(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
2019 年 5 月 23 日 (23.05.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/096051 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2018/114461

(22) 国际申请日: 2018 年 11 月 8 日 (08.11.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711148923.1 2017年11月17日 (17.11.2017) 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: 何承东(**HE, Chengdong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李华(**LI, Hua**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

(54) **Title:** AUTHENTICATION METHOD, DEVICE AND SYSTEM

(54) 发明名称: 鉴权方法、设备及系统

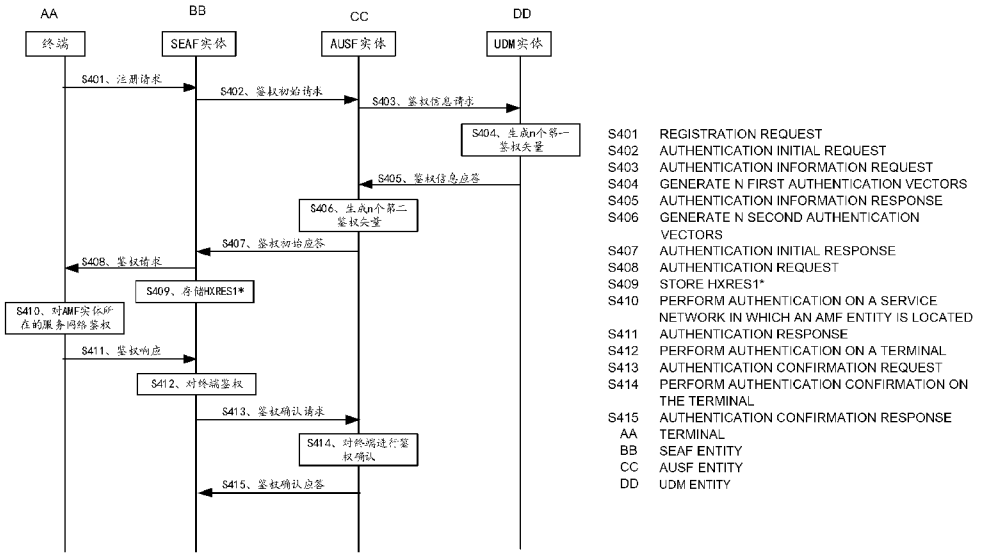


图 4

(57) **Abstract:** Provided in embodiments of the present application are an authentication method, device and system, to at least solve the problem in handling performance and memory resource wastes possibly caused by remaining unused n-1 AVs. The method comprises: receiving by an authentication entity a number n of first authentication vectors from a unified data management entity, n being a positive integer; generating by the authentication entity n second authentication vectors according to the n first authentication vectors; sending by the authentication entity one of the n second authentication vectors to a secure anchor functional entity; receiving by the authentication entity an authentication confirmation request from the secure anchor functional entity, and performing authentication confirmation on a terminal according to the authentication confirmation request; and in the case that the authentication confirmation is successful, sending by the authentication entity the other n-1 unused second authentication vectors in the n second authentication vectors to the secure anchor functional entity.

WO 2019/096051 A1

[见续页]

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))。

(57) 摘要: 本申请实施例提供鉴权方法、设备及系统，以至少解决如何处理剩下未使用的n-1个AV而可能产生的性能和内存资源浪费的问题。方法包括：鉴权实体接收来自统一数据管理实体的n个第一鉴权矢量，n为正整数；该鉴权实体根据该n个第一鉴权矢量，生成n个第二鉴权矢量；该鉴权实体向安全锚点功能实体发送该n个第二鉴权矢量中的其中一个第二鉴权矢量；该鉴权实体接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认；在鉴权确认成功的情况下，该鉴权实体向该安全锚点功能实体发送该n个第二鉴矢量中其他未使用的n-1个第二鉴权矢量。

鉴权方法、设备及系统

本申请要求于2017年11月17日提交中国国家知识产权局、申请号为201711148923.1、发明名称为“鉴权方法、设备及系统”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，尤其涉及鉴权方法、设备及系统。

背景技术

在第三代合作伙伴计划（3rd generation partnership project，3GPP）技术标准（technical standard，TS）33.501 v0.40 所描述的用户注册过程的鉴权流程中，若归属网络中的统一数据管理（unified data management，UDM）实体选择的鉴权算法为第五代认证和密钥协商（5rd generation-authentication and key agreement，5G-AKA），则 UDM 实体可能一次产生 n 个鉴权矢量（authentication vector，AV），n 为正整数。进而，归属网络中的鉴权服务器功能（authentication server function，AUSF）实体可以接收来自 UDM 实体的 n 个 AV。但对于某些信任类别较低的拜访网络中的安全锚点功能（security anchor function，SEAF）实体，AUSF 实体可能仅向 SEAF 实体发送一个 AV，当 n＞1 时，现有技术并没有明确说明剩下未使用的 n-1 个 AV 如何处理。若剩下未使用的 n-1 个 AV 都保存在 AUSF 实体，可能产生如下问题：

第一，可能对 AUSF 实体和 UDM 实体的处理性能产生一定影响。

第二，剩下未使用的 n-1 个 AV 保存在 AUSF 实体上将会占用 AUSF 实体的内存，比如若 n=10，由于 AV 包括随机数（random number，RAND）、鉴权令牌（authentication token，AUTN）、期望的响应值（expected response，XRES*）和密钥 Kasme*，而 AUTN 和 RAND 分别占用 16 个字节，XRES*占用 16 个字节，Kasme*占用 32 个字节，则对于一个用户来说，n-1 个 AV 保存在 AUSF 实体上将会占用 9*（16+16+16+32）=800 个字节；对于 1000 万用户来说，n-1 个 AV 保存在 AUSF 实体上将会占用 1000 万*800=7.5GB 内存。

因此，如何处理剩下未使用的 n-1 个 AV 而可能产生的性能和内存资源浪费的问题，是目前亟待解决的技术问题。

发明内容

本申请实施例提供鉴权方法、设备及系统，以至少解决如何处理剩下未使用的 n-1 个 AV 而可能产生的性能和内存资源浪费的问题。

为达到上述目的，本申请实施例提供如下技术方案：

第一方面，提供一种鉴权方法，该方法包括：鉴权实体接收来自统一数据管理实体的 n 个第一鉴权矢量，n 为正整数；该鉴权实体根据该 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；该鉴权实体向安全锚点功能实体发送该 n 个第二鉴权矢量中的其中一个第二鉴权矢量；该鉴权实体接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终

端进行鉴权确认；在鉴权确认成功的情况下，该鉴权实体向该安全锚点功能实体发送该 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。基于该方案，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

在一种可能的设计中，该方法还包括：该鉴权实体向该安全锚点功能实体发送鉴权确认标识，其中，该鉴权确认标识用于指示需要鉴权确认。这样后续 SEAF 实体对终端鉴权成功后，可以根据该鉴权确认标识向 AUSF 实体发送鉴权确认请求，由 AUSF 实体进一步对终端进行鉴权确认。

在一种可能的设计中，该方法还包括：该鉴权实体确定需要鉴权确认。

可选的，该鉴权实体确定需要鉴权确认，包括：该鉴权实体接收来自该统一数据管理实体的鉴权确认标识，其中，该鉴权确认标识用于指示需要鉴权确认。也就是说，可以由统一数据管理实体确定是否需要鉴权确认，从而可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

可选的，该鉴权实体确定需要鉴权确认，包括：该鉴权实体根据本地配置的安全策略，确定需要鉴权确认。

在一种可能的设计中，该鉴权确认请求携带响应值 RES*和对应的随机数 RAND；该鉴权实体根据该鉴权确认请求对该终端进行鉴权确认，包括：该鉴权实体根据该 RAND 查找对应的 XRES*，并通过比较该 RES*和该 XRES*对该终端进行鉴权确认。通过该方式，在鉴权实体接收来自安全锚点功能实体的鉴权确认请求之后，由于可以快速查找到与 RES*对应的 XRES*，因此可以解决现有技术中在进行鉴权确认时，在鉴权实体之前从统一数据管理实体中接收多个第一鉴权矢量的情况下，鉴权实体不知道使用哪个鉴权矢量中的 XRES*和接收到的 RES*进行比较，从而影响 AUSF 实体的处理性能的问题，可以实现对终端的快速鉴权确认。

第二方面，提供一种鉴权方法，该方法包括：统一数据管理实体生成 n 个第一鉴权矢量，n 为正整数；该统一数据管理实体向鉴权实体发送该 n 个第一鉴权矢量；该鉴权实体接收来自该统一数据管理实体的 n 个第一鉴权矢量，并根据该 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；该鉴权实体向安全锚点功能实体发送该 n 个第二鉴权矢量中的其中一个第二鉴权矢量；该鉴权实体接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认；在鉴权确认成功的情况下，该鉴权实体向该安全锚点功能实体发送该 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。其中，第二方面所带来的技术效果可参见第一方面所带来的技术效果，此处不再赘述。

在一种可能的设计中，该统一数据管理实体生成 n 个第一鉴权矢量，包括：该统一数据管理实体根据本地配置的缺省鉴权矢量数目 n，生成 n 个第一鉴权矢量。本申请实施例中，由于统一数据管理实体可以根据鉴权算法，生成相应数量的第一鉴权矢量，而不

是像现有技术一样，在鉴权实体发送给统一数据实体的鉴权信息请求中携带鉴权矢量的个数，因此可以避免现有技术中存在的鉴权实体请求的第一鉴权矢量的数量与统一数据实体生成的第一鉴权矢量的数量不一致的问题。比如，若鉴权实体请求的第一鉴权矢量的数量为多个，而统一数据管理实体选择的鉴权算法一次仅生成一个第一鉴权矢量，则无法满足鉴权实体请求的第一鉴权矢量的数量要求。

在一种可能的设计中，该方法还包括：该统一数据管理实体根据本地配置的安全策略，确定需要鉴权确认；该统一数据管理实体向该鉴权实体发送鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认；该鉴权实体接收来自该统一数据管理实体的该鉴权确认标识，并向该安全锚点功能实体发送该鉴权确认标识。

在一种可能的设计中，该统一数据管理实体根据本地配置的安全策略，确定需要鉴权确认，包括：该统一数据管理实体根据该安全锚点功能实体所在的服务网络的标识，以及该本地配置的安全策略中该服务网络的安全策略，确定需要鉴权确认。也就是说，可以由统一数据管理实体确定是否需要鉴权确认，从而可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

第三方面，提供一种鉴权方法，该方法包括：统一数据管理实体根据本地配置的安全策略，确定需要鉴权确认；该统一数据管理实体向鉴权实体发送鉴权信息应答，该鉴权信息应答携带鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认；该鉴权实体接收来自该统一数据实体的该鉴权信息应答；该鉴权实体向安全锚点功能实体发送鉴权初始应答，该鉴权初始应答携带该鉴权确认标识；该鉴权实体接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认。基于该方案，可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

在一种可能的设计中，该方法还包括：该统一数据管理实体生成 n 个第一鉴权矢量；相应的，该鉴权信息应答还携带 n 个第一鉴权矢量；该方法还包括：该鉴权实体根据该 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；相应的，该鉴权初始应答还携带该 n 个第二鉴权矢量中的其中一个第二鉴权矢量；在该鉴权实体接收来自该安全锚点功能实体的鉴权确认请求之后，该方法还包括：在鉴权确认成功的情况下，该鉴权实体向该安全锚点功能实体发送该 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。基于该方案，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

在一种可能的设计中，该方法还包括：该统一数据管理实体生成 n 个第一鉴权矢量；相应的，该鉴权信息应答还携带 n 个第一鉴权矢量；该方法还包括：该鉴权实体根据该 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；相应的，该鉴权初始应答还携带该 n 个第二鉴权矢量。基于该方案，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；

而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

结合上述第一方面至第三方面，在一种可能的设计中，在鉴权实体根据鉴权确认请求对终端进行鉴权确认之后，还包括：在鉴权确认失败的情况下，鉴权实体向安全锚点功能实体发送鉴权确认失败指示，该鉴权确认失败指示用于指示鉴权确认失败。这样可以使得安全锚点功能实体及时获知鉴权确认的结果。

结合上述第一方面至第三方面，在一种可能的设计中，在鉴权实体根据鉴权确认请求对终端进行鉴权确认之后，还包括：在鉴权确认成功的情况下，鉴权实体向安全锚点功能实体发送鉴权确认成功指示，该鉴权确认成功指示用于指示鉴权确认成功。这样可以使得安全锚点功能实体及时获知鉴权确认的结果。

结合上述第一方面至第三方面，在一种可能的设计中，在鉴权实体根据鉴权确认请求对终端进行鉴权确认之后，还包括：在鉴权确认成功的情况下，鉴权实体向安全锚点功能实体发送鉴权确认标识，其中，该鉴权确认标识用于指示需要鉴权确认。

第四方面，提供一种鉴权方法，该鉴权方法包括：统一数据管理实体根据本地配置的安全策略，生成 n 个第一鉴权矢量，n 为正整数；统一数据管理实体向鉴权实体发送 n 个第一鉴权矢量；鉴权实体接收来自该统一数据实体的 n 个第一鉴权矢量，并根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；鉴权实体向该安全锚点功能实体发送该 n 个第二鉴权矢量。基于该方法，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性；同时，还可以避免现有技术中存在的鉴权实体请求的第一鉴权矢量的数量与统一数据管理实体实际生成的第一鉴权矢量的数量不一致的问题。相关技术效果的分析可参考下述方法实施例部分，在此不再赘述。

在一种可能的设计中，该方法还包括：鉴权实体接收来自安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认；在鉴权确认失败的情况下，该鉴权实体向该安全锚点功能实体发送鉴权确认失败指示，该鉴权确认失败指示用于指示鉴权确认失败。这样可以使得安全锚点功能实体及时获知鉴权确认的结果。

在一种可能的设计中，该方法还包括：鉴权实体接收来自安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认；在鉴权确认成功的情况下，该鉴权实体向该安全锚点功能实体发送鉴权确认成功指示，该鉴权确认成功指示用于指示鉴权确认成功。

在一种可能的设计中，统一数据管理实体根据本地配置的安全策略，生成 n 个第一鉴权矢量，包括：统一数据管理实体根据该安全锚点功能实体所在的服务网络的标识，以及该本地配置的安全策略中该服务网络的安全策略，生成 n 个第一鉴权矢量。

第五方面，提供了一种鉴权实体，该鉴权实体具有实现上述第一方面所述的方法的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

第六方面，提供了一种鉴权实体，包括：处理器和存储器；该存储器用于存储计算机执行指令，当该鉴权实体运行时，该处理器执行该存储器存储的该计算机执行指令，以使该鉴权实体执行如上述第一方面中任一所述的鉴权方法。

第七方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第一方面中任意一项所述的鉴权方法。

第八方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面中任意一项所述的鉴权方法。

第九方面，提供了一种芯片系统，该芯片系统包括处理器，用于支持鉴权实体实现上述方面中所涉及的功能，例如根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存鉴权实体必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第五方面至第九方面中任一种设计方式所带来的技术效果可参见第一方面中不同设计方式所带来的技术效果，此处不再赘述。

第十方面，提供一种鉴权系统，该鉴权系统包括统一数据管理实体和鉴权实体；该统一数据管理实体，用于生成 n 个第一鉴权矢量，n 为正整数；该统一数据管理实体，还用于向鉴权实体发送该 n 个第一鉴权矢量；该鉴权实体，用于接收来自该统一数据管理实体的 n 个第一鉴权矢量，并根据该 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；该鉴权实体，还用于向安全锚点功能实体发送该 n 个第二鉴权矢量中的其中一个第二鉴权矢量；该鉴权实体，还用于接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认；该鉴权实体，还用于在鉴权确认成功的情况下，向该安全锚点功能实体发送该 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。其中，第十方面所带来的技术效果可参见第二方面所带来的技术效果，此处不再赘述。

第十一方面，提供一种鉴权系统，该鉴权系统包括：统一数据管理实体和鉴权实体；该统一数据管理实体，用于根据本地配置的安全策略，确定需要鉴权确认；该统一数据管理实体，还用于向鉴权实体发送鉴权信息应答，该鉴权信息应答携带鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认；该鉴权实体，用于接收来自该统一数据实体的该鉴权信息应答；该鉴权实体，还用于向安全锚点功能实体发送鉴权初始应答，该鉴权初始应答携带该鉴权确认标识；该鉴权实体，还用于接收来自该安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对该终端进行鉴权确认。其中，第十一方面所带来的技术效果可参见第三方面所带来的技术效果，此处不再赘述。

本申请的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

附图说明

图 1 为本申请实施例提供的鉴权系统的架构示意图；

图 2 为本申请实施例提供的 5G 网络架构的示意图；

图 3 为本申请实施例提供的通信设备的硬件结构示意图；

图 4 为本申请实施例提供的鉴权方法的流程示意图一；

图 5 为本申请实施例提供的鉴权方法的流程示意图二；

图 6 为本申请实施例提供的鉴权实体的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。其中，在本申请的描述中，除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本文中的“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。并且，在本申请的描述中，除非另有说明，“多个”是指两个或多于两个。另外，为了便于清楚描述本申请实施例的技术方案，在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同，本申请实施例对此不作具体限定。

本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络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。

如图 1 所示，为本申请实施例提供的一种鉴权系统 10，该鉴权系统 10 包括统一数据管理实体 101 和鉴权实体 102。其中，统一数据管理实体 101 和鉴权实体 102 之间可以直接通信，也可以通过其他设备的转发进行通信，本申请实施例对此不作具体限定。

一种可能的实现方式中，统一数据管理实体 101，用于生成 n 个第一鉴权矢量，并向鉴权实体 102 发送 n 个第一鉴权矢量，n 为正整数。

鉴权实体 102，用于接收来自统一数据实体 101 的 n 个第一鉴权矢量，并根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量。

鉴权实体 102，还用于向安全锚点功能实体发送 n 个第二鉴权矢量中的其中一个第二鉴权矢量。

鉴权实体 102，还用于接收来自安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对终端进行鉴权确认；在鉴权确认成功的情况下，向安全锚点功能实体发送 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。

其中，本申请实施例中的第一鉴权矢量可以包括 RAND、AUTN、XRES*和 Kasme*。与该第一鉴权矢量对应的第二鉴权矢量可以包括 RAND、AUTN、哈希（Hash） XRES*（HXRES*）和 Kasme*，在此统一说明，以下不再赘述。其中，HXRES*是根据 RAND 和 XRES*确定的，具体可参考现有的实现方式，本申请实施例对此不予赘述。

本申请实施例提供的鉴权系统中，鉴权实体在根据接收到的 n 个第一鉴权矢量生成 n 个第二鉴权矢量之后，向安全锚点功能实体发送 n 个第二鉴权矢量中的其中一个第二鉴权矢量，并在接收来自安全锚点功能实体的鉴权确认请求，且根据鉴权确认请求对终端进行鉴权确认成功之后，向安全锚点功能实体发送 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。这样，一方面，不仅可以避免每次服务网络的安全锚点功能实体重新对终端鉴权时，均需要向归属网络的鉴权实体请求第一鉴权矢量，从而对鉴权实体的处理性能产生的影响；

也可以避免归属网络中的鉴权实体并不知道拜访网络中的安全锚点功能实体何时会再次发起鉴权，比如终端已经离开了安全锚点功能实体所在的拜访网络，或者，比如距离下次安全锚点功能实体会再次发起鉴权的时间还很长。此时若采用老化删除机制，则安全锚点功能实体向鉴权实体再次请求第一鉴权矢量时，由于第一鉴权矢量已经老化被删除，统一数据管理实体还得重新生成需要的第一鉴权矢量，从而对统一数据管理实体的处理性能产生的影响；同时可以避免安全锚点功能实体向鉴权实体再次请求第一鉴权矢量时，由于安全锚点功能实体和鉴权实体之间因为链路不通而导致获取不到第一鉴权矢量，从而对终端鉴权失败的问题。另一方面，可以解决现有技术中存在的剩下未使用的 n-1 个第一鉴权矢量可能产生的鉴权实体的内存资源浪费的问题。也就是说，基于该方案，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。

另一种可能的实现方式中，统一数据管理实体 101，用于根据本地配置的安全策略，生成 n 个第一鉴权矢量，并向鉴权实体 102 发送 n 个第一鉴权矢量 n 为正整数。

鉴权实体 102，用于接收来自统一数据实体 101 的 n 个第一鉴权矢量，并根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量后，向安全锚点功能实体发送 n 个第二鉴权矢量。

可选的，本申请实施例中，本地配置的安全策略可以包括不同服务网络的安全策略列表，该安全策略列表中可以包括当前为终端服务的安全锚点功能实体所在的服务网络的安全策略，本申请实施例对此不作具体限定。

其中，本申请实施例中，服务网络的安全策略具体可以包括服务网络的信任等级，该服务网络的信任等级例如可以包括信任等级高或信任等级低。信任等级高表示信任该服务网络；信任等级低表示不信任该服务网络。在此统一说明，以下不再赘述。

其中，本申请实施例中的服务网络可以是归属网络，比如可以是终端非漫游场景下的归属地公共陆地移动网络（home public land mobile network，HPLMN）；或者，该服务网络也可以是拜访网络，比如可以是终端漫游场景下的访问地公共陆地移动网络（visited public land mobile network，VPLMN），本申请实施例对此不作具体限定。在此统一说明，以下不再赘述。

示例性的，本地配置的安全策略可以如表一所示。

表一

服务网络	安全策略
PLMN1	信任等级高
PLMN2	信任等级高
PLMN3	信任等级低
PLMN4	信任等级高
……	……

需要说明的是，表一仅是示例性的给出了一种本地配置的安全策略的列表形式，当然，本地配置的安全策略还可能是其他的形式，比如文本形式等，本申请实施例对此不作具体限定。

本申请实施例提供的鉴权系统中，鉴权实体根据本地配置的安全策略，生成 n 个第一鉴权矢量，并向鉴权实体发送 n 个第一鉴权矢量，由鉴权实体根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量之后，向安全锚点功能实体发送 n 个第二鉴权矢量。比如，本地配置的安全策略中该安全锚点功能实体所在的服务网络的安全策略为信任等级高，可以生成多个第一鉴权矢量，这样鉴权实体可以得到多个第二鉴权矢量后，向安全锚点功能实体发送多个第二鉴权矢量；或者，本地配置的安全策略中该安全锚点功能实体所在的服务网络的安全策略为信任等级低，可以生成一个第一鉴权矢量，这样鉴权实体可以得到一个第二鉴权矢量后，向安全锚点功能实体发送一个第二鉴权矢量。这样，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于安全锚点功能实体和鉴权实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。同时，由于统一数据管理实体是根据本地配置的安全策略，生成 n 个第一鉴权矢量，而不是像现有技术一样，在鉴权实体发送给统一数据管理实体的鉴权信息请求（authentication information request）中携带鉴权矢量的个数，因此不仅使得后续过程中鉴权实体可以向安全锚点功能实体发送 n 个第二鉴权矢量，而且可以避免现有技术中存在的鉴权实体请求的第一鉴权矢量的数量与统一数据管理实体实际生成的第一鉴权矢量的数量不一致的问题。比如，若鉴权实体请求的第一鉴权矢量的数量为多个，而统一数据管理实体选择的鉴权算法为增强的基于认证和密钥协商的可扩展认证协议（extensible authentication protocol- authentication and key agreement，EAP- AKA'）算法，则统一数据管理实体一次仅生成一个第一鉴权矢量，从而无法满足鉴权实体请求的第一鉴权矢量的数量要求。

再一种可能的实现方式中，统一数据管理实体 101，用于根据本地配置的安全策略，确定需要鉴权确认后，向鉴权实体 102 发送鉴权信息应答，该鉴权信息应答携带鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认。其中，本地配置的安全策略的描述可参考上述实施例中的相关描述，在此不再赘述。

鉴权实体 102，用于接收来自统一数据实体的鉴权信息应答，并向安全锚点功能实体发送鉴权初始应答，该鉴权初始应答携带鉴权确认标识。

鉴权实体 102，还用于接收来自安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对终端进行鉴权确认。

本申请实施例提供的鉴权系统中，统一数据管理实体可以根据本地配置的安全策略，确定需要鉴权确认后，通过鉴权实体向安全锚点功能实体发送鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认；进而，鉴权实体可以接收来自安全锚点功能实体的鉴权确认请求，并根据该鉴权确认请求对终端进行鉴权确认。这样，后续安全锚点功能实体向统一数据管理实体请求注册和获取用户签约数据的过程中，即使统一数据管理实体未获取到鉴权确认结果，由于统一数据管理实体可以获知网络的安全状况，因此统一数据管理实体可以根据网络的安全情况选择拒绝请求或者接受请求。而不像现有技术中一样，在后续安全锚点功能实体向统一数据管理实体请求注册和获取用户签约数据的过程中，在统一数据管理实体未获取到鉴权确认结果的情况下，由于不知道网络是否安全，可能直接拒绝，也可能直接接受，从而对网络安全造成的影响。比如，若统一数据管理实体直接接受，则恶意的

安全锚点功能实体就可以利用这一点，比如，即使安全锚点功能实体上对终端鉴权失败，或者安全锚点功能实体和终端之间从来没有进行过鉴权流程，安全锚点功能实体也可以随时向统一数据管理实体请求注册和获取用户签约数据，从而骗取统一数据管理实体的信任，从而将可能导致拜访网络和归属网络之间的计费纠纷。或者，若统一数据管理实体直接拒绝，那么即使终端在安全锚点功能实体所在的服务网络鉴权已经成功，则终端也可能永远无法在安全锚点功能实体所在的服务网络注册成功，从而无法访问安全锚点功能实体所在的服务网络，其效果类似于拒绝服务攻击(deny of service)。也就是说，基于该方案，可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。

可选的，图 1 所示的鉴权系统 10 可以应用于 5G 网络以及未来其它的网络，本发明实施例对此不作具体限定。

其中，若图 1 所示的鉴权系统 10 应用于 5G 网络，则如图 2 所示，则鉴权实体可以为 5G 网络中的 AUSF 实体；统一数据管理实体可以为 5G 网络中的 UDM 实体，安全锚点功能实体可以为 5G 网络中的 SEAF 实体。

此外，如图 2 所示，该 5G 网络还可以包括接入设备与接入和移动性管理(core access and mobility management function，AMF）实体等，本申请实施例对此不作具体限定。

虽然未示出，该 5G 网络还可以包括策略控制功能（policy control function，PCF）实体、用户面功能（user plane function，UPF）实体和会话管理功能（session management function，SMF）实体等，本申请实施例对此不作具体限定。

需要说明的是，本申请实施例中，SEAF 实体和 AMF 实体可能合一部署，也可能分开部署，本申请实施例对此不作具体限定。其中，本申请实施例均以 SEAF 实体和 AMF 实体分开部署为例进行说明；当然，若 SEAF 实体和 AMF 实体合一部署，则本申请实施例的 SEAF 实体需要替换为 AMF 实体，在此统一说明，以下不再赘述。

其中，如图 2 所示，终端通过下一代网络（next generation，N）接口 1（简称 N1）与 AMF 实体通信，接入设备通过 N 接口 2（简称 N2）与 AMF 实体通信，AMF 实体通过 N 接口 8（简称 N8）与 UDM 实体通信，AUSF 实体通过 N 接口 13（简称 N13）与 UDM 实体通信，SEAF 实体可以分别与 AUSF 实体和 AMF 实体通信。

需要说明的是，图 2 中的各个网元之间的接口名字只是一个示例，具体实现中接口名字可能为其他名字，本申请实施例对此不作具体限定。

需要说明的是，图 2 的接入设备、SEAF 实体、AMF 实体、AUSF 实体或 UDM 实体等仅是一个名字，名字对设备本身不构成限定。在 5G 网络以及未来其它的网络中，接入设备、SEAF 实体、AMF 实体、AUSF 实体或 UDM 实体所对应的网元或实体也可以是其他的名字，本申请实施例对此不作具体限定。例如，该 UDM 实体还有可能被替换为用户归属服务器（home subscriber server，HSS）或者用户签约数据库（user subscription database，USD）或者数据库实体或者用户数据管理实体，等等，在此进行统一说明，以下不再赘述。

可选的，本申请实施例中所涉及到的终端（terminal）可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备；还可以包括用户单元（subscriber unit）、蜂窝电话（cellular phone）、智能电话（smart phone）、

无线数据卡、个人数字助理（personal digital assistant，PDA）电脑、平板型电脑、无线调制解调器（modem）、手持设备（handheld）、膝上型电脑（laptop computer）、无绳电话（cordless phone）或者无线本地环路（wireless local loop，WLL）台、机器类型通信（machine type communication, MTC）终端、用户设备（user equipment，UE），移动台（mobile station，MS），终端设备（terminal device）等。为方便描述，本申请中，上面提到的设备统称为终端。

可选的，本申请实施例中所涉及到的接入设备指的是接入核心网的设备，例如可以是基站，宽带网络业务网关（broadband network gateway，BNG），汇聚交换机，非第三代合作伙伴计划（3rd generation partnership project，3GPP）接入设备等。基站可以包括各种形式的基站，例如：宏基站，微基站（也称为小站），中继站，接入点等。

可选的，图 1 中的统一数据管理实体 101 或鉴权实体 102 可以由一个实体设备实现，也可以由多个实体设备共同实现，还可以是一个实体设备内的一个逻辑功能模块，本申请实施例对此不作具体限定。

例如，图 1 中的统一数据管理实体 101 或鉴权实体 102 可以通过图 3 中的通信设备来实现。图 3 所示为本申请实施例提供的通信设备的硬件结构示意图。该通信设备 300 包括至少一个处理器 301，通信线路 302，存储器 303 以及至少一个通信接口 304。

处理器 301 可以是一个通用中央处理器（central processing unit，CPU），微处理器，特定应用集成电路（application-specific integrated circuit，ASIC），或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路 302 可包括一通路，在上述组件之间传送信息。

通信接口 304，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，无线接入网（radio access network，RAN），无线局域网(wireless local area networks，WLAN)等。

存储器 303 可以是只读存储器（read-only memory，ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory，EEPROM）、只读光盘（compact disc read-only memory，CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 302 与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 303 用于存储执行本申请方案的计算机执行指令，并由处理器 301 来控制执行。处理器 301 用于执行存储器 303 中存储的计算机执行指令，从而实现本申请下述实施例提供的鉴权方法。

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

在具体实现中，作为一种实施例，处理器 301 可以包括一个或多个 CPU，例如图 3 中的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，通信设备 300 可以包括多个处理器，例如图 3 中的处理器 301 和处理器 308。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

在具体实现中，作为一种实施例，通信设备 300 还可以包括输出设备 305 和输入设备 306。输出设备 305 和处理器 301 通信，可以以多种方式来显示信息。例如，输出设备 305 可以是液晶显示器（liquid crystal display，LCD），发光二级管（light emitting diode，LED)显示设备，阴极射线管（cathode ray tube，CRT) 显示设备，或投影仪（projector）等。输入设备 306 和处理器 301 通信，可以以多种方式接收用户的输入。例如，输入设备 306 可以是鼠标、键盘、触摸屏设备或传感设备等。

上述的通信设备 300 可以是一个通用设备或者是一个专用设备。在具体实现中，通信设备 300 可以是台式机、便携式电脑、网络服务器、掌上电脑（personal digital assistant，PDA）、移动手机、平板电脑、无线终端设备、嵌入式设备或有图 3 中类似结构的设备。本申请实施例不限定通信设备 300 的类型。

下面将结合图 1 至图 3，对本申请实施例提供的鉴权方法进行具体阐述。

需要说明的是，本申请下述实施例中的参数名字或者各个网元之间的消息名字只是一个示例，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。

需要说明的是，本申请下述实施例中各个网元之间交互的消息中除了携带所描述的参数外，还可能携带其他参数，本申请实施例对此不作具体限定。

以图 1 所示的鉴权系统应用于如图 2 所示的 5G 网络为例，如图 4 所示，为本申请实施例提供的一种鉴权方法，该鉴权方法包括如下步骤：

S401、终端向 SEAF 实体发送注册请求（registration request），以使得 SEAF 实体接收来自终端的注册请求。其中，该注册请求中携带用户的签约标识。

可选的，本申请实施例中，用户的签约标识例如可以是国际移动用户标识（international mobile subscriber identity，IMSI）或者其他，本申请实施例对此不作具体限定。

S402、SEAF 实体向 AUSF 实体发送鉴权初始请求（authentication initiation request），以使得 AUSF 实体接收来自 SEAF 实体的鉴权初始请求。其中，该鉴权初始请求中携带用户的签约标识以及 SEAF 实体所在的服务网络的标识。

S403、AUSF 实体向 UDM 实体发送鉴权信息请求，以使得 UDM 实体接收来自 AUSF 实体的鉴权信息请求。其中，该鉴权信息请求中携带用户的签约标识以及 SEAF 实体所在的服务网络的标识。

S404、UDM 实体生成 n 个第一鉴权矢量，n 为正整数。

可选的，本申请实施例中，UDM 实体在接收来自 AUSF 实体的鉴权信息请求之后，可以根据配置选择鉴权算法，进而可以根据鉴权算法，生成相应数量的第一鉴权矢量。比如，若 UDM 实体选择的鉴权算法为 5G-AKA 算法，则 UDM 实体可以根据本地配置的缺省鉴权矢量数目 n，生成 n 个第一鉴权矢量；或者，若 UDM 实体选择的鉴权算法为 EAP- AKA'算法，则 UDM 实体可以仅生成一个第一鉴权矢量。

其中，UDM 实体根据配置选择鉴权算法的相关实现可参考现有的方式，在此不予赘述。

需要说明的是，本申请实施例中，对应不同的鉴权算法，UDM 实体本地配置的缺省鉴权矢量数目 n 可能相同，也可能不同，本申请实施例对此不作具体限定。

本申请实施例中，由于 UDM 实体可以根据鉴权算法，生成相应数量的第一鉴权矢量，而不是像现有技术一样，在 AUSF 实体发送给 UDM 实体的鉴权信息请求中携带鉴权矢量的个数，因此可以避免现有技术中存在的 AUSF 实体请求的第一鉴权矢量的数量与 UDM 实体生成的第一鉴权矢量的数量不一致的问题。比如，若 AUSF 实体请求的第一鉴权矢量的数量为多个，而 UDM 实体选择的鉴权算法为 EAP- AKA'算法，则 UDM 实体一次仅生成一个第一鉴权矢量，从而无法满足鉴权实体请求的第一鉴权矢量的数量要求。

S405、UDM 实体向 AUSF 实体发送鉴权信息应答（authentication information answer），以使得 AUSF 实体接收来自 UDM 实体的鉴权信息应答。其中，该鉴权信息应答中携带 n 个第一鉴权矢量。

可选的，本申请实施例中，UDM 实体可以根据本地配置的安全策略确定需要鉴权确认。比如，UDM 实体可以根据步骤 S403 中携带的 SEAF 实体所在的服务网络的标识，以及本地配置的安全策略中该 SEAF 实体所在的服务网络的安全策略，确定是否需要鉴权确认。若确定需要鉴权确认，可以在鉴权信息应答中携带鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认，这样后续 SEAF 实体对终端鉴权成功后，可以根据该鉴权确认标识向 AUSF 实体发送鉴权确认请求，由 AUSF 实体进一步对终端进行鉴权确认。若确认不需要鉴权确认，由于 UDM 实体可以获知网络的安全情况，即使获取不到鉴权确认结果，也可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。

示例性的，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为服务网络的信任等级低，则 UDM 实体可以确定需要进行鉴权确认，进而在鉴权信息应答中携带鉴权确认标识；或者，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为服务网络的信任等级高，则 UDM 实体可以确定需要不进行鉴权确认，进而不需要在鉴权信息应答中携带鉴权确认标识。

S406、AUSF 实体根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量。

其中，步骤 S406 的具体实现可参考现有的实现方式，在此不予赘述。

S407、AUSF 实体向 SEAF 实体发送鉴权初始应答(authentication initiation answer)，以使得 SEAF 实体接收来自 AUSF 实体的鉴权初始应答。其中，该鉴权初始应答中携带 n 个第二鉴权矢量中的其中一个第二鉴权矢量。

可选的，本申请实施例中，若步骤 S405 中的鉴权信息应答中携带鉴权确认标识，则步骤 S407 中的鉴权初始应答中还携带该鉴权确认标识，这样后续 SEAF 实体对终端鉴权成功后，可以根据该鉴权确认标识向 AUSF 实体发送鉴权确认请求，由 AUSF 实体进一步对终端进行鉴权确认。

可选的，本申请实施例中，若步骤 S405 中的鉴权信息应答中未携带鉴权确认标识，则 AUSF 实体接收来自 UDM 实体的鉴权信息应答之后，可以根据本地配置的安全策略，确定是否需要鉴权确认。比如，AUSF 实体可以根据步骤 S402 中携带的 SEAF 实体所在的服务网络的标识，以及本地配置的安全策略中该 SEAF 实体所在的服务网络的安全策略，确定是否需要鉴权确认。若确定需要鉴权确认，可以在步骤 S407 中的鉴权初始应答中还携带该鉴权确认标识，这样后续 SEAF 实体对终端鉴权成功后，可以根据该鉴权确认标识向 AUSF 实体发送鉴权确认请求，由 AUSF 实体进一步对终端进行鉴权确认。

示例性的，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为服务网络的信任等级低，则 AUSF 实体可以确定需要进行鉴权确认，进而在鉴权初始应答中携带鉴权确认标识；或者，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为服务网络的信任等级高，则 UDM 实体可以确定需要不进行鉴权确认，进而不需要在鉴权初始应答中携带鉴权确认标识。

可选的，本申请实施例中，若 SEAF 实体根据本地配置的安全策略确定不需要进行鉴权确认，则可能说明服务网络的信任等级高，进而 AUSF 实体可以向 SEAF 实体发送鉴权初始应答，该鉴权初始应答中携带 n 个第二鉴权矢量，本申请实施例对此不作具体限定。这样不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于 SEAF 实体和 AUSF 实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。

可选的，本申请实施例中，假设鉴权初始应答中携带的第二鉴权矢量为（RAND1、AUTN1、HXRES1*和 Kasme1*），对应的第一鉴权矢量为（RAND1、AUTN1、XRES1*和 Kasme1*），则 AUSF 实体还可能保存 RAND1 和 XRES1*的对应关系，以便后续步骤 S414 中使用，本申请实施例对此不作具体限定。

S408、SEAF 实体向终端发送鉴权请求（ authentication request)，以使得终端接收来自 SEAF 实体的鉴权请求。其中，该鉴权请求中携带 RAND1 和 AUTN1。

S409、SEAF 实体存储鉴权初始应答中携带的第二鉴权矢量中的 HXRES1*，以便后续步骤 S412 中使用，在此不再赘述。

需要说明的是，本申请实施例中，步骤 S408 和步骤 S409 之间没有必然的先后顺序，可以是先执行步骤 S408，再执行步骤 S409；或者，可以先执行步骤 S409，再执行步骤 S408；或者，可以同时执行步骤 S408 和步骤 S409，本申请实施例对此不作具体限定。

S410、终端根据 AUTN1 对 SEAF 实体所在的服务网络进行鉴权，并根据 RAND1 计算 RES*。

其中，步骤 S410 的具体实现可参考现有的实现方式，在此不予赘述。

S411、终端向 SEAF 实体发送鉴权响应（authentication response），以使得 SEAF 实体接收来自终端的鉴权响应，其中，该鉴权响应中携带 RES*。

可选的，该鉴权响应中还可以携带鉴权初始应答中携带的第二鉴权矢量中的 RAND1，以便后续步骤 S414 中使用，在此不再赘述。

S412、SEAF 实体对终端进行鉴权。

可选的，本申请实施例中，SEAF 实体可以根据 RES*以及 3GPP 33.501 规范中定义的算法，计算出 HRES*，通过比较 HRES*和步骤 S409 中存储的 HXRES1*，完成对终端的鉴权。比如，若 HRES*和步骤 S409 中存储的 HXRES1*相等，则可以确定对终端鉴权成功；或者，若 HRES*和步骤 S409 中存储的 HXRES1*不相等，则可以确定对终端鉴权失败。

在对终端鉴权成功之后，SEAF 实体可以根据步骤 S407 中的鉴权初始应答中携带的鉴权确认标识，执行下述步骤 S413；或者，在对终端鉴权成功之后，SEAF 实体可以直接执行下述步骤 S413，本申请实施例对此不作具体限定。

当然，若对终端鉴权失败，SEAF 实体可以向终端发送注册拒绝消息，本申请实施例对此不作具体限定。

S413、SEAF 实体向 AUSF 实体发送鉴权确认请求（authentication confirmation request），以使得 AUSF 实体接收来自 SEAF 实体的鉴权确认请求。其中，该鉴权确认请求中携带 RES*。

可选的，若步骤 S411 中的鉴权响应中还携带 RAND1，则步骤 S413 中的鉴权确认请求中还携带 RAND1；或者，若步骤 S411 中的鉴权响应中未携带 RAND1，则步骤 S413 中的鉴权确认请求中还可以携带步骤 S407 中的 RAND1，本申请实施例对此不作具体限定。

S414、AUSF 实体对终端进行鉴权确认。

可选的，本申请实施例中，若步骤 S413 中的鉴权确认请求中还携带 RAND1，则 AUSF 实体可以根据该 RAND1，以及预先存储的 RAND1 和 XRES1*的对应关系，查找到该 XRES1*，进而通过比较 XRES1*和 RES*，完成对终端的鉴权确认。比如，若 XRES1*和 RES*相等，则可以确定对终端鉴权确认成功；或者，若 XRES1*和 RES*不相等，

则可以确定对终端鉴权确认失败。通过该方式，在 AUSF 实体接收来自 SEAF 实体的鉴权确认请求之后，由于可以快速查找到与 RES*对应的 XRES1*，因此可以解决现有技术中在进行鉴权确认时，在 AUSF 实体之前从 UDM 实体中接收多个第一鉴权矢量的情况下，AUSF 实体不知道使用哪个鉴权矢量中的 XRES*和接收到的 RES*进行比较，从而影响 AUSF 实体的处理性能的问题，可以实现对终端的快速鉴权确认。

S415、AUSF 实体向 SEAF 实体发送鉴权确认应答（authentication confirmation answer），以使得 SEAF 实体接收来自 AUSF 实体的鉴权确认应答。

其中，在鉴权确认成功的情况下，该鉴权确认应答中携带 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。可选的，该鉴权确认应答中还可以携带上述的鉴权确认标识。这样，后续若 SEAF 实体需要重新对终端鉴权时，可以直接使用 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。比如，在 SEAF 实体接收来自终端的周期性注册请求或者跟踪区域更新请求之后，可以直接使用 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量，采用上述步骤 S408-S412 的方式对终端鉴权；或者采用上述步骤 S408-S415 的方式对终端鉴权后再对终端进行鉴权确认，本申请实施例在此不再赘述。

可选的，本申请实施例中，在鉴权确认成功的情况下，该鉴权确认应答中还可以携带 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量中的部分第二鉴权矢量。这样，后续若 SEAF 实体需要重新对终端鉴权时，可以直接按照上述方式使用鉴权确认应答中携带的部分第二鉴权矢量，本申请实施例对此不作具体限定。

可选的，在鉴权确认成功的情况下，该鉴权确认应答中可以携带鉴权确认成功指示，该鉴权确认成功指示用于指示鉴权确认成功，以便 SEAF 实体可以及时获知鉴权确认的结果。其中，该鉴权确认成功指示例如可以是鉴权确认响应中的一个成功码，本申请实施例对此不作具体限定。

其中，在鉴权确认失败的情况下，该鉴权确认应答中可以携带鉴权确认失败指示，该鉴权确认失败指示用于指示鉴权确认失败，以便 SEAF 实体可以及时获知鉴权确认的结果。其中，该鉴权确认失败指示例如可以是鉴权确认响应中的一个失败码，本申请实施例对此不作具体限定。

可选的，在鉴权确认失败的情况下，还可以不通过鉴权确认应答携带鉴权确认失败指示，而是通过一个专用的消息携带该鉴权确认失败指示，本申请实施例对此不作具体限定。

基于该方案，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于 SEAF 实体和 AUSF 实体之间因为链路不通而导致的对终端鉴权失败的问题，从而提高了鉴权结果的可靠性。

其中，上述步骤 S401 至 S415 中 AUSF 实体和 UDM 实体的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码来执行，本申请实施例对此不作任何限制。

可选的，以图 1 所示的鉴权系统应用于如图 2 所示的 5G 网络为例，如图 5 所示，为本申请实施例提供的另一种鉴权方法，该鉴权方法包括如下步骤：

S501-S503、同步骤 S401-S403，具体可参考图 4 所示的实施例，在此不再赘述。

S504、UDM 实体根据本地配置的安全策略，生成 n 个第一鉴权矢量，n 为正整数。

可选的，本申请实施例中，UDM 实体可以根据步骤 S403 中携带的 SEAF 实体所在的服务网络的标识，以及本地配置的安全策略中该 SEAF 实体所在的服务网络的安全策略，生成 n 个第一鉴权矢量。

示例性的，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为信任等级高，则 UDM 实体可以根据本地配置的缺省鉴权矢量数目 n，生成 n 个第一鉴权矢量；或者，若本地配置的安全策略中 SEAF 实体所在的服务网络的安全策略为信任等级低，则 UDM 实体可以生成一个第一鉴权矢量。

可选的，本申请实施例中，UDM 实体在确定待生成的第一鉴权矢量的数量时，也可以结合选择的鉴权算法。比如，若选择的鉴权算法为 5G-AKA 算法，则 UDM 实体再根据步骤 S503 中携带的 SEAF 实体所在的服务网络的标识，以及本地配置的安全策略，生成 n 个第一鉴权矢量，n 为正整数；若选择的鉴权算法为 EAP- AKA'算法，则 UDM 实体可以仅生成一个第一鉴权矢量，本申请实施例对此不作具体限定。

S505-S506、同步骤 S405-S406，具体可参考图 4 所示的实施例，在此不再赘述。

S507、与步骤 S407 类似，区别仅在于，图 4 所示的实施例中，鉴权初始应答中携带 n 个第二鉴权矢量中的其中一个第二鉴权矢量；而本申请实施例中，由于 n 个第一鉴权矢量是 UDM 实体根据本地配置的安全策略生成的，因此鉴权初始应答中可以携带 n 个第二鉴权矢量，相关描述可参考图 4 所示的实施例，在此不再赘述。

假设后续使用的第二鉴权矢量为（RAND1、AUTN1、HXRES1*和 Kasme1*），则本申请实施例提供的鉴权方法还包括如下步骤：

S508-S512、同步骤 S408-S412，具体可参考图 4 所示的实施例，在此不再赘述。

可选的，本申请实施例还可以包括如下步骤：

S513-S514、同步骤 S413-S414，具体可参考图 4 所示的实施例，在此不再赘述。

S515、与步骤 S415 类似，区别仅在于，图 4 所示的实施例中，在鉴权确认成功的情况下，该鉴权确认应答中携带 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量；而本申请实施例中，由于步骤 S407 中已经将 n 个第二鉴权矢量发送给 SEAF 实体，因此不需要再鉴权确认应答中携带 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量，相关描述可参考图 4 所示的实施例，在此不再赘述。

基于本申请实施例提供的鉴权方法，不仅可以解决现有技术中存在的如何处理剩下未使用的 n-1 个第一鉴权矢量而可能产生的性能和内存资源浪费的问题，从而提高了第一鉴权矢量的使用效率；而且可以减少由于 SEAF 实体和 AUSF 实体之间因为链路不通而导致的对

终端鉴权失败的问题，从而提高了鉴权结果的可靠性；同时，还可以避免现有技术中存在的AUSF请求的第一鉴权矢量的数量与UDM实体生成的第一鉴权矢量的数量不一致的问题。

其中，上述步骤S501至S515中AUSF实体和UDM实体的动作可以由图3所示的通信设备300中的处理器301调用存储器303中存储的应用程序代码来执行，本申请实施例对此不作任何限制。

可选的，以图1所示的鉴权系统应用于如图2所示的5G网络为例，本申请实施例还提供的一种鉴权方法，该鉴权方法中，UDM实体接收来自AUSF实体的鉴权信息后，根据本地配置的安全策略，确定需要鉴权确认，进而向AUSF实体发送鉴权信息应答，该鉴权信息应答携带鉴权确认标识，该鉴权确认标识用于指示需要鉴权确认。AUSF实体接收来自UDM实体的鉴权信息应答后，向SEAF实体发送鉴权初始应答，该鉴权初始应答携带鉴权确认标识。这样，后续SEAF实体对终端鉴权成功后，可以向AUSF实体发送鉴权确认请求，以使得AUSF实体接收来自SEAF实体的鉴权确认请求后，根据该鉴权确认请求对终端进行鉴权确认。在该鉴权方法中，可以采用图4所示的实施例的方式生成n个第一鉴权矢量，以及发送n个第二鉴权矢量；也可以采用图5所示的实施例的方式生成n个第一鉴权矢量，以及发送n个第二鉴权矢量，本申请实施例对此不作具体限定。相关描述可参考图4或图5所示的实施例，在此不再赘述。

基于本申请实施例提供的鉴权方法，可以避免现有技术中可能存在的拜访网络和归属网络之间的计费纠纷或者拒绝服务攻击，提升网络的安全性。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是，上述鉴权实体为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，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，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

本申请实施例可以根据上述方法示例对鉴权实体进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块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。需要说明的是，本申请实施例中对模块的划分是示意性的，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。

比如，以采用集成的方式划分各个功能模块的情况下，图6示出了一种鉴权实体60的结构示意图。该鉴权实体60包括：收发模块601和处理模块602。收发模块601，用于接收来自统一数据管理实体的n个第一鉴权矢量，n为正整数。处理模块602，用于根据n个第一鉴权矢量，生成n个第二鉴权矢量。收发模块601，还用于向安全锚点功能实体发送n个第二鉴权矢量中的其中一个第二鉴权矢量。收发模块601，还用于接收来自安全锚点功能实体的鉴权确认请求，并根据鉴权确认请求对终端进行鉴权确认；收发模块601，还用于在鉴权确认成功的情况下，向安全锚点功能实体发送n个第二鉴矢量中其他未使用的n-1个第

二鉴权矢量。

可选的，收发模块601，还用于向安全锚点功能实体发送鉴权确认标识，其中，该鉴权确认标识用于指示需要鉴权确认。

可选的，处理模块602，还用于确定需要鉴权确认。

在一种可能的实现方式中，处理模块 602 用于确定需要鉴权确认，包括：用于接收来自统一数据管理实体的鉴权确认标识，其中，鉴权确认标识用于指示需要鉴权确认。

在一种可能的实现方式中，处理模块 602 用于确定需要鉴权确认，包括：用于根据本地配置的安全策略，确定需要鉴权确认。

可选的，鉴权确认请求携带 RES*和对应的 RAND；处理模块 602 用于根据鉴权确认请求对终端进行鉴权确认，包括：用于根据 RAND 查找对应的 XRES*，并通过比较 RES*和 XRES*对终端进行鉴权确认。

可选的，收发模块601，还用于在鉴权确认失败的情况下，向安全锚点功能实体发送鉴权确认失败指示，鉴权确认失败指示用于指示鉴权确认失败。

可选的，收发模块601，还用于在鉴权确认成功的情况下，向安全锚点功能实体发送鉴权确认成功指示，鉴权确认成功指示用于指示鉴权确认成功。

可选的，收发模块601，还用于在鉴权确认成功的情况下，向安全锚点功能实体发送鉴权确认标识，其中，鉴权确认标识用于指示需要鉴权确认。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。

在本实施例中，该鉴权实体 60 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”可以指特定应用集成电路（application-specific integrated circuit，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/或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鉴权实体 60 可以采用图 3 所示的形式。

比如，图 3 中的处理器 301 可以通过调用存储器 303 中存储的计算机执行指令，使得鉴权实体 60 执行上述方法实施例中的鉴权方法。

具体的，图 6 中的收发模块 601 和处理模块 602 的功能/实现过程可以通过图 3 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现。或者，图 6 中的处理模块 602 的功能/实现过程可以通过图 3 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现，图 6 中的收发模块 601 的功能/实现过程可以通过图 3 中的通信接口 304 来实现。

由于本申请实施例提供的鉴权实体可用于执行上述鉴权方法，因此其所能获得的技术效果可参考上述方法实施例，在此不再赘述。

上述实施例中，鉴权实体 60 以采用集成的方式划分各个功能模块的形式来呈现。当然，本申请实施例也可以对应各个功能划分鉴权实体的各个功能模块，本申请实施例对此不作具体限定。

可选的，本申请实施例提供了一种芯片系统，该芯片系统包括处理器，用于支持鉴权实体实现上述的鉴权方法，例如根据 n 个第一鉴权矢量，生成 n 个第二鉴权矢量。在一种可能的设计中，该芯片系统还包括存储器。该存储器，用于保存鉴权实体必要的程序指

令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件，本申请实施例对此不作具体限定。

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。当使用软件程序实现时，可以全部或部分地以计算机程序产品的形式来实现。该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计算机程序指令时，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、服务器或者数据中心通过有线（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以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，DVD）、或者半导体介质（例如固态硬盘（solid state disk，SSD））等。

尽管在此结合各实施例对本申请进行了描述，然而，在实施所要求保护的本申请过程中，本领域技术人员通过查看所述附图、公开内容、以及所附权利要求书，可理解并实现所述公开实施例的其他变化。在权利要求中，“包括”（comprising）一词不排除其他组成部分或步骤，“一”或“一个”不排除多个的情况。单个处理器或其他单元可以实现权利要求中列举的若干项功能。相互不同的从属权利要求中记载了某些措施，但这并不表示这些措施不能组合起来产生良好的效果。

尽管结合具体特征及其实施例对本申请进行了描述，显而易见的，在不脱离本申请的精神和范围的情况下，可对其进行各种修改和组合。相应地，本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明，且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。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、一种鉴权方法，其特征在于，所述方法包括:

鉴权实体接收来自统一数据管理实体的第一鉴权矢量;

所述鉴权实体根据所述第一鉴权矢量，生成第二鉴权矢量;

所述鉴权实体向安全锚点功能实体发送所述第二鉴权矢量;

所述鉴权实体接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请求对终端进行鉴权确认;

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认成功指示，所述鉴权确认成功指示用于指示鉴权确认成功；或，在鉴权确认失败的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认失败指示，所述鉴权确认失败指示用于指示鉴权确认失败。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

所述鉴权实体向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

3、根据权利要求 1 或 2 所述方法，其特征在于，所述方法还包括:

所述鉴权实体确定需要鉴权确认。

4、根据权利要求 3 所述的方法，其特征在于，所述鉴权实体确定需要鉴权确认，包括:

所述鉴权实体接收来自所述统一数据管理实体的鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

5、根据权利要求 3 所述的方法，其特征在于，所述鉴权实体确定需要鉴权确认，包括:

所述鉴权实体根据本地配置的安全策略，确定需要鉴权确认。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述第一鉴权矢量是用增强的基于认证和密钥协商的可扩展认证协议生成的。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述鉴权确认请求携带响应值 RES* 和对应的随机数 RAND;

所述鉴权实体根据所述鉴权确认请求对所述终端进行鉴权确认，包括:

所述鉴权实体根据所述 RAND 查找对应的 XRES*，并通过比较所述 RES*和所述 XRES* 对所述终端进行鉴权确认。

8、根据权利要求 1-7 任一项所述的方法，其特征在于，在所述鉴权实体根据所述鉴权确认请求对所述终端进行鉴权确认之后，还包括:

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

9、一种鉴权方法，该鉴权方法包括:

统一数据管理实体生成第一鉴权矢量;

所述统一数据管理实体向鉴权实体发送所述第一鉴权矢量;

所述鉴权实体接收来自所述统一数据管理实体的所述第一鉴权矢量，并根据所述第一鉴权矢量，生成第二鉴权矢量;

所述鉴权实体向安全锚点功能实体发送所述第二鉴权矢量;

所述鉴权实体接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请

求对终端进行鉴权确认;

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认成功指示，所述鉴权确认成功指示用于指示鉴权确认成功；或，在鉴权确认失败的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认失败指示，所述鉴权确认失败指示用于指示鉴权确认失败。

10、根据权利要求 9 所述的方法，其特征在于，所述统一数据管理实体生成第一鉴权矢量具体包括：所述统一数据管理实体根据本地配置的安全策略生成第一鉴权矢量。

11、根据权利要求 10 所述的方法，其特征在于，所述统一数据管理实体根据本地配置的安全策略，生成第一鉴权矢量，包括：所述统一数据管理实体根据所述安全锚点功能实体所在的服务网络的标识，以及所述本地配置的安全策略中所述服务网络的安全策略，生成所述第一鉴权矢量。

12、根据权利要求 9-11 任一所述的方法，所述统一数据管理实体采用增强的基于认证和密钥协商的可扩展认证协议生成所述第一鉴权矢量。

13、一种鉴权实体，其特征在于，所述鉴权实体包括：收发模块和处理模块;

所述收发模块，用于接收来自统一数据管理实体的第一鉴权矢量;

所述处理模块，用于根据所述第一鉴权矢量，生成第二鉴权矢量;

所述收发模块，还用于向安全锚点功能实体发送所述第二鉴权矢量;

所述收发模块，还用于接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请求对所述终端进行鉴权确认;

所述收发模块，还用于在鉴权确认成功的情况下，向所述安全锚点功能实体发送鉴权确认成功指示，所述鉴权确认成功指示用于指示鉴权确认成功；或，在鉴权确认失败的情况下，向所述安全锚点功能实体发送鉴权确认失败指示，所述鉴权确认失败指示用于指示鉴权确认失败。

14、根据权利要求 13 所述的鉴权实体，其特征在于，所述收发模块，还用于向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

15、根据权利要求 13 或 14 所述的鉴权实体，其特征在于，所述鉴权实体处理模块，还用于确定需要鉴权确认。

16、根据权利要求 15 所述的鉴权实体，其特征在于，所述处理模块用于确定需要鉴权确认，包括:

用于接收来自所述统一数据管理实体的鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

17、根据权利要求 15 所述的鉴权实体，其特征在于，所述处理模块用于确定需要鉴权确认，包括:

用于根据本地配置的安全策略，确定需要鉴权确认。

18、根据权利要求 13-17 任一项所述的鉴权实体，其特征在于，所述鉴权确认请求携带响应值 RES*和对应的随机数 RAND;

所述处理模块用于根据所述鉴权确认请求对所述终端进行鉴权确认，包括:

用于根据所述 RAND 查找对应的 XRES*，并通过比较所述 RES*和所述 XRES*对所述终端进行鉴权确认。

19、根据权利要求 13-18 任一项所述的鉴权实体，其特征在于，所述收发模块，还用于在

鉴权确认成功的情况下，向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

20、一种鉴权系统，其特征在于，所述鉴权系统包括：统一数据管理实体和鉴权实体；

所述统一数据管理实体，用于生成第一鉴权矢量；

所述统一数据管理实体，还用于向鉴权实体发送所述第一鉴权矢量；

所述鉴权实体，用于接收来自所述统一数据管理实体的所述第一鉴权矢量，并根据所述第一鉴权矢量，生成第二鉴权矢量；

所述鉴权实体，还用于向安全锚点功能实体发送所述第二鉴权矢量；

所述鉴权实体，还用于接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请求对所述终端进行鉴权确认；

所述鉴权实体，还用于在鉴权确认成功的情况下，向所述安全锚点功能实体发送鉴权确认成功指示，所述鉴权确认成功指示用于指示鉴权确认成功；或，在鉴权确认失败的情况下，向所述安全锚点功能实体发送鉴权确认失败指示，所述鉴权确认失败指示用于指示鉴权确认失败。

21、根据权利要求 20 所述的鉴权系统，其特征在于，所述统一数据管理实体用于生成第一鉴权矢量，具体包括：所述统一数据管理实体根据本地配置的安全策略生成第一鉴权矢量。

22、根据权利要求 21 所述的鉴权系统，其特征在于，所述统一数据管理实体用于根据本地配置的安全策略，确定需要鉴权确认，包括：

所述统一数据管理实体根据所述安全锚点功能实体所在的服务网络的标识，以及所述本地配置的安全策略中所述服务网络的安全策略，生成所述第一鉴权矢量。

23、一种鉴权方法，其特征在于，所述方法包括：

鉴权实体接收来自统一数据管理实体的 n 个第一鉴权矢量，n 为正整数；

所述鉴权实体根据所述 n 个第一鉴权矢量，生成 n 个第二鉴权矢量；

所述鉴权实体向安全锚点功能实体发送所述 n 个第二鉴权矢量中的其中一个第二鉴权矢量；

所述鉴权实体接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请求对所述终端进行鉴权确认；

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送所述 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。

24、根据权利要求 23 所述的方法，其特征在于，所述方法还包括：

所述鉴权实体向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

25、根据权利要求 23 或 24 所述方法，其特征在于，所述方法还包括：

所述鉴权实体确定需要鉴权确认。

26、根据权利要求 25 所述的方法，其特征在于，所述鉴权实体确定需要鉴权确认，包括：

所述鉴权实体接收来自所述统一数据管理实体的鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

27、根据权利要求 25 所述的方法，其特征在于，所述鉴权实体确定需要鉴权确认，包括：

所述鉴权实体根据本地配置的安全策略，确定需要鉴权确认。

28、根据权利要求 23-27 任一项所述的方法，其特征在于，所述鉴权确认请求携带响应

值 RES*和对应的随机数 RAND;

所述鉴权实体根据所述鉴权确认请求对所述终端进行鉴权确认，包括:

所述鉴权实体根据所述 RAND 查找对应的 XRES*，并通过比较所述 RES*和所述 XRES*对所述终端进行鉴权确认。

29、根据权利要求 23-28 任一项所述的方法，其特征在于，在所述鉴权实体根据所述鉴权确认请求对所述终端进行鉴权确认之后，还包括:

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认成功指示，所述鉴权确认成功指示用于指示鉴权确认成功。

30、根据权利要求 23-29 任一项所述的方法，其特征在于，在所述鉴权实体根据所述鉴权确认请求对所述终端进行鉴权确认之后，还包括:

在鉴权确认成功的情况下，所述鉴权实体向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

31、一种鉴权实体，其特征在于，所述鉴权实体包括: 收发模块和处理模块;

所述收发模块，用于接收来自统一数据管理实体的 n 个第一鉴权矢量，n 为正整数;

所述处理模块，用于根据所述 n 个第一鉴权矢量，生成 n 个第二鉴权矢量;

所述收发模块，还用于向安全锚点功能实体发送所述 n 个第二鉴权矢量中的其中一个第二鉴权矢量;

所述收发模块，还用于接收来自所述安全锚点功能实体的鉴权确认请求，并根据所述鉴权确认请求对所述终端进行鉴权确认;

所述收发模块，还用于在鉴权确认成功的情况下，向所述安全锚点功能实体发送所述 n 个第二鉴矢量中其他未使用的 n-1 个第二鉴权矢量。

32、根据权利要求 31 所述的鉴权实体，其特征在于，所述收发模块，还用于向所述安全锚点功能实体发送鉴权确认标识，其中，所述鉴权确认标识用于指示需要鉴权确认。

33、一种鉴权实体，其特征在于，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，当所述会话管理功能实体运行时，所述处理器执行所述存储器存储的该计算机执行指令，以使所述鉴权实体执行如权利要求 1-8 任一项所述的鉴权方法。

34、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，使得计算机可以执行如权利要求 1-8 任一项所述的鉴权方法。

35、一种计算机程序产品，其特征在于，所述计算机程序产品中存储有指令，当其在计算机上运行时，使得计算机可以执行如权利要求 1-8 任一项所述的鉴权方法。

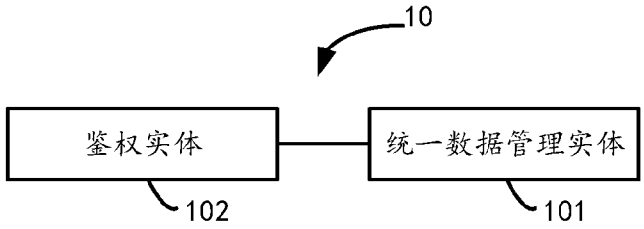

10
鉴权实体
统一数据管理实体
102
101

图 1

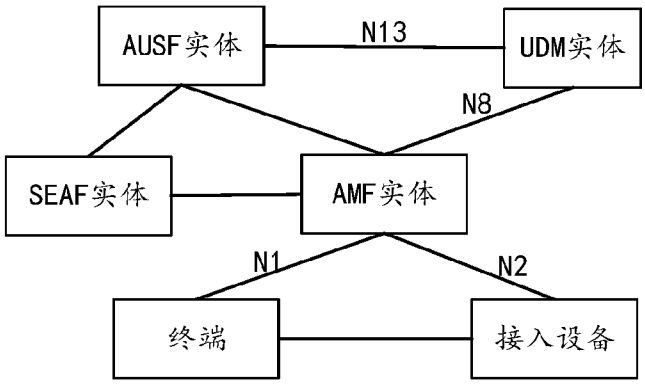

AUSF实体
N13
UDM实体
N8
SEAF实体
AMF实体
N1
N2
终端
接入设备

图 2

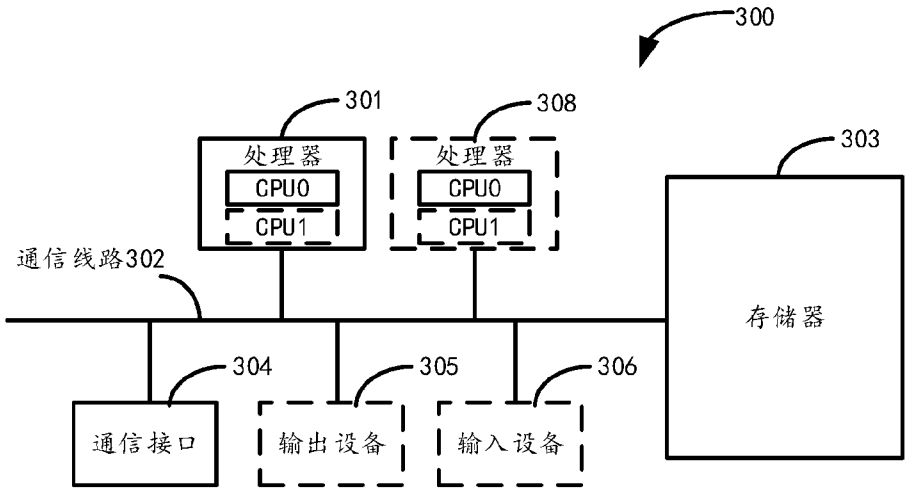

300
301
处理器
CPU0
CPU1
308
处理器
CPU0
CPU1
303
通信线路302
存储器
304
305
306
通信接口
输出设备
输入设备

图 3

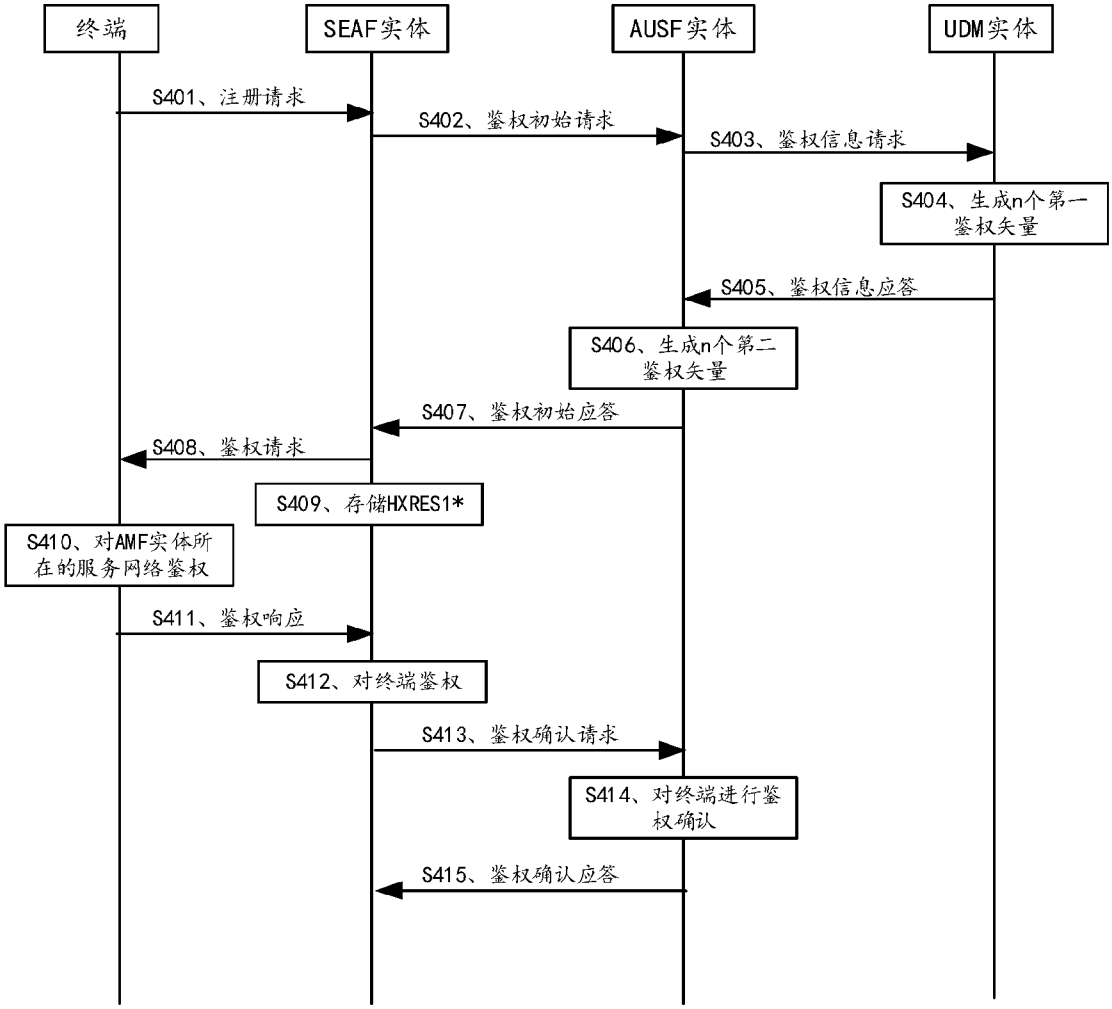

终端
SEAF实体
AUSF实体
UDM实体
S401、注册请求
S402、鉴权初始请求
S403、鉴权信息请求
S404、生成n个第一鉴权矢量
S405、鉴权信息应答
S406、生成n个第二鉴权矢量
S407、鉴权初始应答
S408、鉴权请求
S409、存储HXRES1*
S410、对AMF实体所在的服务网络鉴权
S411、鉴权响应
S412、对终端鉴权
S413、鉴权确认请求
S414、对终端进行鉴权确认
S415、鉴权确认应答

图 4

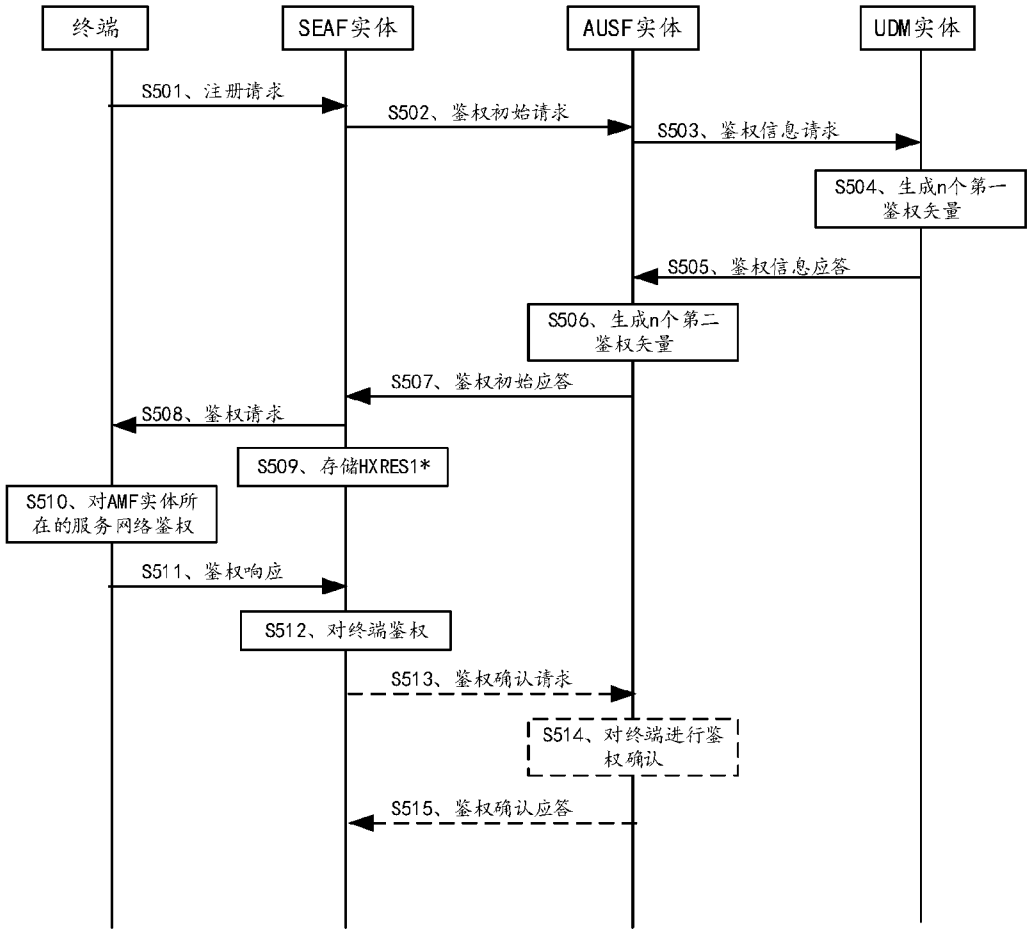

终端
SEAF实体
AUSF实体
UDM实体
S501、注册请求
S502、鉴权初始请求
S503、鉴权信息请求
S504、生成n个第一鉴权矢量
S505、鉴权信息应答
S506、生成n个第二鉴权矢量
S507、鉴权初始应答
S508、鉴权请求
S509、存储HXRES1*
S510、对AMF实体所在的服务网络鉴权
S511、鉴权响应
S512、对终端鉴权
S513、鉴权确认请求
S514、对终端进行鉴权确认
S515、鉴权确认应答

图 5

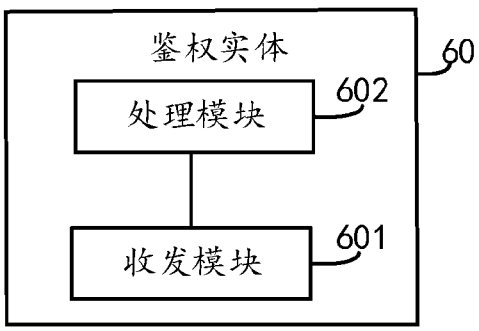

鉴权实体
60
处理模块
602
收发模块
601

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/114461

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)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 数目, 个数, 数量, number, 未使用, unused, 鉴权, authentication, 矢量, vector, 确认, confirmation, AUSF, UDM, SEAF

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KPN. "Rewriting Clause 6.1.2 and 6.1.3 in Normative Language and Adding Annex A" *3GPP TSG SA WG3 (Security) Meeting #88Bis Adhoc S3-172569,* 13 October 2017 (2017-10-13), section 6.1.3	1-22, 33-35
X	KPN. "Rewriting Clause 6.1.2 and 6.1.3 in Normative Language and Adding Annex A" *3GPP TSG SA WG3 (Security) Meeting #88Bis Adhoc S3-172224,* 13 October 2017 (2017-10-13), section 6.1.3	1-22, 33-35
A	CN 1815954 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 August 2006 (2006-08-09) entire document	1-35
A	CN 101772020 A (HUAWEI TECHNOLOGIES CO., LTD.) 07 July 2010 (2010-07-07) entire document	1-35
A	EP 1169880 A1 (NOKIA CORP.) 09 January 2002 (2002-01-09) entire document	1-35

☐ 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 January 2019	**30 January 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/114461

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	1815954	A	09 August 2006	WO	2006081742	A1	10 August 2006
CN	101772020	A	07 July 2010	WO	2010075745	A1	08 July 2010
				US	2011265146	A1	27 October 2011
EP	1169880	A1	09 January 2002	AT	306798	T	15 October 2005
				CN	1156196	C	30 June 2004
				CA	2368530	A1	30 August 2001
				AT	472909	T	15 July 2010
				DK	1432271	T3	18 October 2010
				JP	2003524353	A	12 August 2003
				IL	145606	A	01 August 2006
				ES	2249455	T3	01 April 2006
				ES	2346435	T3	15 October 2010
				DE	60142494	D1	12 August 2010
				US	2002044552	A1	18 April 2002
				GB	0004178	D0	12 April 2000
				CN	1363195	A	07 August 2002
				US	2012051225	A1	01 March 2012
				US	2006159031	A1	20 July 2006
				CY	1111052	T1	11 June 2015
				EP	1432271	A2	23 June 2004
				US	2014323091	A1	30 October 2014
				AU	2848501	A	03 September 2001
				PT	1432271	E	24 August 2010
				WO	0163954	A1	30 August 2001
				DE	60113925	D1	23 February 2006
				IL	175752	A	30 June 2011

国际检索报告

国际申请号
PCT/CN2018/114461

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）)

CNPAT,CNKI,WPI,EPODOC,3GPP:数目，个数，数量，number,未使用，unused, 鉴权, authentication, 矢量, vector, 确认，confirmation, AUSF，UDM，SEAF

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	KPN. "Rewriting Clause 6.1.2 and 6.1.3 in normative language and adding Annex A" 3GPP TSG SA WG3 (Security) Meeting #88Bis Adhoc S3-172569, 2017年 10月 13日 (2017-10-13), 第6.1.3节	1-22，33-35
X	KPN. "Rewriting Clause 6.1.2 and 6.1.3 in normative language and adding Annex A" 3GPP TSG SA WG3 (Security) Meeting #88Bis Adhoc S3-172224, 2017年 10月 13日 (2017-10-13), 第6.1.3节	1-22，33-35
A	CN 1815954 A (华为技术有限公司) 2006年 8月 9日 (2006-08-09) 全文	1-35
A	CN 101772020 A (华为技术有限公司) 2010年 7月 7日 (2010-07-07) 全文	1-35
A	EP 1169880 A1 (NOKIA CORP.) 2002年 1月 9日 (2002-01-09) 全文	1-35

☐ 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
2019年 1月 14日	2019年 1月 30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 雷永俊 电话号码 86-(10)-53961669

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/114461

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	1815954	A	2006年 8月 9日	WO	2006081742	A1	2006年 8月 10日
CN	101772020	A	2010年 7月 7日	WO	2010075745	A1	2010年 7月 8日
				US	2011265146	A1	2011年 10月 27日
EP	1169880	A1	2002年 1月 9日	AT	306798	T	2005年 10月 15日
				CN	1156196	C	2004年 6月 30日
				CA	2368530	A1	2001年 8月 30日
				AT	472909	T	2010年 7月 15日
				DK	1432271	T3	2010年 10月 18日
				JP	2003524353	A	2003年 8月 12日
				IL	145606	A	2006年 8月 1日
				ES	2249455	T3	2006年 4月 1日
				ES	2346435	T3	2010年 10月 15日
				DE	60142494	D1	2010年 8月 12日
				US	2002044552	A1	2002年 4月 18日
				GB	0004178	D0	2000年 4月 12日
				CN	1363195	A	2002年 8月 7日
				US	2012051225	A1	2012年 3月 1日
				US	2006159031	A1	2006年 7月 20日
				CY	1111052	T1	2015年 6月 11日
				EP	1432271	A2	2004年 6月 23日
				US	2014323091	A1	2014年 10月 30日
				AU	2848501	A	2001年 9月 3日
				PT	1432271	E	2010年 8月 24日
				WO	0163954	A1	2001年 8月 30日
				DE	60113925	D1	2006年 2月 23日
				IL	175752	A	2011年 6月 30日