

(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
2021 年 5 月 6 日 (06.05.2021)



(10) 国际公布号
WO 2021/083000 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2020/122423

(22) 国际申请日: 2020 年 10 月 21 日 (21.10.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201911059164.0 2019 年 11 月 1 日 (01.11.2019) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION CO., LTD RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

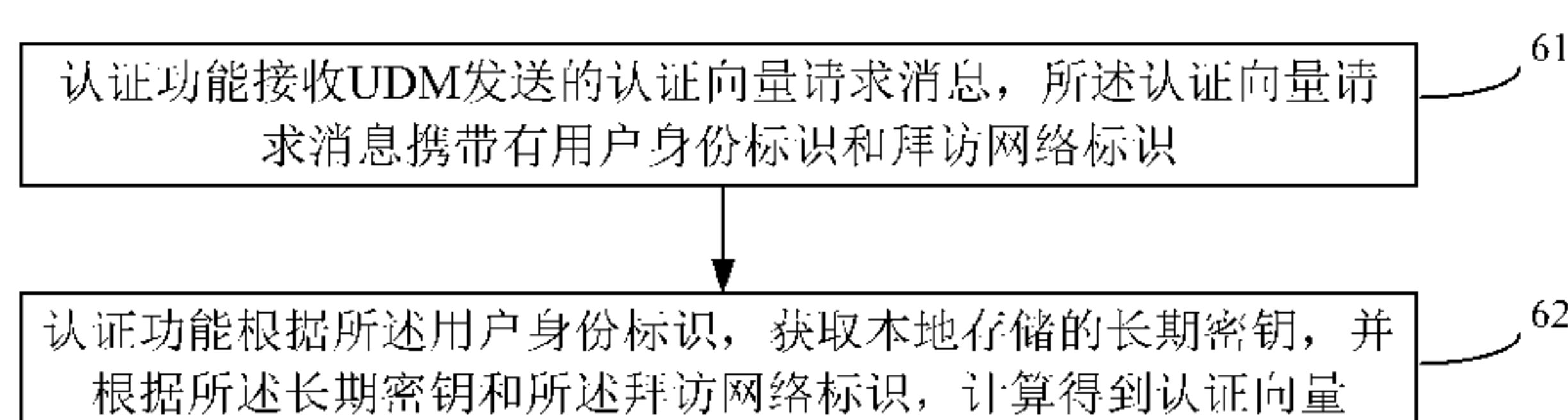
(72) 发明人: 齐旻鹏 (QI, Minpeng); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。刘畅 (LIU, Chang); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街 32 号院枫蓝国际中心 2 号楼 10 层, Beijing 100082 (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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) Title: AUTHENTICATION VECTOR GENERATION METHOD, ACQUISITION METHOD, AND DEVICE

(54) 发明名称: 认证向量的生成方法、获取方法及设备



61 An authentication function receives an authentication vector request message sent by UDM, the authentication vector request message carrying a user identity identifier and a visited network identifier
62 On the basis of the user identity identifier, the authentication function acquires a long-term key stored locally, and calculates an authentication vector on the basis of the long-term key and the visited network identifier

图 6

(57) Abstract: Provided in the present disclosure are an authentication vector generation method, an acquisition method, and a device, wherein processing such as the storage of long-term keys and the generation of authentication vectors are placed in an authentication function, and the authentication function is separated from UDM, thereby ensuring that the storage of long-term keys and the production of authentication vectors is implemented in the same network element, avoiding the risk of leakage caused by the transmission of long-term keys in different network elements; and also ensuring that the UDM serves as a data management device that is only responsible for information processing and does not participate in data storage. In addition, UDM transparent transmission is introduced, so that the relevant authentication structure is effectively inherited, avoiding the problem of the network being incapable of backward compatibility due to the introduction of new network elements/network functions causing changes to the message interface.

(57) 摘要: 本公开提供了一种认证向量的生成方法、获取方法及设备, 本公开将长期密钥的存储及认证向量的生成等处理放在了认证功能中, 并将认证功能与UDM分离, 从而可以保证长期密钥的存储与认证向量的产生是在同一网元中进行的, 避免了长期密钥在不同网元中传输所导致的泄露风险; 同时也保证了UDM作为数据管理设备, 只负责信息处理, 不参与数据存储。此外, 引入UDM透传, 还有效的继承了相关的认证架构, 防止因为引入新的网元/网络功能导致消息接口发生变化, 进而导致网络无法后向兼容的问题。



(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, CI, 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))。

认证向量的生成方法、获取方法及设备

相关申请的交叉引用

本申请主张在 2019 年 11 月 1 日在中国提交的中国专利申请号 No. 201911059164.0 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及移动通信技术领域，具体涉及一种认证向量的生成方法、获取方法及设备。

背景技术

目前，用户在接入 5G 网络时，需要与网络相互确认身份并建立安全连接，因此需要与 5G 网络进行双向认证，通过认证来实现用户 (User Equipment, UE) 与 5G 网络之间的双向身份确认并为后续安全连接产生必须的会话密钥。上述认证被称为 5G 网络主认证。

图 1 给出了相关技术的 5G 网络主认证的流程，包括步骤 0~12 等多个步骤，如图 1 所示：

当用户尝试接入网络进行主认证时，用户将会向网络接入和移动管理功能 (Access and Mobility Management Function, AMF) 发起接入请求，而 AMF 会将接入请求发给身份认证服务器功能 (Authentication Server Function, AUSF)，AUSF 再通过 Nudm_Authentication_Get Request 消息发给身份认证凭据存储库和处理功能 (Authentication credential Repository and Processing Function, ARPF)。ARPF 负责保存用户认证所需要的长期密钥并负责根据长期密钥产生认证所需参数，通常集成在统一数据管理 (Unified Data Management, UDM) 中。UDM/ARPF 需要对每个 Nudm_Authenticate_Get Request 消息创建一个 5G 归属环境认证向量 (Home Environment Authentication Vector, HEAV)。为此，UDM/ARPF 首先生成一个认证管理域 (Authentication Management Field, AMF)，其中的 “separation bit” 为 1。然后，UDM/ARPF 根据长期密钥 K 推导出 K_{AUSF} 和 $XRES^*$ 。最后，UDM/ARPF 应创建一个包含

RAND、AUTN、XRES* 和 K_{AUSF} 的 5G HE AV，并在 Nudm_UEAuthentication_Get Response 消息中向 AUSF 返回所请求的 5G HE AV。从图 1 所示的流程可以看出，相关技术的认证向量的存储和产生均是在 UDM/ARPF 中完成的。

发明内容

本公开的至少一个实施例提供了一种认证向量的生成方法、获取方法及设备，减少长期密钥的泄露风险，提升系统的安全性。

根据本公开的至少一个方面，至少一个实施例提供了一种认证向量的生成方法，应用于认证功能，包括：

所述认证功能接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

所述认证功能根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

可选的，所述认证功能与 UDM 相互独立，且两者之间存在有预设接口 Narpf；

所述认证功能通过所述预设接口 Narpf 接收 UDM 发送的所述认证向量请求消息，以及，通过所述预设接口 Narpf 向 UDM 发送携带有所述认证向量的认证向量响应消息。

可选的，所述认证向量请求消息为 Narpf_authentication_get Request 消息；

所述认证向量响应消息为 Narpf_authentication_get Response 消息。

可选的，根据所述长期密钥和所述拜访网络标识，计算得到认证向量的步骤，包括：

所述认证功能获取长期密钥及其对应的序列号 SQN，并生成随机数 RAND；

所述认证功能对所述随机数 RAND 和运营商的配置参数 OPc 进行异或运算，并利用长期密钥进行加密运算，得到第一中间结果；

利用第一参数组，对所述第一中间结果进行第一运算处理，得到第一运算结果，将所述第一运算结果的前半部分的预设比特位与序列号 SQN 进行异

或运算，得到第一参数；

所述认证功能基于所述第一计算结果的后半部分、所述随机数 RAND 以及拜访网络标识，生成一响应值 XRES*；

利用第二参数组和第三参数组，分别对所述第一中间结果进行所述第一运算处理，得到认证流程后使用的会话加密密钥 CK 和会话完整性密钥 IK；以及，根据所述 CK、IK 和拜访地运营商的标识，产生一中间密钥 K_{AUSF}；

将序列号 SQN、本地保存的认证所需的认证管理参数 AMF、SQN 以及 AMF 级联，并利用第四参数组，对级联得到的参数进行第二运算处理，得到第二运算结果，提取第二计算结果的前半部分，得到第二参数；

将所述第一参数、AMF、第二参数级联，得到认证令牌 AUTN，以及，将所述 RAND、AUTN、XRES* 和 K_{AUSF} 作为认证向量参数，得到认证向量。

根据本公开的另一方面，至少一个实施例提供了一种认证向量的获取方法，应用于统一数据管理 UDM，包括：

所述 UDM 在接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息后，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；

所述 UDM 接收认证功能发送的携带有认证向量的认证向量响应消息。

可选的，所述 UDM 与认证功能相互独立，且两者之间存在有预设接口 Narpf；

所述 UDM 通过所述预设接口 Narpf 向认证功能发送所述第二认证向量请求消息，以及，通过所述预设接口 Narpf 接收认证功能发送的携带有认证向量的认证向量响应消息。

可选的，所述第二认证向量请求消息为 Narpf_authentication_get Request 消息；

所述认证向量响应消息为 Narpf_authentication_get Response 消息。

根据本公开的另一方面，至少一个实施例提供了一种 UDM，包括：

第一接收模块，用于接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息；

发送模块，用于在接收到所述第一认证向量请求消息后，向认证功能发

送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；

第二接收模块，用于接收认证功能发送的携带有认证向量的认证向量响应消息。

根据本公开的另一方面，至少一个实施例提供了一种 UDM，包括收发机和处理器，其中，

所述收发机，用于接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息；

所述处理器，用于在所述收发机接收到第一认证向量请求消息，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；以及，接收认证功能发送的携带有认证向量的认证向量响应消息。

根据本公开的另一方面，至少一个实施例提供了一种 UDM，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如上所述的认证向量的获取方法的步骤。

根据本公开的另一方面，至少一个实施例提供了一种认证功能，包括：

接收模块，用于接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

计算模块，用于根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

根据本公开的另一方面，至少一个实施例提供了一种认证功能，包括收发机和处理器，其中，

所述收发机，用于接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

所述处理器，用于根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

根据本公开的另一方面，至少一个实施例提供了一种认证功能，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如上所述的认证向量的获取方法的步骤。

根据本公开的另一方面，至少一个实施例提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有程序，所述程序被处理器执行时，实现如上所述的方法的步骤。

与相关技术相比，本公开实施例提供的认证向量的生成方法、获取方法及设备，将长期密钥的存储及认证向量的生成等处理放在了认证功能中，并将认证功能与 UDM 分离，这样可以保证长期密钥的存储与认证向量的产生是在同一网元中进行的，避免了长期密钥在不同网元中传输所导致的泄露风险；同时也保证了 UDM 作为数据管理设备，只负责信息处理，不参与数据存储。此外，引入 UDM 透传，还有效的继承了相关的认证架构，防止因为引入新的网元/网络功能导致消息接口发生变化，进而导致网络无法后向兼容的问题。

附图说明

通过阅读下文可选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出可选实施方式的目的，而并不认为是对本公开的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为相关技术的 5G 网络主认证的流程示意图；

图 2 为本公开实施例的一种应用场景示意图；

图 3 相关技术的认证向量的生成流程的示意图；

图 4 为本公开实施例提供的认证向量的获取方法的一种流程图；

图 5 为本公开实施例提供的认证向量的获取方法的另一种流程图；

图 6 为本公开实施例提供的认证向量的生成方法的一种流程图；

图 7 为本公开实施例提供的 UDM 的一种结构示意图；

图 8 为本公开实施例提供的 UDM 的另一种结构示意图；

图 9 为本公开实施例提供的认证功能的一种结构示意图；

图 10 为本公开实施例提供的认证功能的另一种结构示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。说明书以及权利要求中“和/或”表示所连接对象的至少其中之一。

本文所描述的技术不限于 NR 系统以及长期演进型 (Long Time Evolution, LTE) /LTE 的演进 (LTE-Advanced, LTE-A) 系统，并且也可用于各种无线通信系统，诸如码分多址 (Code Division Multiple Access, CDMA)、时分多址 (Time Division Multiple Access, TDMA)、频分多址 (Frequency Division Multiple Access, FDMA)、正交频分多址 (Orthogonal Frequency Division Multiple Access, OFDMA)、单载波频分多址 (Single-carrier Frequency-Division Multiple Access, SC-FDMA) 和其他系统。术语“系统”和“网络”常被可互换地使用。CDMA 系统可实现诸如 CDMA2000、通用地面无线电接入 (Universal Terrestrial Radio Access, UTRA) 等无线电技术。UTRA 包括宽带 CDMA (Wideband Code Division Multiple Access, WCDMA) 和其他 CDMA 变体。TDMA 系统可实现诸如全球移动通信系统 (Global System for Mobile Communication, GSM) 之类的无线电技术。OFDMA 系统可实现诸如超移动宽带 (UltraMobile Broadband, UMB)、演进型 UTRA (Evolution-UTRA, E-UTRA)、IEEE 802.21 (Wi-Fi)、IEEE 802.16 (WiMAX)、IEEE 802.20、Flash-OFDM 等无线电技术。UTRA 和 E-UTRA 是通用移动通信系统 (Universal Mobile Telecommunications System, UMTS) 的部分。LTE 和更高级的 LTE (如

LTE-A) 是使用 E-UTRA 的新 UMTS 版本。UTRA、E-UTRA、UMTS、LTE、LTE-A 以及 GSM 在来自名为“第三代伙伴项目”(3rd Generation Partnership Project, 3GPP) 的组织的文献中描述。CDMA2000 和 UMB 在来自名为“第三代伙伴项目 2”(3GPP2) 的组织的文献中描述。本文所描述的技术既可用于以上提及的系统 and 无线电技术, 也可用于其他系统和无线电技术。然而, 以下描述出于示例目的描述了 NR 系统, 并且在以下大部分描述中使用 NR 术语, 尽管这些技术也可应用于 NR 系统应用以外的应用。

以下描述提供示例而并非限定权利要求中阐述的范围、适用性或者配置。可以对所讨论的要素的功能和布置作出改变而不会脱离本公开的精神和范围。各种示例可恰适地省略、替代、或添加各种规程或组件。例如, 可以按不同于所描述的次序来执行所描述的方法, 并且可以添加、省去、或组合各种步骤。另外, 参照某些示例所描述的特征可在其他示例中被组合。

请参见图 2, 图 2 示出本公开实施例可应用的一种无线通信系统的框图。无线通信系统包括终端 21 和网络设备 22。其中, 终端 21 也可以称作用户终端或用户设备 (User Equipment, UE), 终端 21 可以是手机、平板电脑 (Tablet Personal Computer)、膝上型电脑 (Laptop Computer)、个人数字助理 (Personal Digital Assistant, PDA)、移动上网装置 (Mobile Internet Device, MID)、可穿戴式设备 (Wearable Device) 或车载设备等终端侧设备, 需要说明的是, 在本公开实施例中并不限定终端 21 的具体类型。网络设备 22 可以是基站和/或核心网网元, 其中, 上述基站可以是 5G 及以后版本的基站 (例如: gNB、5G NR NB 等), 或者其他通信系统中的基站 (例如: eNB、WLAN 接入点、或其他接入点等), 其中, 基站可被称为节点 B、演进节点 B、接入点、基收发机站 (Base Transceiver Station, BTS)、无线电基站、无线电收发机、基本服务集 (Basic Service Set, BSS)、扩展服务集 (Extended Service Set, ESS)、B 节点、演进型 B 节点 (eNB)、家用 B 节点、家用演进型 B 节点、WLAN 接入点、WiFi 节点或所述领域中其他某个合适的术语, 只要达到相同的技术效果, 所述基站不限于特定技术词汇, 需要说明的是, 在本公开实施例中仅以 NR 系统中的基站为例, 但是并不限定基站的具体类型。

基站可在基站控制器的控制下与终端 21 通信, 在各种示例中, 基站控制

器可以是核心网或某些基站的一部分。一些基站可通过回程与核心网进行控制信息或用户数据的通信。在一些示例中，这些基站中的一些可以通过回程链路直接或间接地彼此通信，回程链路可以是有线或无线通信链路。无线通信系统可支持多个载波（不同频率的波形信号）上的操作。多载波发射机能同时在这多个载波上传送经调制信号。例如，每条通信链路可以是根据各种无线电技术来调制的多载波信号。每个已调信号可在不同的载波上发送并且可携带控制信息（例如，参考信号、控制信道等）、开销信息、数据等。

基站可经由一个或多个接入点天线与终端 21 进行无线通信。每个基站可以为各自相应的覆盖区域提供通信覆盖。接入点的覆盖区域可被划分成仅构成该覆盖区域的一部分的扇区。无线通信系统可包括不同类型的基站（例如宏基站、微基站、或微微基站）。基站也可利用不同的无线电技术，诸如蜂窝或 WLAN 无线电接入技术。基站可以与相同或不同的接入网或运营商部署相关联。不同基站的覆盖区域（包括相同或不同类型的基站的覆盖区域、利用相同或不同无线电技术的覆盖区域、或属于相同或不同接入网的覆盖区域）可以交叠。

无线通信系统中的通信链路可包括用于承载上行链路（Uplink, UL）传输（例如，从终端 21 到网络设备 22）的上行链路，或用于承载下行链路（Downlink, DL）传输（例如，从网络设备 22 到终端 21）的下行链路。UL 传输还可被称为反向链路传输，而 DL 传输还可被称为前向链路传输。下行链路传输可以使用授权频段、非授权频段或这两者来进行。类似地，上行链路传输可以使用有授权频段、非授权频段或这两者来进行。

在相关的 5G 技术方案中，ARPF 被定义为存储长期密钥 K 及产生认证向量的网元，并与 UDM 合并。如图 3 所示，在相关技术的认证向量生成过程中，AUSF 向 UDM 发起认证请求，并从 UDM 获取认证向量；另外，为了便于网络维护，在后期设计时将计算与存储相分离，新定义了统一数据存储库（Unified Data Repository, UDR）作为统一数据存储设备，仅用于存储数据，包括用于认证的长期密钥 K，但 UDR 没有计算能力；UDM 为统一数据管理设备，负责利用长期密钥 K 产生认证向量，但 UDM 失去了数据存储的能力。

从图 3 可以看出，由于 UDR 能用于存储而不能计算，而 UDM 仅能够计

算而不能存储，因此 UDM 需要通过 Nudr 接口从 UDR 获取密钥，从而导致密钥可能在 UDM 与 UDR 之间的传输接口上被泄露，严重影响到后续认证及通信过程的安全性。

为解决以上问题中的至少一种，本申请提供了一种新的认证向量获取方法，可以减少长期密钥 K 因传输而存在泄露风险的问题，并能与相关系统的大部分网元兼容。

具体的，如图 4 所示，本申请提出了一种将认证功能与 UDM 相分离的方案，引入独立的认证功能（也可以将其称作 ARPF），即认证功能与 UDM 相互独立，认证功能不再作为 UDM 的一个功能，而作为另外一个实体而独立存在。并且，在认证功能与 UDM 之间新定义一个接口（这里可以将该接口命名为 Narpf）。由认证功能（ARPF）负责存储长期密钥，以及与认证相关的参数。认证功能（ARPF）同时还具备使用认证算法（如相关技术推荐的认证框架 MILENAGE）和自身保存参数产生相关认证向量的能力。当用户发起接入请求并由网络判断需要认证的情况下，在 UDM 接收到认证向量请求消息时，不再由 UDM 进行处理，而是将认证向量请求消息发送给独立的认证功能。在认证功能生成认证向量后，再通过新定义的接口将认证向量发送给 UDM，UDM 再将认证向量利用现有接口传给 AUSF。

需要说明的是，本文中提及到的各个功能，如 AUSF、UDM、ARPF、UDR 和 AMF 等等，可以是网络中的某个具体网元或功能模块或实体。

请参照图 4，本申请的认证向量获取过程，包括：

步骤 41，AUSF 向 UDM 发送认证向量请求消息，具体的，AUSF 可以通过现有的 Nudm_authentication_get Request 消息向 UDM 发起认证向量请求。

步骤 42，UDM 接收到认证向量请求消息后，通过新定义的 UDM 与认证功能之间的接口（可被称为 Narpf），向认证功能发送认证向量请求消息，并在该认证向量请求消息中携带用户的身份标识（Identity）。具体的，UDM 可以通过 Narpf_authentication_get Request 消息，携带用户身份标识和拜访网络的标识（ID）发送给 ARPF。

步骤 43，认证功能接收到认证向量请求消息后，根据用户身份标识获取到存储在认证功能中的长期密钥 K，利用长期密钥 K 计算出认证向量（5G HE

AV)。下面提供一种具体的认证向量生成算法：

a) 认证功能获取长期密钥 K (128 位) 和对应的序列号 SQN (48 位), 并生成随机数 $RAND$ (128 位)。然后认证功能将随机数 $RAND$, 结合运营商的配置参数 OPc (128 位) 进行异或运算, 然后使用 K 对异或运算结果进行加密运算 (例如, 可以使用 AES 加密算法, 或其他加密算法), 再将运算后的结果 (记做第一中间结果 1) 再次与 OPc 进行异或运算, 再根据位移参数 $r2$ (128 位) 对异或运算结果进行循环位移, 再将循环位移得到的结果与混淆参数 $c2$ (128 位) 进行异或运算后再使用 K 对异或运算结果进行加密运算, 然后, 再用 OPc 对加密运算结果进行异或运算, 并将上述异或运算结果 (为了便于描述, 将该异或运算结果成为第一参数) 拆成前半部分和后半部分 (前后 2 个 64 位), 然后将前 64 位中的前 48 位 (记做 AK) 与 SQN 进行异或运算, 将运算结果作为输出参数中的一部分 (记做 $SQNAK$)。

b) 认证功能将上述计算得到的第一参数的后 64 位记为 RES 或者 $XRES$, 然后再与 $RAND$ 和拜访网络的 ID 一起产生响应值 (记为 RES^* 或者 $XRES^*$) 作为输出参数中的一部分。

c) 认证功能将第一中间结果 1 与 OPc 进行异或运算, 再根据位移参数 $r3$ (128 位) 对异或运算结果进行循环位移, 再对循环位移得到的结果与混淆参数 $c3$ (128 位) 进行异或运算后, 再使用 K 对异或运算结果进行加密运算, 然后, 再用 OPc 对加密运算结果进行异或运算, 将得到的结果 (128 位) 作为认证流程后使用的会话加密密钥 (记做 CK);

d) 认证功能用 $r4$ 和 $c4$ 替换上述 c) 过程中的 $r3$ 和 $c3$ 参数后执行, 将得到的结果 (128 位) 作为认证流程后使用的会话完整性密钥 (记做 IK);

e) 认证功能根据 CK 、 IK 和拜访地运营商的 ID 产生一个中间密钥 K_{AUSF} (256 位)

f) 认证功能自身保存认证所需的认证管理域参数 AMF , 将 $SQN||AMF||SQN||AMF$ ($||$ 为并联符号) 作为输入参数, 与 OPc 进行异或, 再根据位移参数 $r1$ (128 位) 对异或运算结果进行循环位移, 再将位移结果与混淆参数 $c1$ (128 位) 进行异或运算, 得到第二中间结果 2, 再将第二中间结果 2 与第一中间结果 1 进行异或运算, 然后使用 K 对异或运算结果进行加密

运算后，再用 OPc 对加密运算结果进行异或运算，并将所得结果拆成前后 2 个 64 位，然后将前 64 位（记为 MAC），作为输出参数中的一部分；

g) 认证功能将 SQN || AK || AMF || MAC 记为 AUTN，然后将 RAND, AUTN, XRES*, K_{AUSF} 作为认证向量参数，从而得到 5G HE AV。

步骤 44，认证功能将认证向量传送到 UDM，具体的，ARPF 可以通过现有的 Narpf_authentication_get Response 消息，将 5G HE AV 发送给 UDM。

步骤 45，UDM 将认证向量透传给 AUSF，具体的，UDM 可以通过现有的 Nudm_authentication_get Response 消息将 5G HE AV 发送给 AUSF。

从以上流程可以看出，本申请将长期密钥的存储及认证向量的生成等处理放在了认证功能中，并将认证功能与 UDM 分离，这样可以保证长期密钥的存储与认证向量的产生是在同一网元中进行的，避免了长期密钥在不同网元中传输所导致的泄露风险；同时也保证了 UDM 作为数据管理设备，只负责信息处理，不参与数据存储。此外，引入 UDM 透传，还有效的继承了相关的认证架构，防止因为引入新的网元/网络功能导致消息接口发生变化，进而导致网络无法后向兼容的问题。

下面进一步从 UDM 和认证功能侧分别介绍本申请的认证向量的获取方法。

请参照图 5，本申请的认证向量的获取方法在应用于 UDM 侧时，包括：

步骤 51，所述 UDM 在接收到 AUSF 发送的第一认证向量请求消息后，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识。

根据本申请的至少一个实施例，所述 UDM 与认证功能为相互独立的两个网元，并且在两者之间新定义一个接口，本文称之为 Narpf。在上述步骤 51 中，UDM 可以通过所述预设接口 Narpf 向认证功能发送所述第二认证向量请求消息，具体的，所述第二认证向量请求消息可以为 Narpf_authentication_get Request 消息。

步骤 52，所述 UDM 接收认证功能发送的携带有认证向量的认证向量响应消息。

根据本申请的至少一个实施例，UDM 可以通过所述预设接口 Narpf 接收

认证功能发送的认证向量响应消息。具体的，所述认证向量响应消息可以为 Narpf_authentication_get Response 消息。

可选的，所述 UDM 还可以将所述认证向量转发给所述 AUSF。

通过以上步骤，本申请不再由 UDM 生成认证向量，而是向另一网元（认证功能）请求认证向量，从而避免了长期密钥在网元间传输导致的泄露风险，提高了认证的安全性。

请参照图 6，本申请的认证向量的生成方法在应用于认证功能侧时，包括：

步骤 61，认证功能接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识。

根据本申请的至少一个实施例，所述 UDM 与认证功能为相互独立的两个网元，并且在两者之间新定义一个接口，本文称之为 Narpf。在上述步骤 61 中，认证功能可以通过所述预设接口 Narpf 接收 UDM 发送的第二认证向量请求消息，具体的，所述第二认证向量请求消息可以为 Narpf_authentication_get Request 消息。

这里，所述用户身份标识具体包括但不限于 SUPI/SUCI/5G-GUTI/NAI，所述拜访网络标识包括但不限于 SN ID（Serving Network Identifier）。其中，SUPI 是指用户永久标识符（Subscription Permanent Identifier），SUCI 是指用户隐藏标识符（Subscriber Concealed Identifier），5G-GUTI 是指 5G 全局唯一的临时 UE 标识（5G Globally Unique Temporary UE Identity），NAI 是指网络接入标识符（NAI Network Access Identifier）。

步骤 62，所述认证功能根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

根据本申请的至少一个实施例，在步骤 62 中，所述认证功能可以按照以下步骤计算所述认证向量：

A）所述认证功能获取长期密钥及其对应的序列号 SQN，并生成随机数 RAND；

B）所述认证功能对所述随机数 RAND 和运营商的配置参数 OPc 进行异或运算，并利用长期密钥进行加密运算，得到第一中间结果；

C) 利用第一参数组, 对所述第一中间结果进行第一运算处理, 得到第一运算结果, 将所述第一运算结果的前半部分的预设比特位与序列号 SQN 进行异或运算, 得到第一参数, 所述第一运算处理包括依次进行的异或运算、循环移位、异或运算、加密运算和异或运算处理;

D) 所述认证功能基于所述第一计算结果的后半部分、所述随机数 RAND 以及拜访网络标识, 生成一响应值 XRES*;

E) 利用第二参数组和第三参数组, 分别对所述第一中间结果进行所述第一运算处理, 得到认证流程后使用的会话加密密钥 CK 和会话完整性密钥 IK; 以及, 根据所述 CK、IK 和拜访地运营商的标识, 产生一中间密钥 K_{AUSF} ;

F) 将序列号 SQN、本地保存的认证所需的认证管理参数 AMF、SQN 以及 AMF 级联, 并利用第四参数组, 对级联得到的参数进行第二运算处理, 得到第二运算结果, 提取第二计算结果的前半部分, 得到第二参数;

这里, 第二运算处理包括依次进行的异或运算, 循环移位、异或运算、异或运算、加密运算和异或运算。

以上第一参数组至第四参数组, 各自均包括对应的位移参数和移位后用于异或运算的混淆参数。

G) 将所述第一参数、AMF、第二参数级联, 得到认证令牌 AUTN, 以及, 将所述 RAND、AUTN、XRES* 和 K_{AUSF} 作为认证向量参数, 得到认证向量。

更为详细的算法流程可以参看图 4 所示的流程描述, 此处不再赘述。

可选的, 在上述步骤 62 之后, 认证功能还可以向 UDM 发送携带有所述认证向量的认证向量响应消息。

根据本申请的至少一个实施例, 认证功能可以通过所述预设接口 Narpf 向 UDM 发送认证向量响应消息。具体的, 所述认证向量响应消息可以为 Narpf_authentication_get Response 消息。

以上介绍了本公开实施例的各种方法。下面将进一步提供实施上述方法的装置。

请参照图 7, 本公开实施例提供了一种 UDM 70, 包括:

第一接收模块 71, 用于接收到身份认证服务器功能 AUSF 发送的第一认

证向量请求消息;

发送模块 72, 用于在接收到所述第一认证向量请求消息后, 向认证功能发送第二认证向量请求消息, 所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识;

第二接收模块 73, 用于接收认证功能发送的携带有认证向量的认证向量响应消息。

可选的, 所述 UDM 与认证功能相互独立, 且两者之间存在有预设接口 Narpf。

所述发送模块 72, 还用于通过所述预设接口 Narpf 向认证功能发送所述第二认证向量请求消息, 以及, 所述第二接收模块 73, 还用于通过所述预设接口 Narpf 接收认证功能发送的携带有认证向量的认证向量响应消息。

可选的, 所述第二认证向量请求消息为 Narpf_authentication_get Request 消息; 所述认证向量响应消息为 Narpf_authentication_get Response 消息。

请参考图 8, 本公开实施例提供了 UDM 800 的一结构示意图, 包括: 处理器 801、收发机 802、存储器 803 和总线接口, 其中:

所述收发机 802, 用于接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息。

在本公开实施例中, UDM 800 还包括: 存储在存储器上 803 并可在处理器 801 上运行的程序, 所述程序被处理器 801 执行时实现如下步骤:

所述收发机 802, 用于在所述收发机接收到第一认证向量请求消息, 向认证功能发送第二认证向量请求消息, 所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识; 以及, 接收认证功能发送的携带有认证向量的认证向量响应消息。

可理解的, 本公开实施例中, 所述计算机程序被处理器 801 执行时可实现上述图 5 所示的认证向量的获取方法实施例的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

在图 8 中, 总线架构可以包括任意数量的互联的总线和桥, 具体由处理器 801 代表的一个或多个处理器和存储器 803 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的

各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 802 可以是多个元件，即包括发送机和接收机，提供用于在传输介质上与各种其他装置通信的单元。

处理器 801 负责管理总线架构和通常的处理，存储器 803 可以存储处理器 801 在执行操作时所使用的数据。

在本公开的一些实施例中，还提供了一种计算机可读存储介质，其上存储有程序，该程序被处理器执行时实现以下步骤：

在接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息后，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；

接收认证功能发送的携带有认证向量的认证向量响应消息。

该程序被处理器执行时能实现上述应用于 UDM 的认证向量的获取方法中的所有实现方式，且能达到相同的技术效果，为避免重复，此处不再赘述。

本公开实施例提供了图 9 所示的一种认证功能，包括：

接收模块 91，用于接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

计算模块 92，用于根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

可选的，上述认证功能还可以包括：

发送模块，用于向 UDM 发送携带有所述认证向量的认证向量响应消息

可选的，所述认证功能与 UDM 相互独立，且两者之间存在有预设接口 Narpf；

所述接收模块 91，还用于通过所述预设接口 Narpf 接收 UDM 发送的所述认证向量请求消息，以及，所述发送模块，还用于通过所述预设接口 Narpf 向 UDM 发送携带有所述认证向量的认证向量响应消息。

可选的，所述认证向量请求消息为 Narpf_authentication_get Request 消息；所述认证向量响应消息为 Narpf_authentication_get Response 消息。

可选的，计算模块 92，还用于按照以下方式计算得到认证向量：

获取长期密钥及其对应的序列号 SQN，并生成随机数 RAND；

对所述随机数 RAND 和运营商的配置参数 OPc 进行异或运算, 并利用长期密钥进行加密运算, 得到第一中间结果;

利用第一参数组, 对所述第一中间结果进行第一运算处理, 得到第一运算结果, 将所述第一运算结果的前半部分的预设比特位与序列号 SQN 进行异或运算, 得到第一参数, 所述第一运算处理包括依次进行的异或运算、循环移位、异或运算、加密运算和异或运算处理;

基于所述第一计算结果的后半部分、所述随机数 RAND 以及拜访网络标识, 生成一响应值 XRES*;

利用第二参数组和第三参数组, 分别对所述第一中间结果进行所述第一运算处理, 得到认证流程后使用的会话加密密钥 CK 和会话完整性密钥 IK; 以及, 根据所述 CK、IK 和拜访地运营商的标识, 产生一中间密钥 K_{AUSF};

将序列号 SQN、本地保存的认证所需的认证管理参数 AMF、SQN 以及 AMF 级联, 并利用第四参数组, 对级联得到的参数进行第二运算处理, 得到第二运算结果, 提取第二计算结果的前半部分, 得到第二参数;

将所述第一参数、AMF、第二参数级联, 得到认证令牌 AUTN, 以及, 将所述 RAND、AUTN、XRES* 和 K_{AUSF} 作为认证向量参数, 得到认证向量。

请参考图 10, 本公开实施例提供了认证功能 1000 的一结构示意图, 包括: 处理器 1001、收发机 1002、存储器 1003 和总线接口, 其中:

所述收发机 1002, 用于接收 UDM 发送的认证向量请求消息, 所述认证向量请求消息携带有用户身份标识和拜访网络标识;

在本公开实施例中, 认证功能 1000 还包括: 存储在存储器上 1003 并可在处理器 1001 上运行的程序, 所述程序被处理器 1001 执行时实现如下步骤:

根据所述用户身份标识, 获取本地存储的长期密钥, 并根据所述长期密钥和所述拜访网络标识, 计算得到认证向量。

可理解的, 本公开实施例中, 所述计算机程序被处理器 1001 执行时可实现上述图 6 所示的认证向量的生成方法实施例的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

在图 10 中, 总线架构可以包括任意数量的互联的总线和桥, 具体由处理器 1001 代表的一个或多个处理器和存储器 1003 代表的存储器的各种电路链

接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 1002 可以是多个元件，即包括发送机和接收机，提供用于在传输介质上与各种其他装置通信的单元。

处理器 1001 负责管理总线架构和通常的处理，存储器 1003 可以存储处理器 1001 在执行操作时所使用的数据。

在本公开的一些实施例中，还提供了一种计算机可读存储介质，其上存储有程序，该程序被处理器执行时实现以下步骤：

接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

该程序被处理器执行时能实现上述应用于认证功能的认证向量的生成方法中的所有实现方式，且能达到相同的技术效果，为避免重复，此处不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本公开的范围。

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

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

可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本公开实施例方案的目的。

另外，在本公开各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能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，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，本公开的技术方案本质上或者说对相关技术做出贡献的部分或者该技术方案的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计算机设备(可以是个人计算机，服务器，或者网络设备)执行本公开各个实施例所述的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、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本公开的具体实施方式，但本公开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公开揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以权利要求的保护范围为准。

权利要求书

1. 一种认证向量的生成方法，应用于认证功能，包括：

所述认证功能接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

所述认证功能根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

2. 如权利要求 1 所述的方法，其中，

所述认证功能与 UDM 相互独立，且两者之间存在有预设接口 Narpf；

所述认证功能通过所述预设接口 Narpf 接收 UDM 发送的所述认证向量请求消息，以及，通过所述预设接口 Narpf 向 UDM 发送携带有所述认证向量的认证向量响应消息。

3. 如权利要求 1 所述的方法，其中，

所述认证向量请求消息为 Narpf_authentication_get Request 消息；

所述认证向量响应消息为 Narpf_authentication_get Response 消息。

4. 如权利要求 1 所述的方法，其中，根据所述长期密钥和所述拜访网络标识，计算得到认证向量的步骤，包括：

所述认证功能获取长期密钥及其对应的序列号 SQN，并生成随机数 RAND；

所述认证功能对所述随机数 RAND 和运营商的配置参数 OPc 进行异或运算，并利用长期密钥进行加密运算，得到第一中间结果；

利用第一参数组，对所述第一中间结果进行第一运算处理，得到第一运算结果，将所述第一运算结果的前半部分的预设比特位与序列号 SQN 进行异或运算，得到第一参数；

所述认证功能基于所述第一计算结果的后半部分、所述随机数 RAND 以及拜访网络标识，生成一响应值 XRES*；

利用第二参数组和第三参数组，分别对所述第一中间结果进行所述第一运算处理，得到认证流程后使用的会话加密密钥 CK 和会话完整性密钥 IK；以及，根据所述 CK、IK 和拜访地运营商的标识，产生一中间密钥 K_{AUSF}；

将序列号 SQN、本地保存的认证所需的认证管理参数 AMF、SQN 以及 AMF 级联，并利用第四参数组，对级联得到的参数进行第二运算处理，得到第二运算结果，提取第二计算结果的前半部分，得到第二参数；

将所述第一参数、AMF、第二参数级联，得到认证令牌 AUTN，以及，将所述 RAND、AUTN、XRES*和 K_{AUSF} 作为认证向量参数，得到认证向量。

5. 一种认证向量的获取方法，应用于统一数据管理 UDM，包括：

所述 UDM 在接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息后，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；

所述 UDM 接收认证功能发送的携带有认证向量的认证向量响应消息。

6. 如权利要求 5 所述的方法，其中，

所述 UDM 与认证功能相互独立，且两者之间存在有预设接口 Narpf；

所述 UDM 通过所述预设接口 Narpf 向认证功能发送所述第二认证向量请求消息，以及，通过所述预设接口 Narpf 接收认证功能发送的携带有认证向量的认证向量响应消息。

7. 如权利要求 5 所述的方法，其中，

所述第二认证向量请求消息为 Narpf_authentication_get Request 消息；

所述认证向量响应消息为 Narpf_authentication_get Response 消息。

8. 一种认证功能，包括：

接收模块，用于接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

计算模块，用于根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

9. 一种认证功能，包括收发机和处理器，其中，

所述收发机，用于接收 UDM 发送的认证向量请求消息，所述认证向量请求消息携带有用户身份标识和拜访网络标识；

所述处理器，用于根据所述用户身份标识，获取本地存储的长期密钥，并根据所述长期密钥和所述拜访网络标识，计算得到认证向量。

10. 一种认证功能，包括：处理器、存储器及存储在所述存储器上并可

在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 1 至 4 任一项所述的方法的步骤。

11. 一种 UDM，包括：

第一接收模块，用于接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息；

发送模块，用于在接收到所述第一认证向量请求消息后，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；

第二接收模块，用于接收认证功能发送的携带有认证向量的认证向量响应消息。

12. 一种 UDM，包括收发机和处理器，其中，

所述收发机，用于接收到身份认证服务器功能 AUSF 发送的第一认证向量请求消息；

所述处理器，用于在所述收发机接收到第一认证向量请求消息，向认证功能发送第二认证向量请求消息，所述第二认证向量请求消息携带有用户的身份标识和拜访网络标识；以及，接收认证功能发送的携带有认证向量的认证向量响应消息。

13. 一种 UDM，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 5 至 7 任一项所述的方法的步骤。

14. 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 7 任一项所述的方法的步骤。

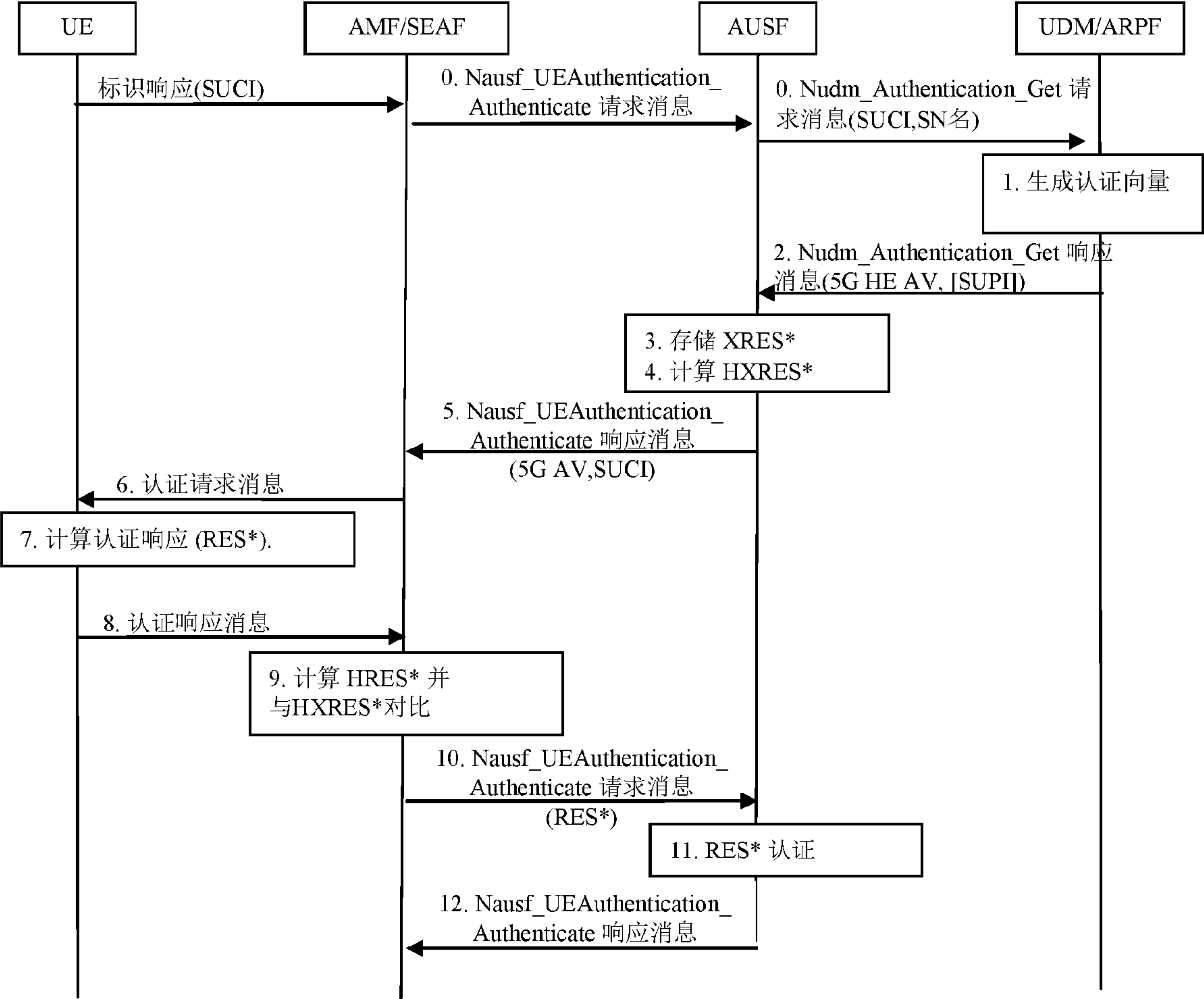


图 1

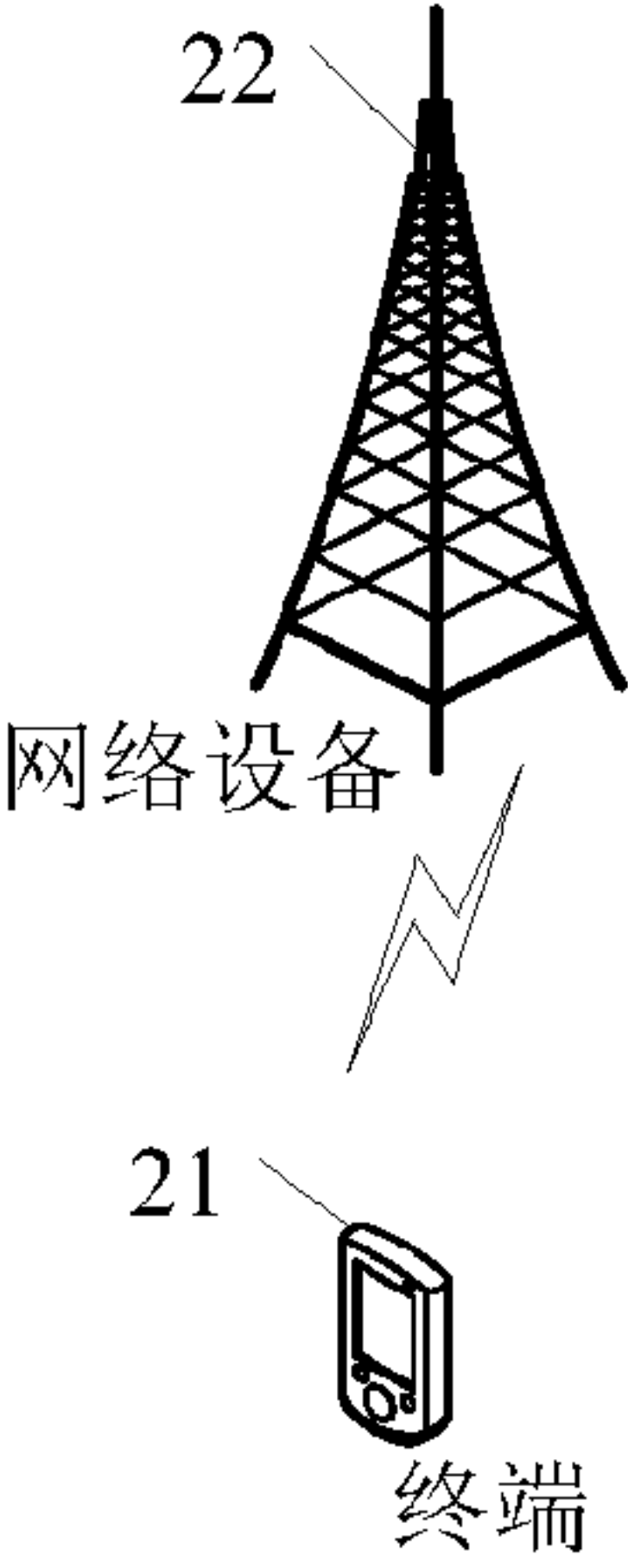


图 2

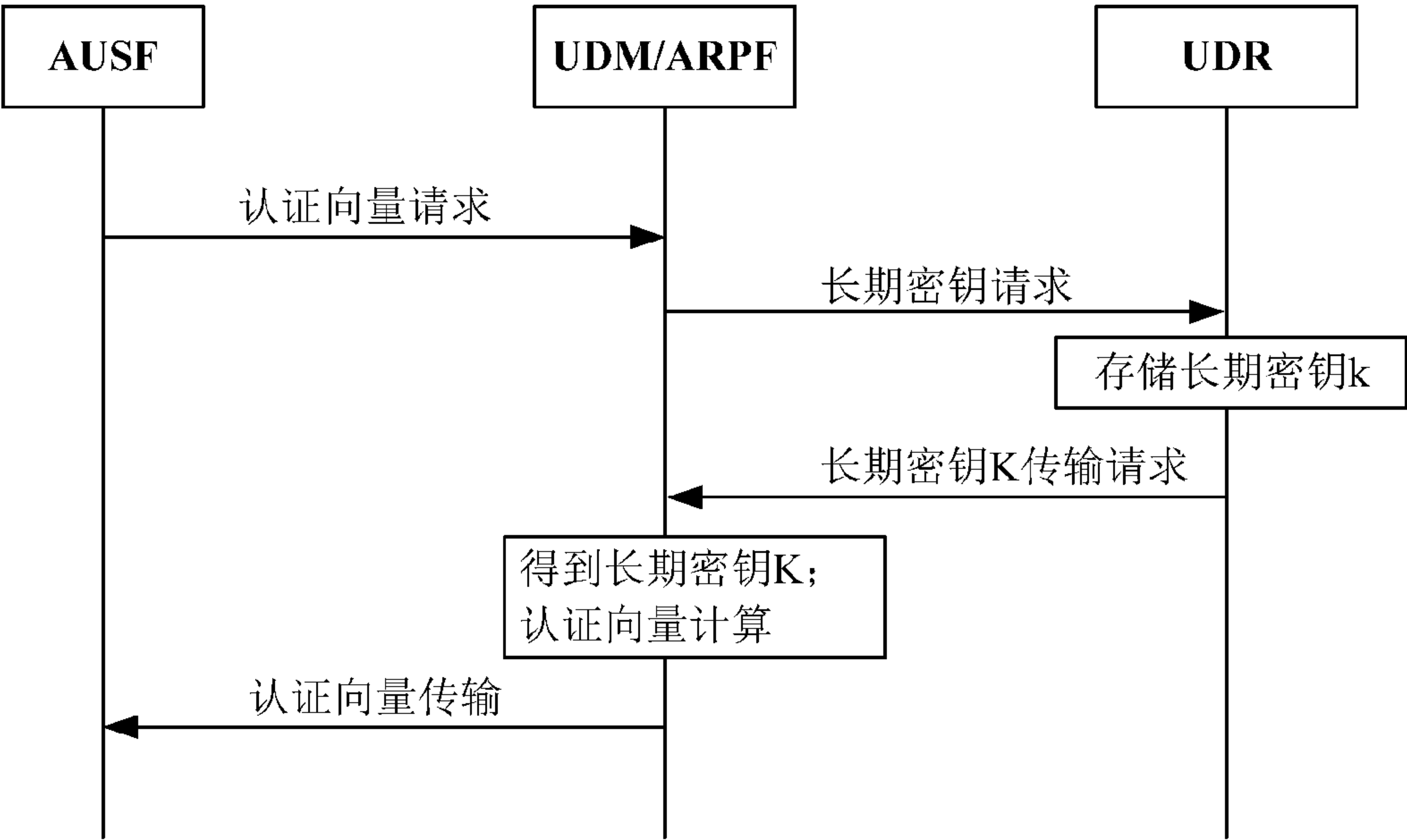


图 3

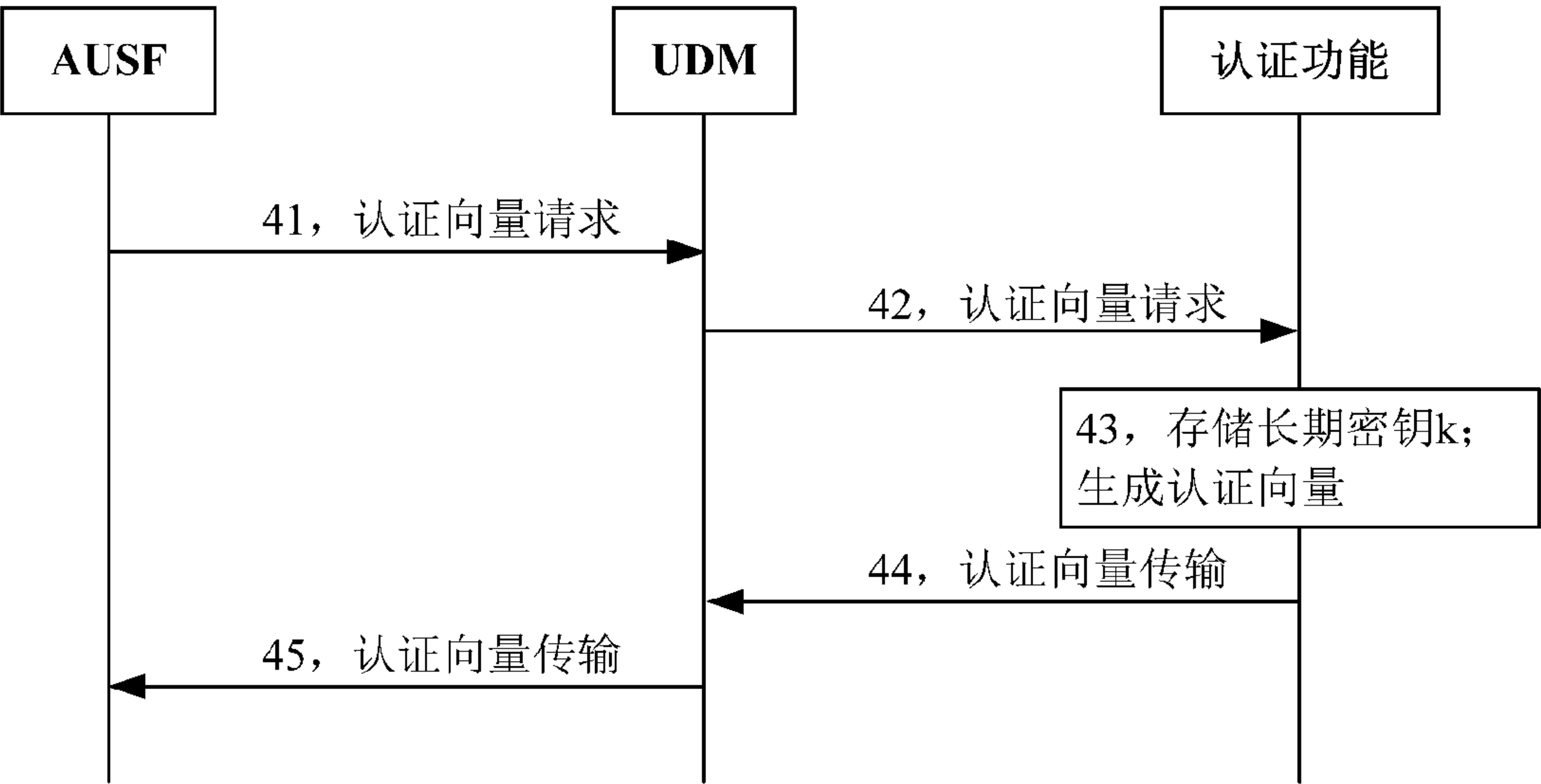


图 4

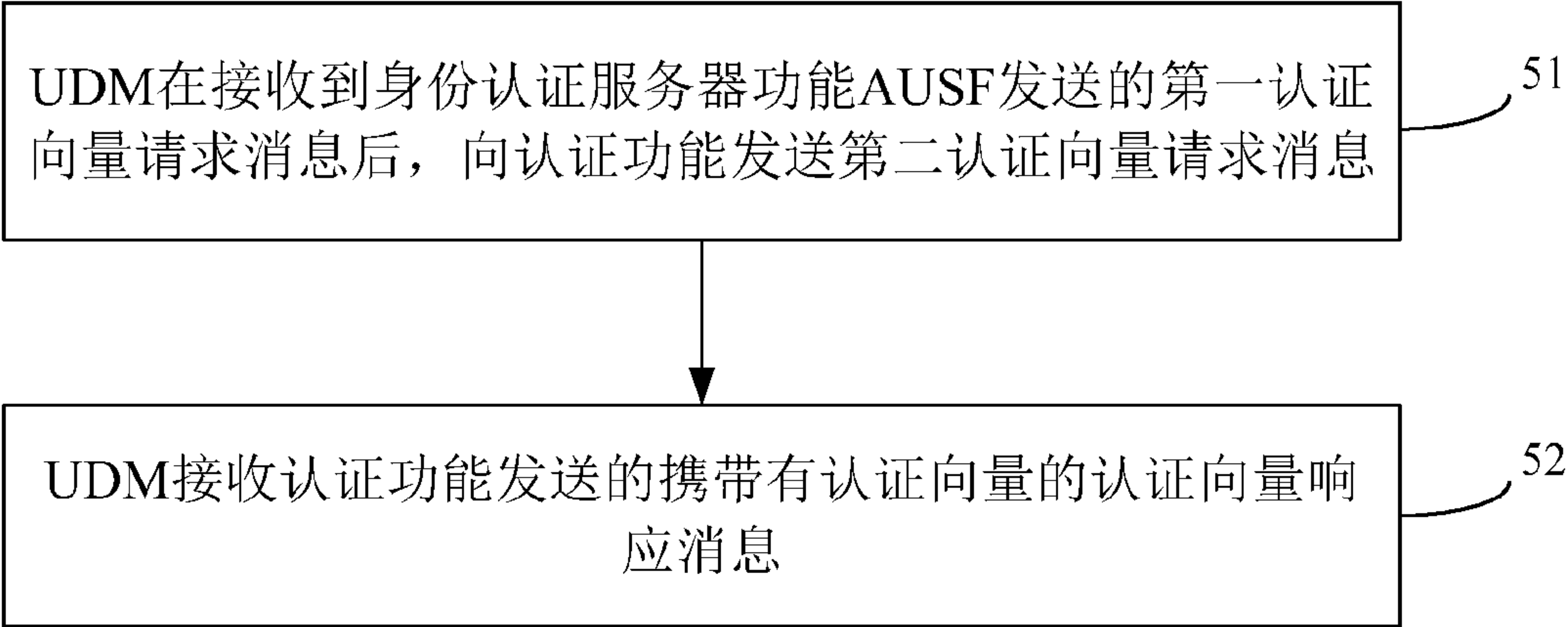


图 5

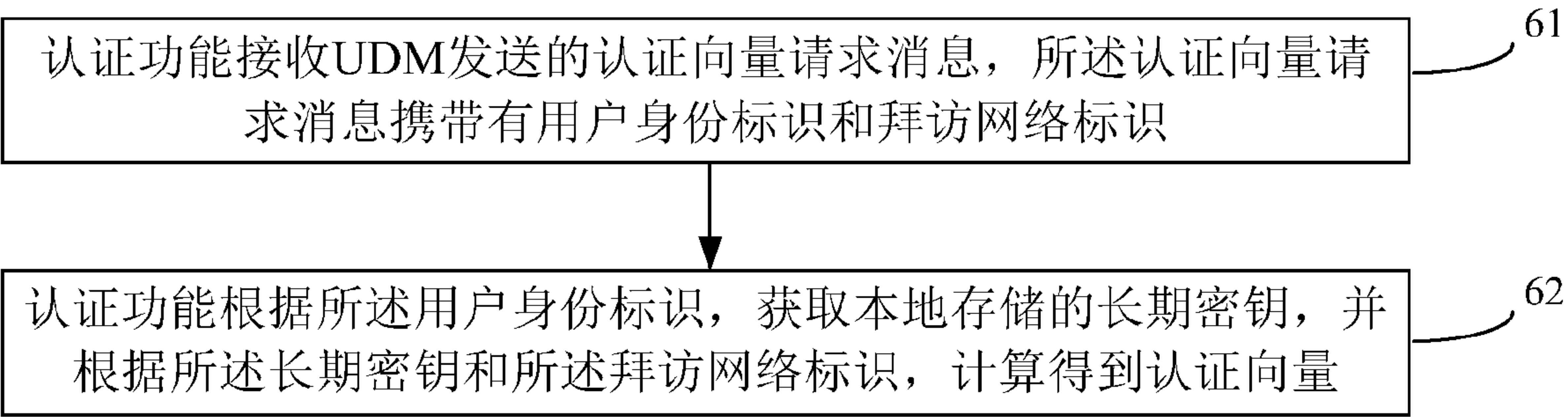


图 6

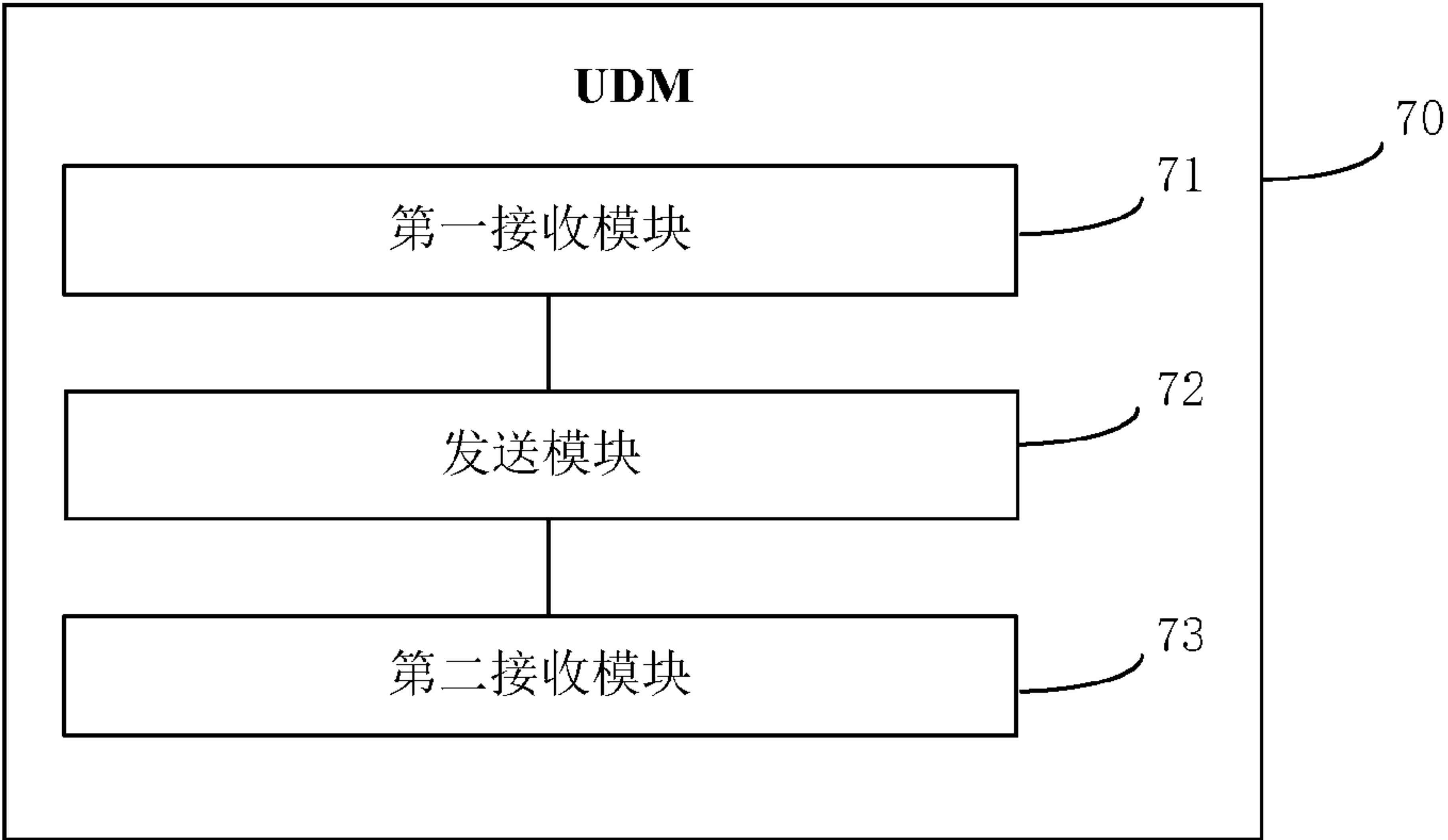


图 7

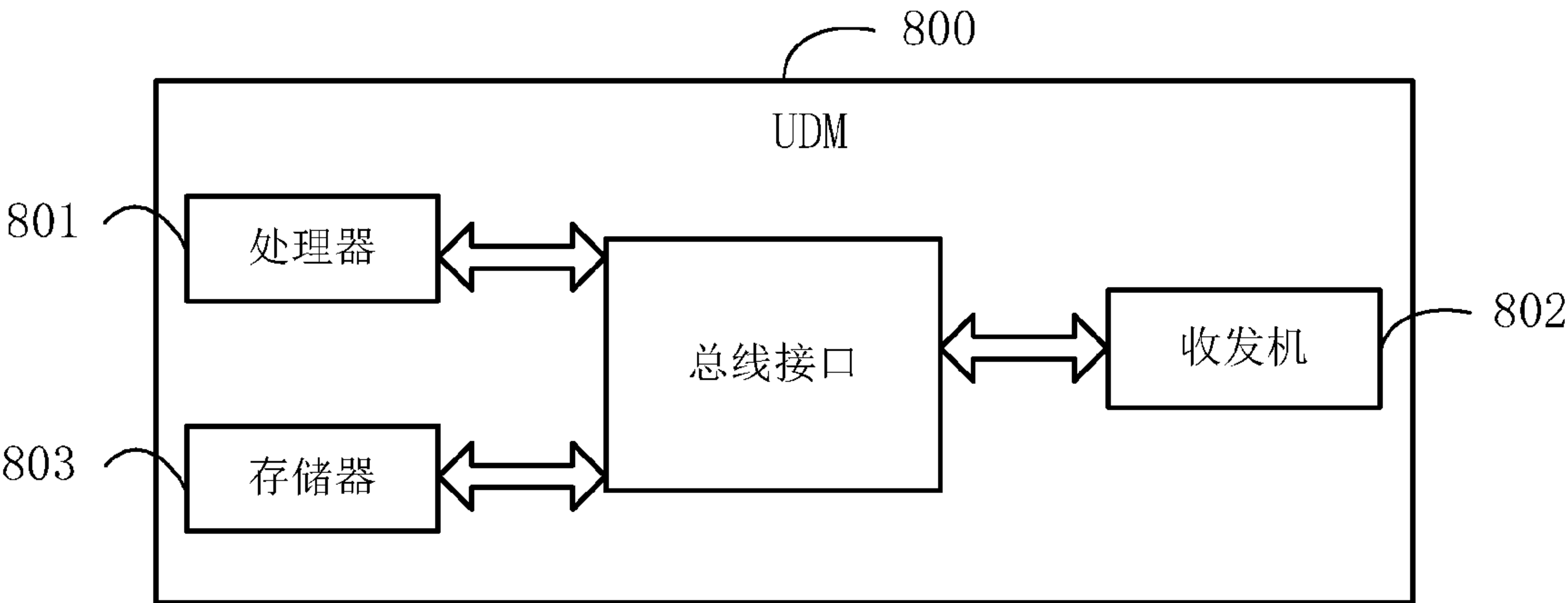


图 8

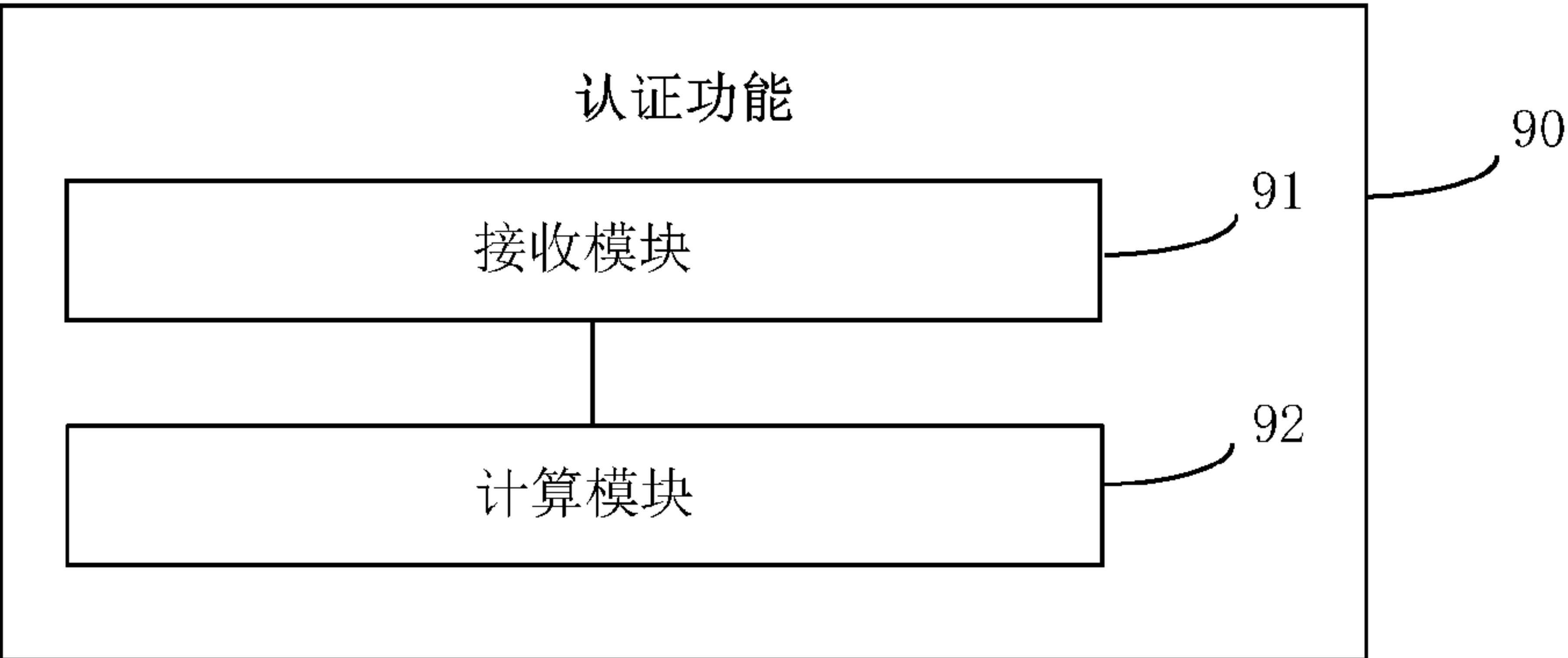


图 9

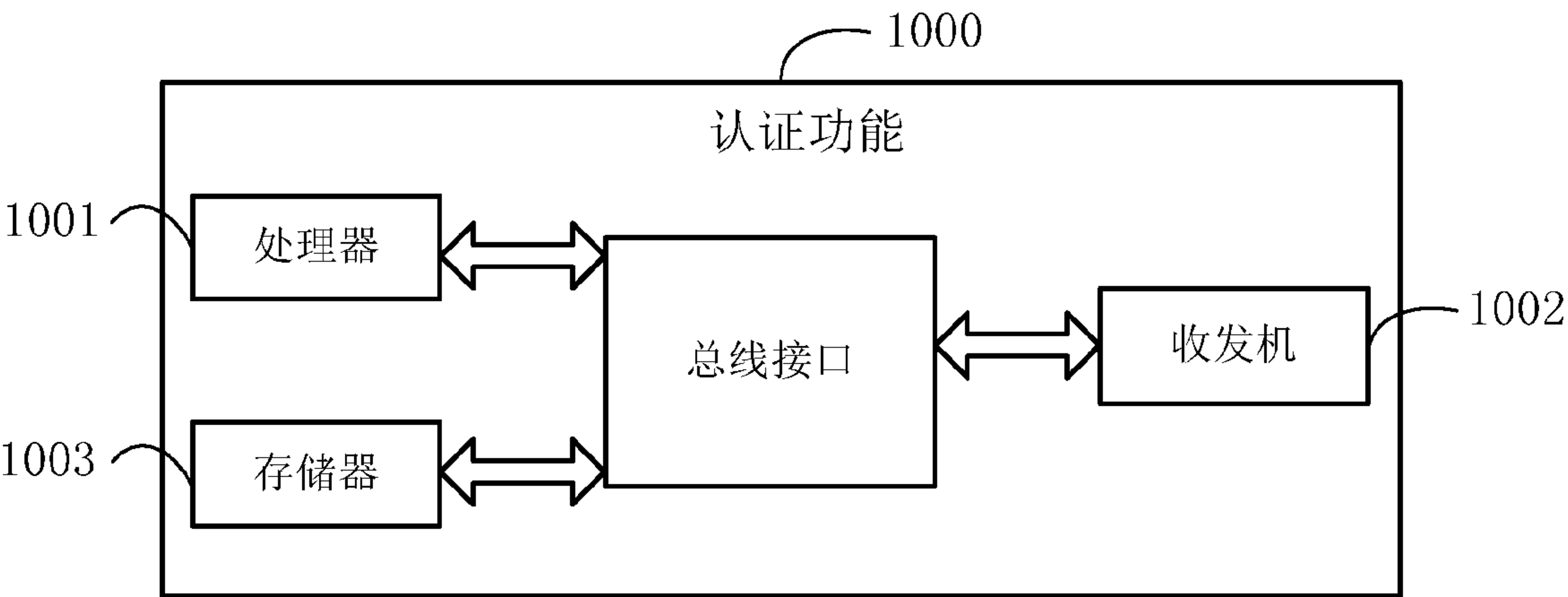


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/122423

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(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

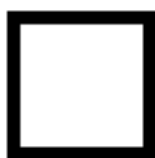
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; 3GPP: 认证, 鉴权, 向量, 矢量, 用户, 身份, 标识, 拜访网络, 密钥, 统一数据管理, 独立, 分离, 分别, 生成, 获取, 认证请求, authentication, vector, user, identity, identifier, ID, visited network, key, UDM, separate, independently, generate, authentication request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110035433 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 July 2019 (2019-07-19) description, paragraphs [0002]-[0004], [0495]-[0523]	1-14
A	CN 102209066 A (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) 05 October 2011 (2011-10-05) entire document	1-14
A	CN 110062381 A (HUAWEI TECHNOLOGIES CO., LTD.) 26 July 2019 (2019-07-26) entire document	1-14
A	CN 110149623 A (ZTE CORPORATION) 20 August 2019 (2019-08-20) entire document	1-14
A	WO 2019017689 A1 (SAMSUNG ELECTRONICS CO., LTD.) 24 January 2019 (2019-01-24) entire document	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search

05 January 2021

Date of mailing of the international search report

13 January 2021

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/CN2020/122423

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110035433	A	19 July 2019	None			
CN	102209066	A	05 October 2011	CN	102209066	B	11 March 2015
CN	110062381	A	26 July 2019	None			
CN	110149623	A	20 August 2019	None			
WO	2019017689	A1	24 January 2019	KR	20200022045	A	02 March 2020
				US	2020221281	A1	09 July 2020
				EP	3656141	A1	27 May 2020
				CN	110945886	A	31 March 2020
				EP	3656141	A4	27 May 2020

国际检索报告		国际申请号 PCT/CN2020/122423
A. 主题的分类 H04L 9/08 (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)) CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; 3GPP: 认证, 鉴权, 向量, 矢量, 用户, 身份, 标识, 拜访网络, 密钥, 统一数据管理, 独立, 分离, 分别, 生成, 获取, 认证请求, authentication, vector, user, identity, identifier, ID, visited network, key, UDM, separate, independently, generate, authentication request		
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 110035433 A (华为技术有限公司) 2019年 7月 19日 (2019 - 07 - 19) 说明书第[0002]-[0004]、[0495]-[0523]段	1-14
A	CN 102209066 A (中国移动通信集团公司) 2011年 10月 5日 (2011 - 10 - 05) 全文	1-14
A	CN 110062381 A (华为技术有限公司) 2019年 7月 26日 (2019 - 07 - 26) 全文	1-14
A	CN 110149623 A (中兴通讯股份有限公司) 2019年 8月 20日 (2019 - 08 - 20) 全文	1-14
A	WO 2019017689 A1 (SAMSUNG ELECTRONICS CO LTD) 2019年 1月 24日 (2019 - 01 - 24) 全文	1-14
☐ 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 2021年 1月 5日		国际检索报告邮寄日期 2021年 1月 13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		授权官员 鲁秋艳 电话号码 86-010-62089459

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/122423

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	110035433	A	2019年 7月 19日	无			
CN	102209066	A	2011年 10月 5日	CN	102209066	B	2015年 3月 11日
CN	110062381	A	2019年 7月 26日	无			
CN	110149623	A	2019年 8月 20日	无			
WO	2019017689	A1	2019年 1月 24日	KR	20200022045	A	2020年 3月 2日
				US	2020221281	A1	2020年 7月 9日
				EP	3656141	A1	2020年 5月 27日
				CN	110945886	A	2020年 3月 31日
				EP	3656141	A4	2020年 5月 27日