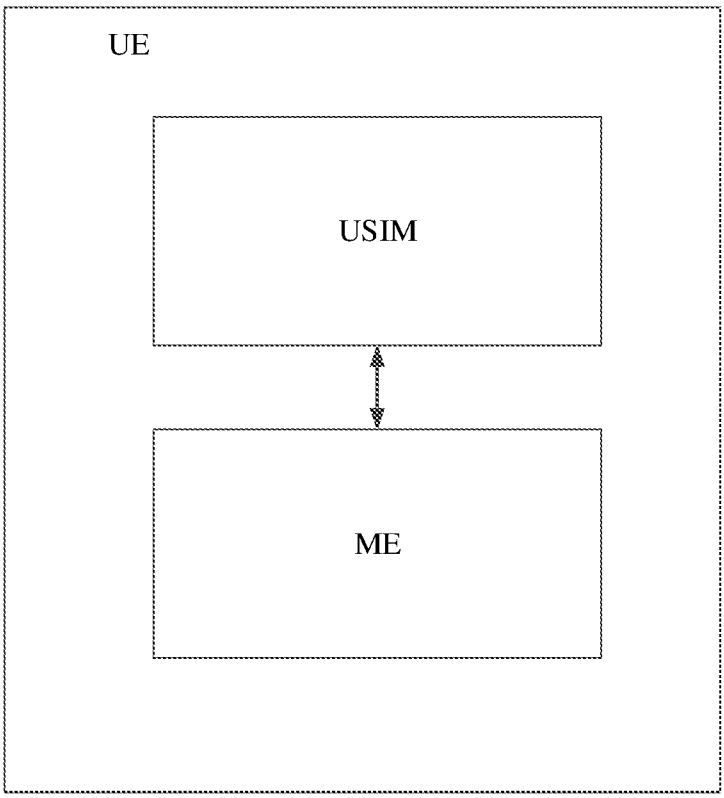

图 1B

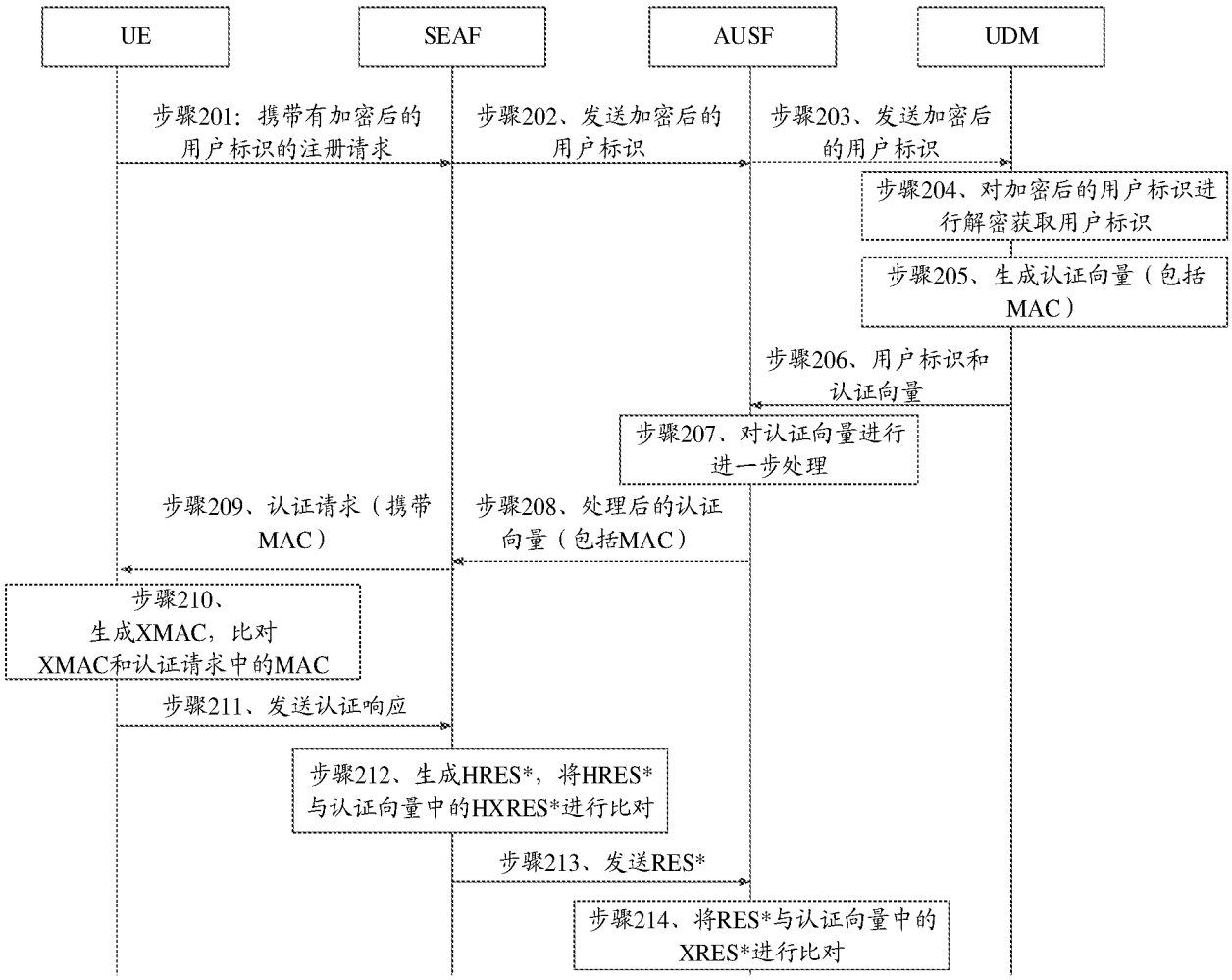
UE
SEAF
AUSF
UDM
步骤201：携带有加密后的用户标识的注册请求
步骤202、发送加密后的用户标识
步骤203、发送加密后的用户标识
步骤204、对加密后的用户标识进行解密获取用户标识
步骤205、生成认证向量（包括MAC）
步骤206、用户标识和认证向量
步骤207、对认证向量进行进一步处理
步骤209、认证请求（携带MAC）
步骤208、处理后的认证向量（包括MAC）
步骤210、生成XMAC，比对XMAC和认证请求中的MAC
步骤211、发送认证响应
步骤212、生成HRES*，将HRES*与认证向量中的HXRES*进行比对
步骤213、发送RES*
步骤214、将RES*与认证向量中的XRES*进行比对

图 2

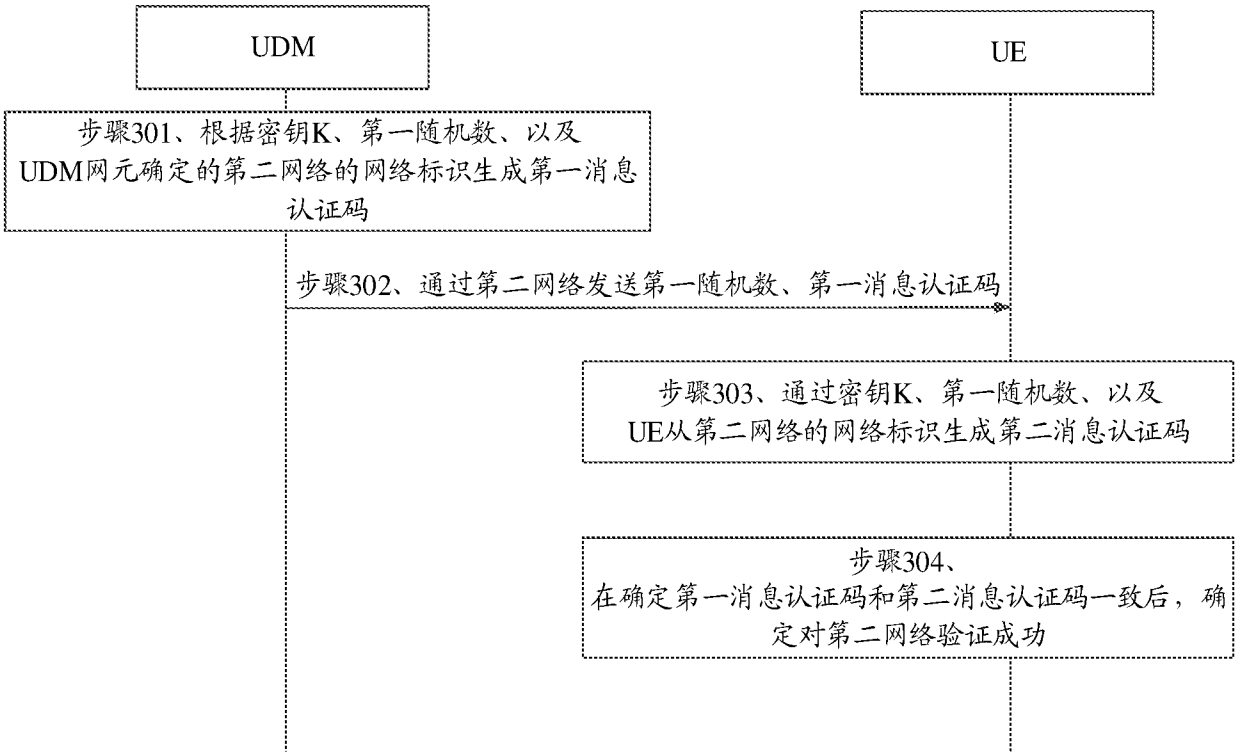
UDM
UE
步骤301、根据密钥K、第一随机数、以及UDM网元确定的第二网络的网络标识生成第一消息认证码
步骤302、通过第二网络发送第一随机数、第一消息认证码
步骤303、通过密钥K、第一随机数、以及UE从第二网络的网络标识生成第二消息认证码
步骤304、在确定第一消息认证码和第二消息认证码一致后，确定对第二网络验证成功

图 3

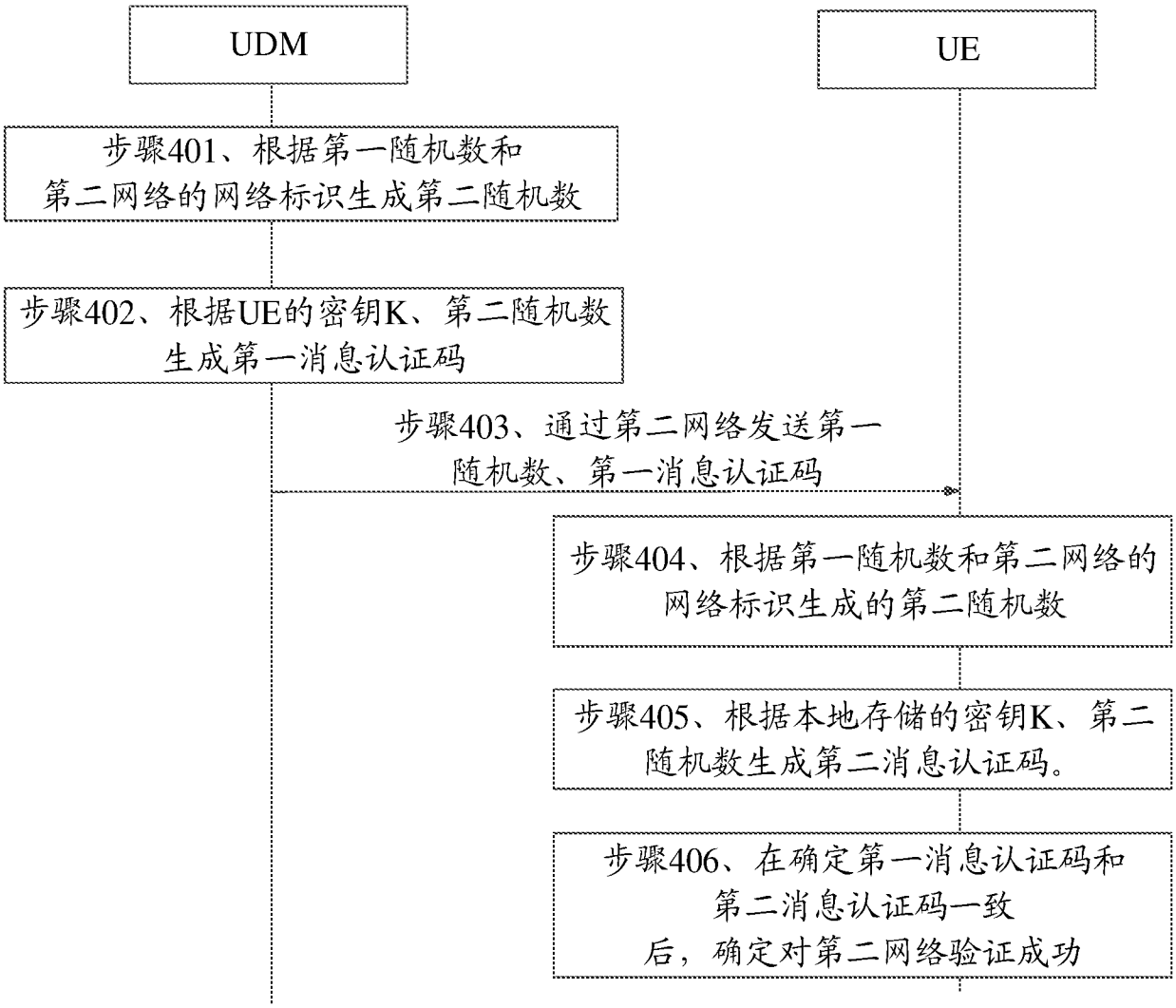
UDM
UE
步骤401、根据第一随机数和第二网络的网络标识生成第二随机数
步骤402、根据UE的密钥K、第二随机数生成第一消息认证码
步骤403、通过第二网络发送第一随机数、第一消息认证码
步骤404、根据第一随机数和第二网络的网络标识生成的第二随机数
步骤405、根据本地存储的密钥K、第二随机数生成第二消息认证码。
步骤406、在确定第一消息认证码和第二消息认证码一致后，确定对第二网络验证成功

图 4

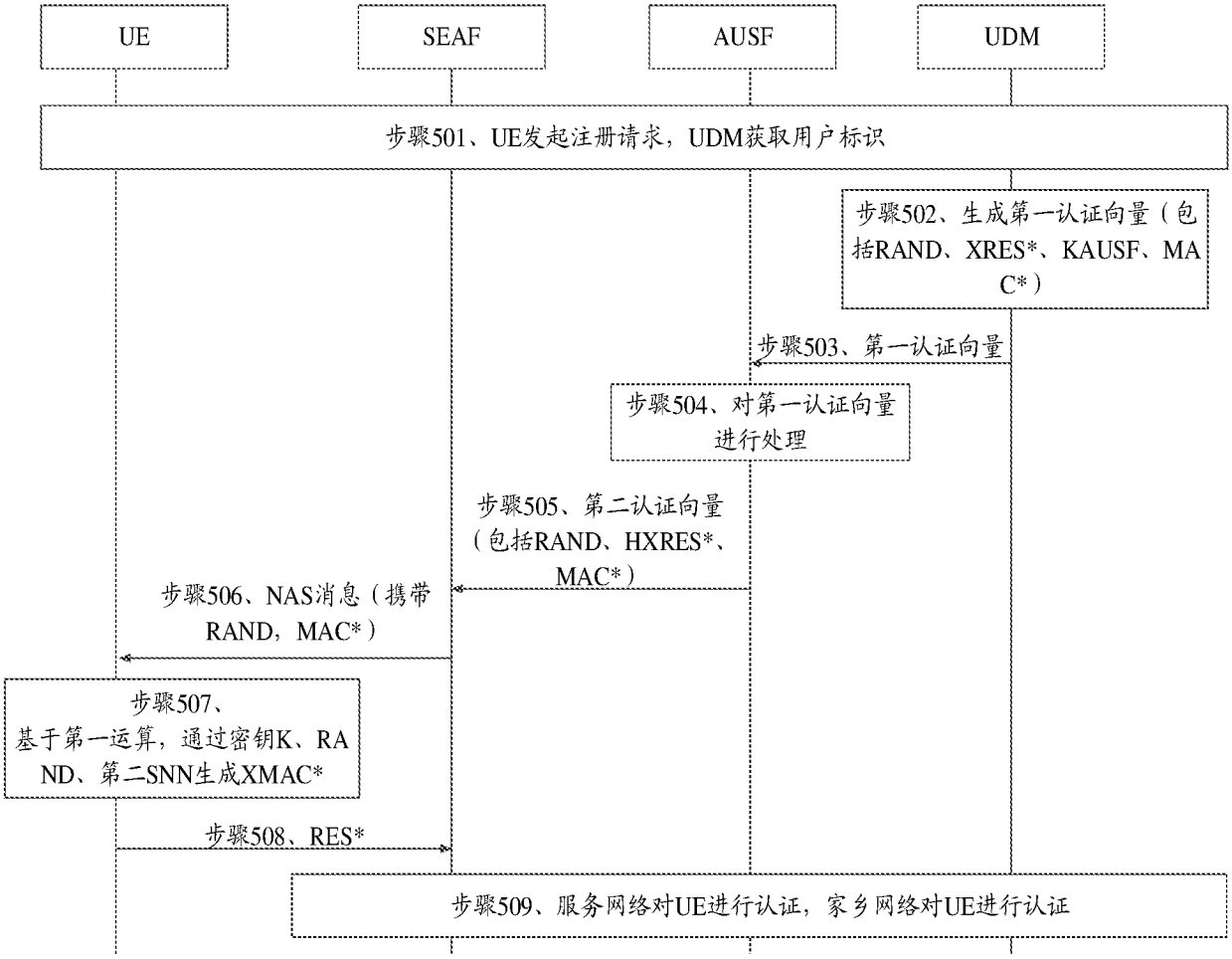
UE
SEAF
AUSF
UDM
步骤501、UE发起注册请求，UDM获取用户标识
步骤502、生成第一认证向量（包括RAND、XRES*、KAUSF、MAC*）
步骤503、第一认证向量
步骤504、对第一认证向量进行处理
步骤505、第二认证向量（包括RAND、HXRES*、MAC*）
步骤506、NAS消息（携带RAND，MAC*）
步骤507、基于第一运算，通过密钥K、RAND、第二SNN生成XMAC*
步骤508、RES*
步骤509、服务网络对UE进行认证，家乡网络对UE进行认证

图 5

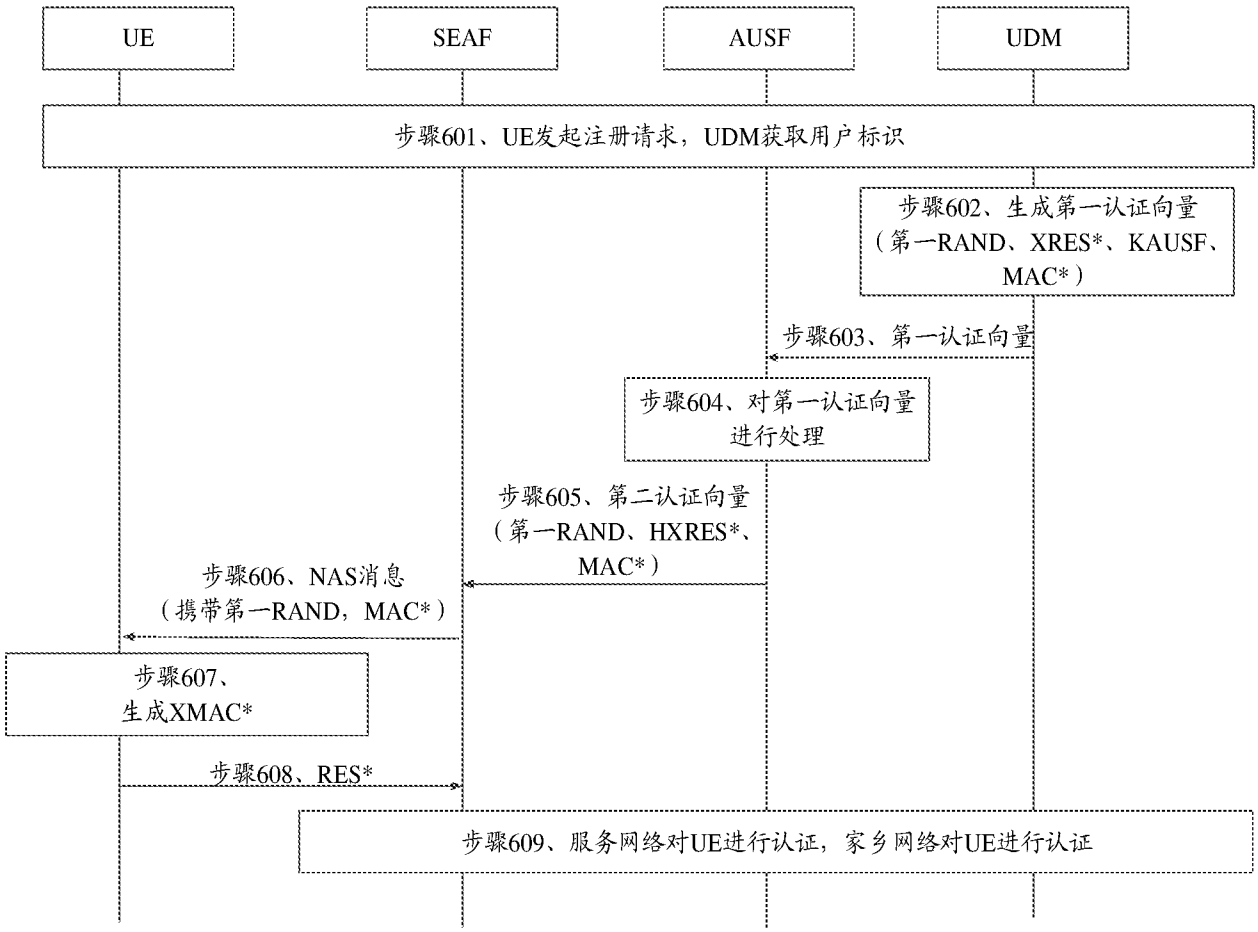
UE
SEAF
AUSF
UDM
步骤601、UE发起注册请求，UDM获取用户标识
步骤602、生成第一认证向量（第一RAND、XRES*、KAUSF、MAC*）
步骤603、第一认证向量
步骤604、对第一认证向量进行处理
步骤605、第二认证向量（第一RAND、HXRES*、MAC*）
步骤606、NAS消息（携带第一RAND，MAC*）
步骤607、生成XMAC*
步骤608、RES*
步骤609、服务网络对UE进行认证，家乡网络对UE进行认证

图 6

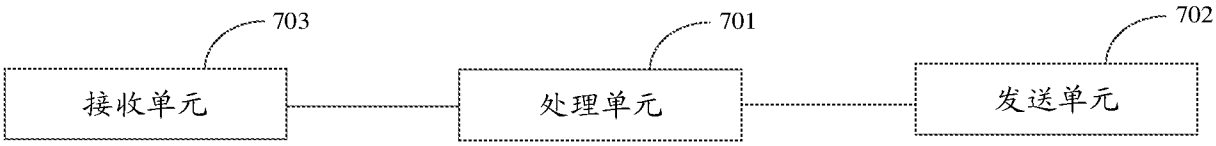
703
701
702
接收单元
处理单元
发送单元

图 7

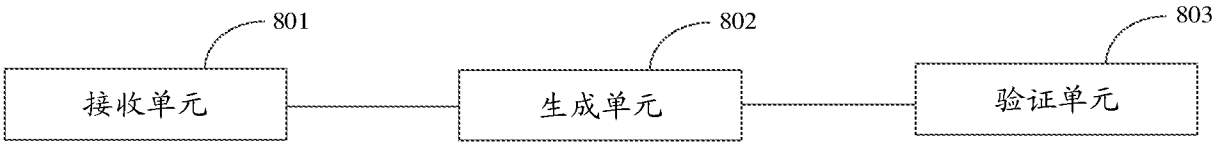
801
802
803
接收单元
生成单元
验证单元

图 8

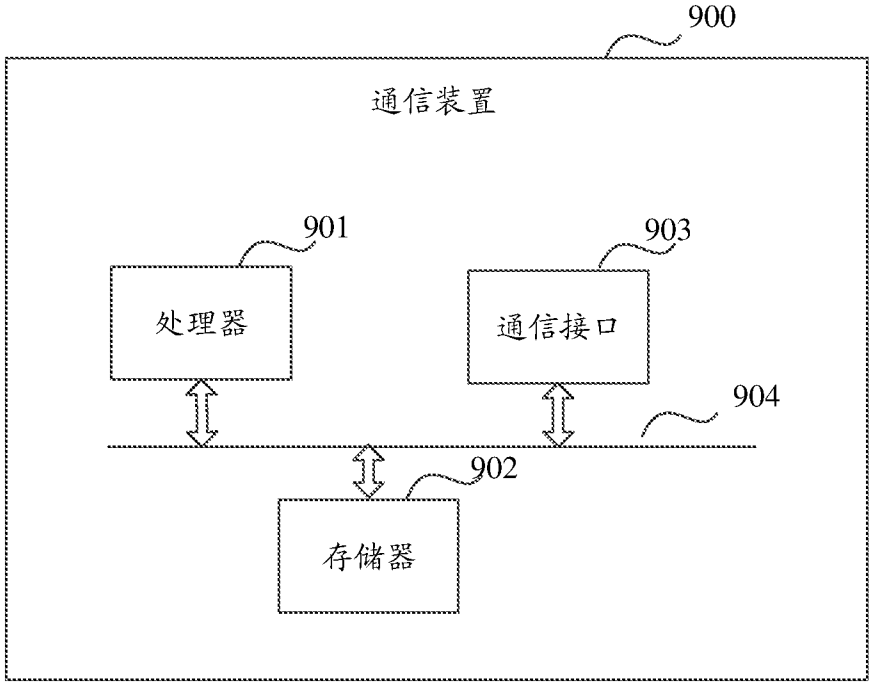
900
通信装置
901
处理器
903
通信接口
904
902
存储器

图 9

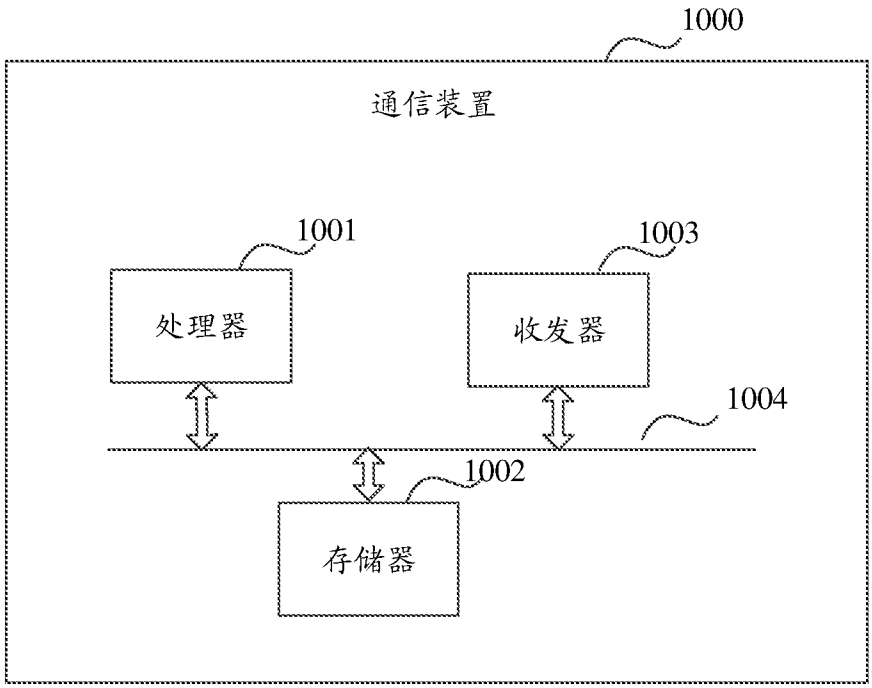
1000
通信装置
1001
处理器
1003
收发器
1004
1002
存储器

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/078309

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L;H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI; CNPAT; WPI; EPODOC; 3GPP: 归属 ,外地 ,访问 ,代理 ,网络 ,第二网络 ,认证码 ,验证 ,认证 ,随机数 ,密钥 ,标识 ,身份 ,一致 ,匹配,加密 ,安全锚 ,SEAF, AUSF, home, proxy, visit+, network, auth+, verif+, random, RAND, secret+, identif+, match, same, anchor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108880813 A (RESEARCH INSTITUTE OF CHINA MOBILE COMMUNICATIONS CORPORATION et al.) 23 November 2018 (2018-11-23) description, paragraphs 131-229, figures 2-4	1-26
A	CN 101473670 A (TNO) 01 July 2009 (2009-07-01) entire document	1-26
A	CN 101867923 A (XIDIAN UNIVERSITY) 20 October 2010 (2010-10-20) entire document	1-26
A	WO 2019000171 A1 (ZTE CORP.) 03 January 2019 (2019-01-03) entire document	1-26
A	CN 101420695 A (TIANGONG UNIVERSITY et al.) 29 April 2009 (2009-04-29) entire document	1-26

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2020	**27 May 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/078309

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108880813	A	23 November 2018	None			
CN	101473670	A	01 July 2009	CA	2656919	A1	27 December 2007
				EP	1871065	A1	26 December 2007
				EP	2039110	A1	25 March 2009
				WO	2007148969	A1	27 December 2007
				US	2009282467	A1	12 November 2009
				KR	20090036562	A	14 April 2009
				JP	2009541843	A	26 November 2009
CN	101867923	A	20 October 2010	None			
WO	2019000171	A1	03 January 2019	None			
CN	101420695	A	29 April 2009	None			

国际检索报告

国际申请号
PCT/CN2020/078309

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L;H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI;CNPAT;WPI;EPODOC;3GPP: 归属，外地，访问，代理，网络，第二网络，认证码，验证，认证，随机数，密钥，标识，身份，一致，匹配，加密，安全锚，SEAF, AUSF, home, proxy, visit+, network, auth+, verif+, random, RAND, secret+, identif+, match, same, anchor

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 108880813 A (中国移动通信有限公司研究院 等) 2018年 11月 23日 (2018-11-23) 说明书第131-229段、图2-4	1-26
A	CN 101473670 A (荷兰应用自然科学研究组织) 2009年 7月 1日 (2009-07-01) 全文	1-26
A	CN 101867923 A (西安电子科技大学) 2010年 10月 20日 (2010-10-20) 全文	1-26
A	WO 2019000171 A1 (ZTE CORP.) 2019年 1月 3日 (2019-01-03) 全文	1-26
A	CN 101420695 A (天津工业大学 等) 2009年 4月 29日 (2009-04-29) 全文	1-26

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 5月 14日	2020年 5月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 汪德闯 电话号码 86-(10)-53961791

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/078309

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108880813	A	2018年 11月 23日	无			
CN	101473670	A	2009年 7月 1日	CA	2656919	A1	2007年 12月 27日
				EP	1871065	A1	2007年 12月 26日
				EP	2039110	A1	2009年 3月 25日
				WO	2007148969	A1	2007年 12月 27日
				US	2009282467	A1	2009年 11月 12日
				KR	20090036562	A	2009年 4月 14日
				JP	2009541843	A	2009年 11月 26日
CN	101867923	A	2010年 10月 20日	无			
WO	2019000171	A1	2019年 1月 3日	无			
CN	101420695	A	2009年 4月 29日	无			