(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
2024 年 11 月 14 日 (14.11.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/229634 A1

(51) 国际专利分类号:
H04W 12/06 (2021.01) *H04L 9/14* (2006.01)

(21) 国际申请号: PCT/CN2023/092602

(22) 国际申请日: 2023 年 5 月 6 日 (06.05.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **OPPO** 广东移动通信有限公司 **(GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人:甘露**(GAN, Lu)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

(74) 代理人:北京易光知识产权代理有限公司**(BEIJING ELITE GROUP INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市朝阳区光华路8号和乔大厦C座1201, Beijing 100020 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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)。

(54) **Title:** AUTHENTICATION METHODS, KEY GENERATION METHOD, AND DEVICE

(54) 发明名称: 认证方法、密钥生成方法和设备

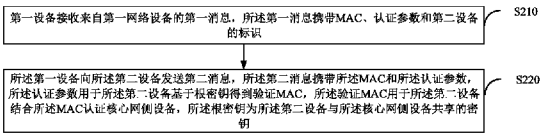

图2

S210 A first device receives a first message from a first network device, the first message carrying a MAC, an authentication parameter, and an identifier of a second device

S220 The first device sends a second message to the second device, the second message carrying the MAC and the authentication parameter, the authentication parameter being used for the second device to obtain a verification MAC on the basis of a root key, the verification MAC being used for the second device to authenticate, in combination with the MAC, a core network side device, and the root key being a key shared by the second device and the core network side device

(57) **Abstract:** The present application relates to authentication methods, a key generation method, a device, a computer-readable storage medium, a computer program product and a computer program. An authentication method comprises: a first device receiving a first message from a first network device, the first message carrying a MAC, an authentication parameter, and an identifier of a second device; and the first device sending a second message to the second device, the second message carrying the MAC and the authentication parameter, the authentication parameter being used for the second device to obtain a verification MAC on the basis of a root key, the verification MAC being used for the second device to authenticate, in combination with the MAC, a core network side device, and the root key being a key shared by the second device and the core network side device.

(57) 摘要: 本申请涉及一种认证方法、密钥生成方法、设备、计算机可读存储介质、计算机程序产品和计算机程序。其中方法包括：第一设备接收来自第一网络设备的第一消息，所述第一消息携带MAC、认证参数和第二设备的标识；所述第一设备向所述第二设备发送第二消息，所述第二消息携带所述MAC和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证MAC，所述验证MAC用于所述第二设备结合所述MAC认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

WO 2024/229634 A1

[见续页]

本国际公布:
— 包括国际检索报告(条约第21条(3))。

认证方法、密钥生成方法和设备

技术领域

本申请涉及通信领域，更具体地，涉及一种认证方法、密钥生成方法、设备、计算机可读存储介质、计算机程序产品和计算机程序。

背景技术

在相关技术中的 UE（用户设备，User Equipment）与核心网的认证过程以及密钥协商过程，所使用的计算函数复杂度较高，密钥架构较复杂。然而，零功耗设备比如 A-IoT 设备，也存在接入网络比如核心网的需求，如何能够使得 A-IoT 设备能够保证安全性的同时，采用较低复杂度的计算方式就实现与网络侧之间的认证，就成为需要解决的问题。

发明内容

本申请实施例提供一种认证方法、密钥生成方法、设备、计算机可读存储介质、计算机程序产品和计算机程序。

本申请实施例提供一种认证方法，包括：

第一设备接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二设备的标识；

所述第一设备向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

本申请实施例提供一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带消息认证码 MAC 和认证参数；

所述第二设备基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与核心网侧设备共享的密钥；

所述第二设备在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

本申请实施例提供一种认证方法，包括：

第一网络设备向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

本申请实施例提供一种密钥生成方法，包括：

电子设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

本申请实施例提供一种认证方法，包括：

第一设备接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；

第一设备向所述第二设备发送第二消息，所述第二消息携带认证参数；

所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共

享的密钥；

所述第一设备向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

本申请实施例提供一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

所述第二设备基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

本申请实施例提供一种认证方法，包括：

第一网络设备向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识；

所述第一网络设备接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

本申请实施例提供一种认证方法，包括：

第一设备向第二设备发送第二消息，所述第二消息携带认证参数；

所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第二 RES 与所述认证参数和第一密钥相关；

所述第一设备基于所述认证参数和所述第一密钥生成第二验证 RES；

所述第一设备在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

本申请实施例提供一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

所述第二设备基于所述认证参数和物理层密钥计算第二 RES，所述第一密钥与所述第一设备相关；

所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

本申请实施例提供一种第一设备，包括：

第一通信单元，用于接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

本申请实施例提供第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带消息认证码 MAC 和认证参数；

第二处理单元，用于基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与核心网侧设备共享的密钥；在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网

侧设备完成认证。

本申请实施例提供一种第一网络设备，包括：

第三通信单元，用于向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

本申请实施例提供一种电子设备，包括：

第四处理单元，用于计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

本申请实施例提供一种第一设备，包括：

第一通信单元，用于接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

本申请实施例提供一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备；

第二处理单元，用于基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

本申请实施例提供一种第一网络设备，包括：

第三通信单元，用于向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识；接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

第三处理单元，用于在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

本申请实施例提供一种第一设备，包括：

第一通信单元，用于向第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第二 RES 与所述认证参数和第一密钥相关；

第一处理单元，用于基于所述认证参数和所述第一密钥生成第二验证 RES；在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

本申请实施例提供一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备；

第二处理单元，用于基于认证参数和第一密钥计算第二 RES，所述第一密钥与所述第一设备相

关。

本申请实施例提供一种第一设备，包括收发器、处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，以使该第一设备执行上述方法。

本申请实施例提供一种第二设备，包括收发器、处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，以使该第二设备执行上述方法。

本申请实施例提供一种第一网络设备，包括收发器、处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，以使该第一网络设备执行上述方法。

本申请实施例提供一种电子设备，包括收发器、处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，以使该电子设备执行上述方法。

本申请实施例提供一种芯片，用于实现上述方法。

具体地，该芯片包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该芯片的设备执行上述的方法。

本申请实施例提供一种计算机可读存储介质，用于存储计算机程序，当该计算机程序被设备运行时使得该设备执行上述方法。

本申请实施例提供一种计算机程序产品，包括计算机程序指令，该计算机程序指令使得计算机执行上述方法。

本申请实施例提供一种计算机程序，当其在计算机上运行时，使得计算机执行上述方法。

通过采用本实施例提供的方案，第一设备向第二设备发送认证参数，进而可以使得第二设备直接根据认证参数和与核心网侧设备共享的根密钥计算得到验证 MAC，基于验证 MAC 对接收到的 MAC 对核心网设备进行认证。如此，在保证了第二设备与核心网侧设备的认证过程的安全性的同时，避免第二设备侧执行较为复杂的计算，提升了第二设备的处理效率，尤其适用于运算能力较低的设备。

附图说明

图 1 是根据本申请实施例的应用场景的示意图。

图 2 是根据本申请一实施例的认证方法的示意性流程图。

图 3 是根据本申请另一实施例的认证方法的示意性流程图。

图 4 是根据本申请另一实施例的认证方法的示意性流程图。

图 5 是根据本申请一实施例的密钥生成方法的示意性流程图。

图 6~图 20 是根据本申请一实施例认证方法的多种示例流程示意图、以及多种密钥架构示意图和多种认证架构示意图。

图 21 是根据本申请一实施例的认证方法的示意性流程图。

图 22 是根据本申请另一实施例的认证方法的示意性流程图。

图 23 是根据本申请另一实施例的认证方法的示意性流程图。

图 24 是根据本申请一实施例的认证方法的示意性流程图。

图 25 是根据本申请另一实施例的认证方法的示意性流程图。

图 26 是相关技术中 AIOT 设备接入网络的场景示意图。

图 27 是 AKA 认证流程示意图。

图 28 是相关技术的认证架构示意图。

图 29 是相关技术中的密钥架构示意图。

图 30 是根据本申请的一实施例的第一设备的示意性框图。

图 31 是根据本申请的一实施例的第二设备的示意性框图。

图 32 是根据本申请的一实施例的第一网络设备的示意性框图。

图 33 是根据本申请的一实施例的电子设备的示意性框图。

图 34 是根据本申请实施例的通信设备示意性框图。

图 35 是根据本申请实施例的芯片的示意性框图。

图 36 是根据本申请实施例的通信系统的示意性框图。

具体实施方式

本申请实施例的技术方案可以应用于各种通信系统，例如：GSM、CDMA、WCDMA、GPRS、LTE、LTE-A、NR、NR 的演进、WLAN、WiFi、或其他通信系统等。

本申请实施例结合网络设备和终端描述了各个实施例，终端可以是移动或固定的，终端也可以称为移动站、用户单元等。终端可以是 WLAN 中的站点，可以是智能终端、无线调制解调器、笔记本电脑、平板电脑等终端。在本申请实施例中，终端可以是 VR 终端/AR 终端、工业控制终端、无人驾驶终端、远程医疗终端、智能电网终端、运输安全终端、智慧城市终端或智慧家庭的无线终端等。作为示例而非限定，在本申请实施例中，该终端还可以是可穿戴设备。

在本申请实施例中，网络设备可以是用于与终端通信的设备，网络设备可以是 WLAN 中的接入点，GSM、CDMA 或 WCDMA 中的基站，还可以是 LTE 中的演进型基站，或者中继站，或者车载设备、可穿戴设备和 NR 网络中的网络设备（gNB）或者未来演进的 PLMN 网络中的网络设备或者非地面网络中的网络设备等。作为示例而非限定，在本申请实施例中，网络设备可以具有移动特性，例如网络设备可以为移动的设备。

应理解，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。应理解，在本申请的实施例中提到的“指示”可以是直接指示，也可以是间接指示，还可以是表示具有关联关系。举例说明，A 指示 B，可以表示 A 直接指示 B，例如 B 可以通过 A 获取；也可以表示 A 间接指示 B，例如 A 指示 C，B 可以通过 C 获取；还可以表示 A 和 B 之间具有关联关系。在本申请实施例的描述中，术语“对应”可表示两者之间具有直接对应或间接对应的关系，也可以表示两者之间具有关联关系，也可以是指示与被指示、配置与被配置等关系。

为便于理解本申请实施例的技术方案，以下对本申请实施例的相关技术进行说明，以下相关技术作为可选方案与本申请实施例的技术方案可以进行任意结合，其均属于本申请实施例的保护范围。

图 1 示例性地示出了一种通信系统 100。该通信系统包括一个网络设备 110 和两个终端 120。在一种可能的实现方式中，该通信系统 100 可以包括多个网络设备 110，并且每个网络设备 110 的覆盖范围内可以包括其它数量的终端 120，本申请实施例对此不做限定。在一种可能的实现方式中，该通信系统 100 还可以包括移动性管理实体、接入与移动性管理功能、等其他网络实体，本申请实施例对此不作限定。其中，网络设备又可以包括接入网设备和核心网设备。即通信系统还可以包括用于与接入网设备进行通信的多个核心网。接入网设备可以是 LTE、LTE-A、或 NR 系统的基站。以图 1 示出的通信系统为例，通信设备可包括具有通信功能的网络设备和终端，通信设备还可包括通信系统中的其他设备，例如网络控制器、移动管理实体等其他网络实体，本申请实施例中对此不做限定。

图 2 是根据本申请一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S210、第一设备接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二

设备的标识；

S220、所述第一设备向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

图 3 是根据本申请另一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S310、第二设备接收来自第一设备的第二消息，所述第二消息携带消息认证码（MAC，Message authentication code）和认证参数；

S320、所述第二设备基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

S330、所述第二设备在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

图 4 是根据本申请另一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S410、第一网络设备向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

图 5 是根据本申请另一实施例的一种密钥生成方法的示意性流程图。该方法包括以下内容的至少部分内容。

S510、电子设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

所述核心网侧设备包括以下之一：一个或多个核心网设备、验证服务器（AS，Authentication Server）。

所述第二设备为环境供能物联网（AIoT，Ambient IoT）设备，该 AIoT 设备还可以表示为 A-IoT 设备，本实施例不对其全部可能的表示方式进行穷举。在一些可能的示例中，第二设备还可以为零功耗设备，比如，可以是有源零功耗设备、或无源零功耗设备、或半无源零功耗设备等等，可选地，该第二设备可以称为标签（Tag），可选地该第二设备还可以为 IoT 设备等等。在另一些可能的示例中，该第二设备可以是运算能力较低的终端。关于该第二设备全部可能的名称或可能的设备，这里不做穷举。

所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备（Authenticator）、第一核心网设备。该第一核心网设备可以包括以下至少之一：AMF(Access and Mobility Management Function，接入和移动性管理功能)、SEAF（安全锚点功能，securityanchorfunction）、专用于 AIoT 服务的核心网网元（比如可以简称为 AIoT 网元）；另外，该第一核心网设备还可以为其他核心网的网元，这里不做穷举。

所述一个或多个核心网设备，至少可以包括以下至少之一：AUSF、UDM（统一数据管理功能，Unified Data Management）、ARPF（Authentication credential Repository and Processing Function 认证凭

证存储库和处理功能)。应理解，这里仅为示例性说明，实际处理中，该一个或多个核心网设备还可以包括核心网的其他设备，只是这里不做穷举。所述第一网络设备可以是前述核心网侧设备中之一，示例性的，所述第一网络设备为 AUSF（鉴权服务功能，Authentication Server Function）或验证服务器。

在一些可能的实施方式中，所述认证参数包括以下之一：匿名密钥（AK, Anonymous Key)、第一随机数。

所述第二设备基于所述认证参数和所述根密钥计算验证 MAC，可以包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC；所述第二设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC；所述第二设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC；所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC。

可选地，所述认证参数包括匿名密钥。相应的，所述第二设备基于所述认证参数和所述根密钥计算验证 MAC，可以包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC；所述第二设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC。

这里，所述第一计算方式可以包括以下至少之一：第二鉴权函数、哈希算法、高级加密标准（AES，Advanced Encryption Standard)、ACSON、SNOW 3G (Snow ThirdGeneration，第三代移动通信积雪)、ZUC（ZUChongzhi，祖冲之)。其中，第二鉴权函数可以表示为 f2（)；哈希算法可以表示为 HASH（)，该哈希算法可以包括 HMAC-SHA-256（Hash based Message Authentication Code-Secure Hash Algorithm-256， 基于散列的消息鉴别码的安全散列算法 256)，或者还可以采用其他哈希算法，本实施例不做穷举。另外，上述第一计算方式也仅为示例性说明，实际处理中，可以用于计算 MAC 或验证 MAC 的其他算法，也可以包含在上述第一计算方式内，这里不做穷举。

示例性的，所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，AK)，其中，MAC'表示验证 MAC，f2（）表示第一计算方式具体为第二鉴权函数，Kr 表示根密钥，AK 表示匿名密钥。上述根密钥除了可以表示为 Kr，还可以表示为 K、PSK（预共享密钥，PreShared Key)、PMK（Pairwise Master Key，成对主密钥）等等任意之一，相应的本实施例（包括下文）所提供的各个公式示例中的 Kr 均可以替换表示为 K、PSK、PMK 等等，这里不做穷举。

示例性的，所述第二设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，可以采用以下公式计算：$RAND = Kr \oplus AK$，其中，RAND 表示第一随机数，Kr 表示根密钥，AK 表示匿名密钥，$\oplus$ 表示异或计算。所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，RAND)，关于该公式中各个参数的含义与前述实施例相同，不做重复说明。

可选地，所述认证参数包括第一随机数。相应的，所述第二设备基于所述认证参数和所述根密钥计算验证 MAC，可以包括以下之一：所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC；所述第二设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC。

示例性的，所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，RAND)，其中，MAC'表示验证 MAC，f2（）表示

第一计算方式具体为第二鉴权函数，Kr 表示根密钥，RAND 表示第一随机数。

示例性的，所述第二设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，可以采用以下公式计算： $AK = Kr \oplus RAND$ ，其中，RAND 表示第一随机数，Kr 表示根密钥，AK 表示匿名密钥， $\oplus$ 表示异或计算。所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，AK），其中，公式中各个参数的含义与前述实施例相同，不做赘述。

可选地，所述第二消息还携带服务参数，所述服务参数包括以下至少之一：用于指示 AIoT 服务类型的类型参数、具备 AIoT 服务功能的服务器的标识、用于指示 AIoT 认证类型的类型参数。

所述用于指示 AIoT 服务类型的类型参数中，该类型参数可以是一个标识符，比如第一标识符用于指示 AIoT 服务类型。该第一标识符的具体取值或具体内容可以根据实际情况设置，比如，第一标识符可以包括内容描述信息“AIoT 服务”；或第一标识符可以包括取值，比如取值为 01 的时候标识 AIOT 服务类型；或者第一标识符可以为其他取值或其他内容，只要唯一用于指示当前的服务类型为 AIoT 服务类型，就在本实施例保护范围内。

用于指示 AIoT 认证类型的类型参数中，该类型参数可以是另一个标识符，比如第二标识符用于指示 AIoT 认证类型。该第二标识符的具体取值或内容可以根据实际情况设置，比如，第二标识符可以包括内容描述信息“AIoT 认证”；或第二标识符可以包括取值，比如取值为 00 的时候标识 AIOT 认证类型；或者第一标识符可以为其他取值或其他内容，只要唯一用于指示当前的认证类型为 AIoT 认证类型，就在本实施例保护范围内。

具备 AIoT 服务功能的服务器，可以指的是提供 AIoT 相关服务的服务器，比如，可以是 AF（应用功能，Application Function）网元，或者可以是核心网侧的具备 AIoT 服务功能的网元，或者也可以是其他服务器，这里不对其进行穷举。上述标识可以包括网络标识和/或 ID；网络标识可以包括：IP 地址（(Internet Protocol Address，互联网协议地址)、MAC（Media Access Control Address，媒体访问控制地址）地址等等至少一种。

其中，所述第二消息可以携带前述认证参数、服务参数以及 MAC。或者，第二消息可以携带认证参数和 MAC，且认证参数中包括以下至少之一：匿名密钥、第一随机数、服务参数；举例来说，该认证参数包括匿名密钥；或该认证参数包括第一随机数；或该认证参数包括匿名密钥以及服务参数；或该认证参数包括第一随机数和服务参数。

所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，包括：所述第二设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所述验证 MAC；和/或，所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC，包括：所述第二设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述验证 MAC。

示例性的，仍然以第一计算方式具体为第二鉴权函数为例，上述第二设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，AK，服务参数），其中各个参数的含义与前述实施例相同，不做赘述。

示例性的，仍然以第一计算方式具体为第二鉴权函数为例，所述第二设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，RAND，服务参数），其中各个参数的含义与前述实施例相同，不做赘述。

需要指出，以上示例中仅采用第二鉴权函数作为第一计算方式为例对生成验证 MAC 进行说明，实际处理中，可以采用上述第一计算方式中任意之一计算验证 MAC，只是不做一一赘述。

在一些可能的实施方式中，所述方法还包括以下之一：所述第一网络设备接收来自第二网络设备的所述 MAC 和所述认证参数；所述第一网络设备生成所述认证参数，所述第一网络设备基于所述根密钥和所述认证参数计算所述 MAC。

所述第一网络设备生成所述认证参数的方式，本实施例不做限定。需要指出的是，认证参数可以包括匿名密钥或第一随机数，在第一网络设备侧可以预先生成匿名密钥以及第一随机数，然后将两种中任意之一作为认证参数。该第一网络设备生成第一随机数的方式本实施例不做限定，该匿名密钥与第一随机数之间的关系可以是：第一随机数与根密钥异或后得到匿名密钥。

所述第一网络设备基于所述根密钥和所述认证参数计算所述 MAC，包括以下之一：所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC；所述第一网络设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC；所述第二设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC；所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC。关于上述第一计算方式的详细说明，与前述实施例相同，不做赘述。

可选地，所述认证参数包括匿名密钥。所述第一网络设备基于所述认证参数和所述根密钥计算 MAC，可以包括以下之一：所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC；所述第一网络设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC。

示例性的，所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，AK），其中，MAC 表示 MAC，f2（）表示第一计算方式具体为第二鉴权函数，Kr 表示根密钥，AK 表示匿名密钥。

示例性的，所述第一网络设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所可以采用的公式与前述实施例相同，不做重复说明。所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，RAND），关于该公式中各个参数的含义与前述实施例相同，不做重复说明。

可选地，所述认证参数包括第一随机数。相应的，所述第一网络设备基于所述认证参数和所述根密钥计算 MAC，可以包括以下之一：所述第一网络设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC；所述第一网络设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC。

所述第一网络设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC，可以采用的公式与前述实施例相同。所述第一网络设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥、以及所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，所采用的公式也与前述实施例相同，因此不做赘述。

需要指出，以上仅以第一计算方式为第二鉴权函数为例进行了示例性说明，在实际处理中，第一计算方式可以不限于上述第二鉴权函数，可以采用上述哈希算法、高级加密标准 AES、ACSON、SNOW 3G、ZUC 中任意之一作为第一计算方式，还可以采用其他计算方式作为第一计算方式，本实施例不做穷举。

可选地，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC，包括：所述第一网络设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所

述 MAC；和/或，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC，包括：所述第一网络设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述 MAC。

这种情况下，所述第一消息还携带所述服务参数。关于服务参数的说明与前述实施例相同，不做重复说明。其中，所述第一消息可以携带前述认证参数、服务参数以及 MAC。或者，第一消息可以携带认证参数和 MAC，且认证参数中包括以下至少之一：匿名密钥、第一随机数、服务参数；举例来说，该认证参数包括匿名密钥；或该认证参数包括第一随机数；或该认证参数包括匿名密钥以及服务参数；或该认证参数包括第一随机数和服务参数。关于第一网络设备生成该服务参数或获取该服务参数的方式，本实施例不做限定。

示例性的，仍然以第一计算方式具体为第二鉴权函数为例，所述第一网络设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，AK，服务参数），其中各个参数的含义与前述实施例相同，不做赘述。

示例性的，仍然以第一计算方式具体为第二鉴权函数为例，所述第一网络设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，RAND，服务参数），其中各个参数的含义与前述实施例相同，不做赘述。

可选地，该第二网络设备可以为核心网侧的设备，也就是该第二网络设备可以为第二核心网设备，由于该第二网络设备为核心网侧的设备，因此该第二网络设备保存有前述第二设备对应的根密钥，关于该第二网络设备生成或获取第二设备对应的根密钥的方式，本实施例不做限定。

其中，所述第二网络设备也可以是前述核心网侧设备中至少之一，示例性的，该第二网络设备可以包括以下至少之一：UDM、ARPF。另外，关于第二网络设备得到 MAC 的方式本实施例也不做限定。

所述第一网络设备接收来自第二网络设备的所述 MAC 和所述认证参数，还可以包括：所述第一网络设备接收来自第二网络设备的服务参数、所述 MAC 和所述认证参数。这种情况下，所述第一消息还携带所述服务参数。关于服务参数的说明与前述实施例相同，不做重复说明。所述第一消息可以携带前述服务参数的方式也与前述实施例相同，不做赘述。

本示例中，关于该第二网络设备计算 MAC 的方式，与前述第一网络设备计算 MAC 的方式相同，因此不做重复说明。

还需要指出，第一网络设备或第二网络设备计算 MAC 所采用的算法，与第二设备计算验证 MAC 所采用的算法应为相同的。比如，以第一网络设备和第二设备为例，第一网络设备同样采用哈希算法基于所述匿名密钥和所述根密钥计算所述 MAC，第二设备采用哈希算法基于所述匿名密钥和所述根密钥计算所述验证 MAC。其他情况与上述说明相同，不做一一赘述。

在一些可能的实施方式中，所述第二设备的处理还可以包括：在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

上述第二设备还可以执行以下处理：第二设备判断验证 MAC 与 MAC 是否相同。另外，还可以包括：在所述验证 MAC 与所述 MAC 不同的情况下，所述第二设备对所述核心网侧设备认证失败。进一步，若第二设备对所述核心网侧设备认证失败，可以不执行后续处理，或者，第二设备还可以向第一设备（比如通过第一设备向第一网络设备）发送对所述核心网侧设备认证失败的消息。

上述第二设备对所述核心网侧设备完成认证，还可以称为第二设备对核心网侧设备的身份认证通过，或第二设备认证核心网侧设备身份通过，或第二设备成功认证核心网侧设备。

在一些可能的实施方式中，上述第三消息可以携带以下至少之一：第一 RES（Response，响应），所述第一 RES 用于所述核心网侧设备认证所述第二设备；第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

在一些可能的示例中，上述第三消息携带第一 RES。

这种情况下，第一设备的处理可以包括：所述第一设备向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES。进一步，所述第一设备还可以向第二设备发送响应消息，比如，该第一设备接收来自第一网络设备的认证第二设备通过的通知，第一设备向第二设备发送响应消息，该响应消息响应于第三消息，该响应消息用于指示核心网侧设备对第二设备认证通过。相应的，第一网络设备接收来自所述第一设备的第四消息之后的处理可以包括：所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定认证所述第二设备通过。示例性的，所述第一网络设备确定认证所述第二设备通过之后，还可以向第一设备发送认证第二设备通过的通知。示例性的，还可以包括：所述第一网络设备在所述第一 RES 和第一验证 RES 不同的情况下，确定认证所述第二设备不通过，进而可以结束处理，或者可以通过第一设备向第二设备发送认证失败的通知，这里不对其后续可能的处理进行限定。进一步地，还可以包括：确定认证所述第二设备通过的情况下，第一网络设备向第一设备发送认证第二设备通过的通知。

前述第二设备计算得到该第一 RES 的方式，包括以下之一：所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES；所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES。

可选地，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES，可以指的是：所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC 的情况下，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES。也就是计算第一 RES（或第一验证 RES）所采用的参数、与前述实施例中计算验证 MAC（或 MAC）所采用的参数至少部分不同。另外，计算第一 RES 所采用的具体算法与计算 MAC 也可以不同，比如计算第一 RES 采用哈希算法，计算 MAC 可以采用第二鉴权函数。

举例来说，所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，AK）。所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES，可以采用以下公式计算：RES=f2（Kr，RAND）。其中，RES 表示第一 RES，Kr 表示根密钥，RAND 表示第一随机数，AK 表示匿名密钥，上述公式中其他内容的含义与前述实施例相同，不做赘述。

进一步地，可以增加服务参数来计算第一 RES。上述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES，可以包括：第二设备采用所述第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算第一 RES。举例来说，第二设备采用所述第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算第一 RES，可以采用以下公式：RES=f2（Kr，RAND，服务参数），其中，公式中各个内容的含义与前述实施例相同，不做赘述。

应理解的是，上述第二设备采用第一计算方式基于服务参数、第一随机数和根密钥计算第一 RES 的情况下，第二设备可以采用服务参数、匿名密钥和根密钥计算验证 MAC，或者第二设备也可以仅采用匿名密钥和根密钥计算验证 MAC。在第二设备采用第一计算方式基于第一随机数和根密钥计算第一 RES 的情况下，第二设备可以采用服务参数、匿名密钥和根密钥计算验证 MAC，或者第二设备也可以仅采用匿名密钥和根密钥计算验证 MAC，以上处理方式均在本实施例保护范围内。

可选地，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES，可以指的是：所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC 的情况下，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES。

举例来说，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC，可以采用以下公式计算：MAC'=f2（Kr，RAND）。所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES，可以采用以下公式计算：RES=f2（Kr，AK），其中，RES 表示第一 RES，公式中其他内容的含义与前述实施例相同，不做赘述。

进一步地，可以增加服务参数来计算第一 RES。所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES，可以包括：所述第二设备采用所述第一计算方式基于所述服务参数、所述匿名密钥和所述根密钥计算第一 RES。举例来说，可以采用以下公式来表示：RES=f2（Kr，AK，服务参数），其中，公式中各个内容的含义与前述实施例相同，不做赘述。

应理解的是，上述第二设备采用所述第一计算方式基于所述服务参数、所述匿名密钥和所述根密钥第一 RES 的情况下，第二设备可以采用服务参数、第一随机数和根密钥计算验证 MAC，或者第二设备也可以仅采用第一随机数和根密钥计算验证 MAC。上述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥第一 RES 的情况下，第二设备可以采用服务参数、第一随机数和根密钥计算验证 MAC，或者第二设备也可以仅采用第一随机数和根密钥计算验证 MAC，以上处理方式均在本实施例保护范围内。

在第一网络设备侧，得到第一验证 RES 的方式，可以包括以下之一：所述第一网络设备接收来自第二网络设备的第一验证 RES；所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES。其中，所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES，包括以下之一：所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES；所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES。

所述第一验证 RES，可以为第一预期响应（XRES，Expected Response）。在下文中，如果没有特殊说明，第一验证 RES 与第一 XRES 含义相同，不做重复解释。

所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES 可以指的是：所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC 的情况下，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES。

举例来说，所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，AK）。所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES，可以采用以下公式计算：XRES=f2（Kr，RAND），其中，XRES 表示第一验证 RES，公式中其他内容的含义与前述实施例相同，不做赘述。

进一步地，可以增加服务参数来计算第一验证 RES。上述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES，可以包括：第一网络设备采用所述第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算第一验证 RES。举例来说，第二设备采用所述第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算第一验证 RES，可以采用以下公式：XRES=f2（Kr，RAND，服务参数），其中，公式中各个内容的含义与前述实施例相同，不做赘述。

应理解的是，上述第一网络设备（或第二网络设备）采用第一计算方式基于服务参数、第一随机数和根密钥计算第一验证 RES 的情况下，第一网络设备（或第二网络设备）可以采用服务参数、匿名密钥和根密钥计算 MAC，或者第一网络设备也可以仅采用匿名密钥和根密钥计算 MAC。在第一网络设备（或第二网络设备）采用第一计算方式基于第一随机数和根密钥计算第一验证 RES 的情况下，第一网络设备（或第二网络设备）可以采用服务参数、匿名密钥和根密钥计算 MAC，或者第一网络设备（或第二网络设备）也可以仅采用匿名密钥和根密钥计算 MAC，以上处理方式均在本实施例保护范围内。

所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES，可以指的是：所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC 的情况下，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES。

举例来说，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC，可以采用以下公式计算：MAC=f2（Kr，RAND)。所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES，可以采用以下公式计算：XRES=f2（Kr，AK)，其中，XRES 表示第一验证 RES，公式中其他内容的含义与前述实施例相同，不做赘述。

进一步地，可以增加服务参数来计算第一验证 RES。所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES，可以包括：所述第一网络设备采用所述第一计算方式基于所述服务参数、所述匿名密钥和所述根密钥计算第一验证 RES。举例来说，可以采用以下公式来表示：XRES=f2（Kr，AK，服务参数)，其中，公式中各个内容的含义与前述实施例相同，不做赘述。

应理解的是，上述第一网络设备（或第二网络设备）采用所述第一计算方式基于所述服务参数、所述匿名密钥和所述根密钥第一验证 RES 的情况下，第一网络设备（或第二网络设备）可以采用服务参数、第一随机数和根密钥计算 MAC，或者第一网络设备（或第二网络设备）也可以仅采用第一随机数和根密钥计算 MAC。上述第一网络设备（或第二网络设备）采用所述第一计算方式基于所述匿名密钥和所述根密钥第一验证 RES 的情况下，第一网络设备（或第二网络设备）可以采用服务参数、第一随机数和根密钥计算 MAC，或者第一网络设备（或第二网络设备）也可以仅采用第一随机数和根密钥计算 MAC，以上处理方式均在本实施例保护范围内。

上述第一网络设备接收来自第二网络设备的第一验证 RES，可以指的是：第一网络设备接收来自第二网络设备的第一验证 RES、MAC、认证参数。同时，该第一网络设备还可以接收来自第二网络设备的服务参数，关于该服务参数的说明与前述实施例相同，不做赘述。

举例来说，第一网络设备可以是同时接收到第二网络设备发来的第一验证 RES、MAC、认证参数，但是仅将其中的 MAC 和认证参数携带在第一消息中，发送给第一设备；相应的，第一设备接收到第一消息之后，将第一消息中的 MAC 和认证参数携带在第二消息中发送给第二设备。再举例来说，第一网络设备可以是同时接收到第二网络设备发来的第一验证 RES、MAC、认证参数和服务参数，但是仅将其中的 MAC、认证参数和服务参数携带在第一消息中，发送给第一设备；相应的，第一设备接收到第一消息之后，将第一消息中的 MAC、认证参数和服务参数携带在第二消息中发送给第二设备。还需要指出的是，若由第二网络设备得到第一验证 RES，该第二网络设备计算该第一验证 RES 的具体方式，与以上实施例中第一网络设备计算第一验证 RES 的方式应为相同的，因此不做重复说明。另外，上述第一消息还可以携带第二设备的标识。

上述第二设备计算第一 RES、第一网络设备（或第二网络设备）计算第一验证 RES 所采用的参数、以及具体的计算函数应为相同的，比如，第二设备采用了第二鉴权函数基于服务参数、所述匿名密钥和所述根密钥计算第一 RES，则第一网络设备（或第二网络设备）也应采用第二鉴权函数基于服务参数、所述匿名密钥和所述根密钥计算第一验证 RES；又比如，第二设备采用了哈希算法基于第一随机数和所述根密钥计算第一 RES，第一网络设备（或第二网络设备）也应采用哈希算法基于第一随机数和所述根密钥计算第一验证 RES。

在一些可能的示例中，上述第三消息携带第一 RES、且所述第一消息还携带所述第一验证 RES。

这种情况下，所述第一设备可以代替第一网络设备认证第二设备，该第一设备接收来自第二设备的第三消息之后的处理可以包括：所述第一设备在所述第一 RES 与所述第一验证 RES 相同的情况下，确定认证所述第二设备通过。关于这种示例中，第一网络设备得到第一验证 RES 的方式、以及第二设备得到第一 RES 的方式，均与前述示例相同，因此不做重复说明。进一步，所述第一设备还可以向第二设备发送响应消息，比如，该第一设备确定认证所述第二设备通过的情况下，第一设备向第二设备发送响应消息，该响应消息响应于第三消息，该响应消息用于指示核心网侧设备对第二设备认证通过。

在一些可能的示例中，上述第三消息携带第二 RES。

这种情况下，第一设备接收来自第二设备的第三消息之后的处理可以包括：所述第一设备在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。进一步，还可以包括：所述第一设备向所述第二设备发送响应消息，所述响应消息用于指示对所述第二设备认证通过。

相应的，第二设备的处理可以包括：所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息，所述响应消息用于指示对所述第二设备认证通过。

示例性的，在间接模式（Indirect mode）下，第二设备通过终端设备、该终端设备对应的第一接入网设备与核心网连接，这种情况下，上述第一设备为终端设备；另外，上述第一设备为终端设备的情况下，该第一设备可以为代理 UE 或中继 UE 等等。在本示例中，终端设备（比如 UE）对第二 RES 进行验证，并在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

示例性的，直接模式（Direct mode）下，第二设备通过对应的接入网设备与核心网连接，这种情况下，上述第一设备为接入网设备（比如可以是第二设备对应的接入网设备），或者，上述第一设备可以为第一核心网设备，比如可以是 AMF、SEAF、专用于 AIoT（或 IoT）的核心网网元等等至少一种。在本示例中，接入网设备（比如 gNB）、或第一核心网设备（比如 AMF、SEAF、专用于 AIoT 的核心网网元）对第二 RES 进行验证，并在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

另外，还可以包括：所述第一设备在第二验证 RES 与所述第二 RES 不同的情况下，确定认证所述第二设备不通过，进而可以结束处理，或者第一设备向第二设备发送认证失败的通知，这里不对其后续可能的处理进行限定。

第二设备计算得到该第二 RES 的方式，包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和第一密钥计算所述第二 RES，所述第一密钥与所述第一设备相关；所述第二设备采用第一计算方式基于所述第一随机数和第一密钥计算所述第二 RES；所述第二设备采用第一计算方式基于所述第一 RES 和第一密钥计算所述第二 RES。

所述第一密钥可以为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

其中，所述物理层密钥可以是第二设备和第一设备之间通过空口的信道信源特征生成的共享密钥，关于该物理层密钥的具体生成方式，本实施例不做限定，只要是在第二设备与第一设备侧共享的相同密钥就在本实施例保护范围内。

所述第一中间密钥的计算方式可以为：采用第二计算方式基于所述第一设备的标识和第二随机数计算所述第一中间密钥；或者，采用所述第二计算方式基于所述第一设备的标识、所述第二随机数和所述匿名密钥计算所述第一中间密钥。

所述第二计算方式至少可以包括密钥派生函数（KEF，Key Derivation Function），进一步上述第二计算方式还可以包括以下之一：、异或计算、直连计算。应理解，这里仅为示例性说明，实际处理中，该第二计算方式还可以是其他计算方式，本实施例不做穷举。

上述第一设备可以是前述终端设备，相应的，第一设备的标识可以为 UE ID；上述第一设备可以是前述第一接入网设备，相应的，第一设备的标识可以表示为 gNB ID（或 eNB ID 或其他可能的类型的接入网设备的 ID）；上述第一设备可以是第一核心网设备，相应的，第一设备的标识可以表示为第一核心网网元的标识、或中间网元标识、或核心网网元标识等等。

以第一设备为第一核心网设备为例，上述采用第二计算方式基于所述第一设备的标识和第二随机数计算所述第一中间密钥，可以表示为：Km=KDF（中间网元标识，第二随机数）。或者，采用所述第二计算方式基于所述第一设备的标识、所述第二随机数和所述匿名密钥计算所述第一中间密钥，可以表示为：Km=KDF（AK，中间网元标识，第二随机数），其中，Km 表示第一中间密钥，AK 表示匿名密钥。上述第一设备若为终端设备，则上述第一中间密钥的计算公式可以适应性的替换为 Km=KDF（UE ID，第二随机数）、或 Km=KDF（AK，UE ID，第二随机数）。上述第一设备为第一接入网设备也可以适应性进行替换，这里不做一一穷举。

另外，上述第二随机数可以是由第一设备发送至第二设备的；关于该第二随机数的生成方式以及发送时机，本实施例不做限定，比如，可以是在前述第二消息中携带，只要是在执行计算第二 RES 之前就在本实施例保护范围内，这里不做穷举。

示例性的，以第一计算方式为第二鉴权函数为例，所述第二设备采用第一计算方式基于所述匿名密钥和物理层密钥计算所述第二 RES，可以表示为：RES'= f2（物理层密钥，AK），其中，RES'表示第二 RES，公式中其他内容的含义与前述实施例相同，不做赘述。或者，所述第二设备采用第一计算方式基于所述匿名密钥和第一中间密钥计算所述第二 RES，可以表示为：RES'= f2（Km，AK），公式中内容的含义与前述实施例相同，不做赘述。

示例性的，以第一计算方式为第二鉴权函数为例，所述第二设备采用第一计算方式基于所述第一随机数和物理层密钥计算所述第二 RES，可以表示为：RES'= f2（物理层密钥，RAND），其中，RES'表示第二 RES，公式中其他内容的含义与前述实施例相同，不做赘述。或者，所述第二设备采用第一计算方式基于所述匿名密钥和第一中间密钥计算所述第二 RES，可以表示为：RES'= f2（Km，RAND），公式中内容的含义与前述实施例相同，不做赘述。

示例性的，以第一计算方式为第二鉴权函数为例，所述第二设备采用第一计算方式基于所述第一 RES 和物理层密钥计算所述第二 RES，可以表示为：RES'= f2（物理层密钥，RES），其中，RES'表示第二 RES，RES 表示第一 RES，公式中其他内容的含义与前述实施例相同，不做赘述。或者，所述第二设备采用第一计算方式基于所述第一 RES 和第一中间密钥计算所述第二 RES，可以表示为：RES'= f2（Km，RES），公式中内容的含义与前述实施例相同，不做赘述。

第一设备计算第二验证 RES 的方式，包括以下之一：所述第一设备采用第一计算方式对匿名密钥

和第一密钥进行计算，得到所述第二验证 RES；所述第一设备采用第一计算方式对第一随机数和第一密钥进行计算，得到所述第二验证 RES；所述第一设备采用第一计算方式对第一验证 RES 和第一密钥进行计算，得到所述第二验证 RES。示例性的，第二验证 RES，也可以是第二 XRES，在下文中如果没有特殊说明，第二验证 RES 与第二 XRES 含义相同，不做重复解释。所述第一密钥的说明与前述实施例相同，不做赘述。

可选地，上述第一设备所接收到的认证参数，可以包括匿名密钥或第一随机数；若该认证参数包括匿名密钥，则第一设备可以执行采用第一计算方式对匿名密钥和第一密钥进行计算，得到所述第二验证 RES 的处理；若认证参数包括第一随机数，则第一设备采用第一计算方式对第一随机数和第一密钥进行计算，得到所述第二验证 RES。

可选地，上述第一验证 RES 可以是由第一网络设备发送至第一设备的，比如，前述第一消息还可以携带该第一验证 RES。若该第一消息携带第一验证 RES，则第一设备可以选择采用第一计算方式对第一验证 RES 和第一密钥进行计算，得到所述第二验证 RES。或者，若第一消息携带第一验证 RES，第一设备也可以采用认证参数所包括的匿名密钥或第一随机数，计算第二验证 RES，均在本实施例保护范围内，这里不对全部可能的情况进行穷举。

可选地，上述第一设备也可以获取到根密钥，第一设备可以根据认证参数中包含的匿名密钥与根密钥进行异或计算，得到第一随机数；或者，第一设备可以根据认证参数中包含的第一随机数与根密钥进行异或计算，得到匿名密钥；或者，第一设备可以采用根密钥、认证参数，采用与第二设备相同的方式，生成第一验证 RES。这种情况下，第一设备可以采用以上任意一种方式生成第二验证 RES。

示例性的，以第一计算方式为第二鉴权函数为例，所述第一设备采用第一计算方式对匿名密钥和第一密钥进行计算，得到所述第二验证 RES，若该第一密钥为物理层密钥，则可以表示为：XRES'= f2（物理层密钥，AK），其中，XRES'表示第二验证 RES，公式中其他内容的含义与前述实施例相同，不做赘述；若第一密钥为第一中间密钥，则可以表示为 XRES'= f2（Km，AK）。

示例性的，以第一计算方式为第二鉴权函数为例，所述第一设备采用第一计算方式对第一随机数和第一密钥进行计算，得到所述第二验证 RES，若该第一密钥为物理层密钥，则可以表示为：XRES'= f2（物理层密钥，RAND），其中，XRES'表示第二验证 RES，公式中其他内容的含义与前述实施例相同，不做赘述；若第一密钥为第一中间密钥，则可以表示为 XRES'= f2（Km，RAND）。

示例性的，以第一计算方式为第二鉴权函数为例，所述第一设备采用第一计算方式对第一验证 RES 和第一密钥进行计算，得到所述第二验证 RES，若该第一密钥为物理层密钥，则可以表示为：XRES'= f2（物理层密钥，XRES），其中，XRES'表示第二验证 RES，XRES 表示第一验证 RES，公式中其他内容的含义与前述实施例相同，不做赘述；若第一密钥为第一中间密钥，则可以表示为 XRES'= f2（Km，XRES）。

上述第二设备计算第二 RES、第一设备计算第二验证 RES 所采用的参数（或参数类型）、以及具体的计算函数应为相同的，比如，第二设备采用了第二鉴权函数基于匿名密钥和物理层密钥计算第二 RES，则第一设备也应采用第二鉴权函数基于匿名密钥和物理层密钥计算第二验证 RES；又比如，第二设备采用了哈希算法基于第一 RES 和物理层密钥计算第二 RES，第一设备也应采用哈希算法基于第一验证 RES 和物理层密钥计算第二验证 RES。

在另外一些可能的示例中，上述第三消息携带第一 RES 和第二 RES。

这种情况下，第一设备的处理可以包括：所述第一设备向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES；所述第一设备在第二验证 RES 与所述第二 RES 相同的情况下，确定所

述第二设备认证通过。另外，还可以包括：所述第一设备在第二验证 RES 与所述第二 RES 不同的情况下，确定所述第二设备认证不通过（或失败）。

第一网络设备的处理可以包括：所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定认证所述第二设备通过。进一步，还可以包括：第一网络设备向第一设备发送认证第二设备通过（或成功）的通知。另外，第一网络设备的处理，还可以包括：所述第一网络设备在所述第一 RES 和第一验证 RES 不同的情况下，确定认证所述第二设备不通过（或失败）。在第一网络设备确定认证所述第二设备不通过（或失败）的情况下，第一网络设备可以结束处理，或者第一网络设备向第一设备发送对第二设备认证失败（或不通过）的通知，这里不对其后续可能的处理进行限定。

第一设备的处理还可以包括以下之一：在所述第一设备确定所述第二设备认证通过、且所述第一设备接收来自第一网络设备的认证第二设备通过（或成功）的通知的情况下，向第二设备发送响应消息，该响应消息用于指示第二设备认证通过；在所述第一设备确定所述第二设备认证不通过（或失败）、和/或所述第一设备接收来自第一网络设备的认证第二设备失败（或不通过）的通知的情况下，向第二设备发送响应消息，该响应消息用于指示对第二设备认证失败（或认证不通过）。进一步，该响应消息可以进一步携带第一设备对第二设备认证失败和/或核心网侧设备对第二设备认证失败等内容，这里不对其进行限定。

本示例中，关于第二设备计算第一 RES、第二 RES，第一设备得到第二验证 RES、第一网络设备得到第一验证 RES 的方式，均与前述实施例相同，不做重复说明。

针对前述实施例，进一步需要说明的是，在第二设备、第一设备和第一网络设备执行上述认证方法时，可以仅由第二设备基于验证 MAC 和 MAC 对核心网侧进行认证。也可以由第二设备基于验证 MAC 和 MAC 对核心网侧进行认证的基础上，进一步增加由第一网络设备基于第一 RES 和第一验证 RES 对第二设备进行认证，和/或增加由第一设备基于第二 RES 和第二验证 RES 对第二设备进行认证。以上多种可能的方案均在本实施例保护范围内。

另外，由于 AK 需要发送，所以不能用异或等可以逆向推导的算法生成 MAC 和 XRES。由于 Kr 是仅在每个第二设备和核心网侧设备共享唯一不重复的密钥，攻击者截获 AK 也不能得到 RAND 或 Kr，因此生成和发送 AK 是安全的，并且具有低功耗的特点。发送 MAC 也是安全的，并且由于 MAC 是基于 Kr 生成的，只有 AUSF 拥有 Kr，因此验证 MAC 可以验证核心网侧设备的身份。并且，由于 RES 是基于 Kr 生成的，只有第二设备和核心网侧设备拥有 Kr，因此核心网侧设备通过验证 RES 可以验证第二设备的身份。并且，由于 RES’（即第二 RES）和 XRES’（即第二验证 RES）是基于物理层密钥生成的，只有第二设备和第一设备拥有共享的物理层密钥，因此第一设备通过验证 RES’可以验证第二设备的身份。

在一些可能的实施方式中，所述第二设备和第一设备进行密钥协商。

第二设备的处理中，还包括：所述第二设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

第一设备的处理中，还可以包括：所述第一设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

示例性的，该密钥生成参数可以直接从认证参数中提取。比如，认证参数中包括匿名密钥，则密钥生成参数为该认证参数中包含的匿名密钥；或者，认证参数中包括第一随机数，则密钥生成参数为该认证参数中包含的第一随机数。

示例性的，上述密钥生成参数与前述认证参数不同，该密钥生成参数可以是在第二设备基于认证参数执行前述计算验证 MAC、计算第一 RES、计算第二 RES 中任意之一的处理时所得到的。比如，认证参数包括匿名密钥，在第二设备执行前述计算验证 MAC、计算第一 RES、计算第二 RES 中任意之一的处理时得到了第一随机数，第二设备将该第一随机数作为密钥生成参数；又比如，认证参数包括第一随机数，在第二设备执行前述计算验证 MAC、计算第一 RES、计算第二 RES 中任意之一的处理时得到了匿名密钥，第二设备将该匿名密钥作为密钥生成参数。

在一些可能的示例中，所述第二设备和第一设备进行完整性保护密钥的协商。

上述完整性保护密钥用于对第二设备和网络实体（如第一设备）的完整性保护。其中，网络实体可以包括但不限于以下至少之一：UE、其他网络设备；其他网络设备可以包括：AP、small cell（小区）、gNB、CPE、AMF、UPF、MEC 等。由于在第二设备侧和第一设备侧需要分别生成各自的完整性保护密钥进行完整性保护处理，第二设备和第一设备侧生成各自的完整性保护密钥所使用的参数和计算方式应为相同的，因此，本示例中，将第二设备和第一设备称为电子设备来进行完整性保护密钥的生成方式的说明，应指出的是，本示例中的电子设备可以为第二设备也可以为第一设备，不做重复说明。

所述计算完整性保护密钥包括以下之一，包括以下之一：采用第二计算方式基于所述匿名密钥和第三随机数计算所述完整性保护密钥；采用所述第二计算方式基于所述第一随机数和所述第三随机数计算所述完整性保护密钥；采用第二计算方式基于所述匿名密钥、所述第一密钥和第三随机数计算所述完整性保护密钥；采用所述第二计算方式基于所述第一随机数、所述第一密钥和所述第三随机数计算所述完整性保护密钥；采用所述第二计算方式基于第二中间密钥和所述第三随机数计算所述完整性保护密钥，所述第二中间密钥与所述密钥生成参数相关；采用所述第二计算方式基于第三中间密钥和所述第三随机数计算所述完整性保护密钥，所述第三中间密钥与根密钥和所述密钥生成参数相关。

所述方法还包括以下至少之一：采用第三计算方式基于所述匿名密钥计算所述第二中间密钥；采用所述第三计算方式基于所述第一随机数计算所述第二中间密钥；采用第三计算方式基于所述匿名密钥和所述第一密钥计算所述第二中间密钥；采用所述第三计算方式基于所述第一随机数和所述第一密钥计算所述第二中间密钥；采用所述第三计算方式基于所述根密钥和所述第一随机数计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥、所述第一密钥和所述第一随机数计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥、所述第一密钥计算所述第三中间密钥。

所述第三计算方式包括以下之一：第三密钥生成函数、异或计算、直连计算、KDF。

可选地，所述采用第二计算方式基于所述匿名密钥和第三随机数计算所述完整性保护密钥。举例来说，可以表示为：$KI = AK \oplus NONCE1$，其中，KI 表示完整性保护密钥，NONCE1 表示第三随机数，AK 表示匿名密钥；或者可以表示为：$KI = KDF(AK, NONCE1)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述；或者可以表示为：$KI = AK \,||\, NONCE1$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做

赘述。

可选地，采用第二计算方式基于所述匿名密钥、所述第一密钥和第三随机数计算所述完整性保护密钥。

举例来说，上述第一密钥具体可以为物理层密钥，则上述处理可以表示为：$KI = 物理层密钥 \oplus AK \oplus NONCE1$，其中，KI 表示完整性保护密钥，NONCE1 表示第三随机数，AK 表示匿名密钥，该公式中其他内容的含义与前述实施例相同，不做赘述。或者可以表示为：$KI = KDF(物理层密钥, AK, NONCE1)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述。或者可以表示为：$KI = 物理层密钥 || AK || NONCE1$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

举例来说，上述第一密钥具体可以为第一中间密钥，关于该第一中间密钥的生成方式在前述实施例已经详述，不做重复说明。相应的，上述处理可以表示为：$KI = \mathrm{Km} \oplus AK \oplus NONCE1$，其中，KI 表示完整性保护密钥，NONCE1 表示第三随机数，AK 表示匿名密钥，Km 为第一中间密钥。或者可以表示为：$KI = KDF(Km, AK, NONCE1)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述。或者可以表示为：$KI = Km || AK || NONCE1$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

可选地，所述第二设备采用第二计算方式基于所述第一随机数和所述第三随机数计算所述完整性保护密钥。比如，$KI = RAND \oplus NONCE1$，其他计算公式也可以做相似的替换，这里不做一一赘述。

可选地，采用所述第二计算方式基于所述第一随机数、所述第一密钥和所述第三随机数计算所述完整性保护密钥。

以第一密钥为物理层密钥为例，可以将上述 KI 的计算公式中的 AK（匿名密钥）替换为第一随机数 RAND，比如，$KI = 物理层密钥 \oplus RAND \oplus NONCE1$，其他计算公式也可以做相似的替换，这里不做一一赘述。

以第一密钥为第一中间密钥为例，可以将上述 KI 的计算公式中的 AK（匿名密钥）替换为第一随机数 RAND，比如，$KI = Km \oplus RAND \oplus NONCE1$，其他计算公式也可以做相似的替换，这里不做一一赘述。

可选地，所述第二设备采用所述第二计算方式基于第二中间密钥和所述第三随机数计算所述完整性保护密钥。这里，第二中间密钥的生成方式为以下之一：采用第三计算方式基于所述匿名密钥计算所述第二中间密钥；采用所述第三计算方式基于所述第一随机数计算所述第二中间密钥；采用第三计算方式基于所述匿名密钥和所述第一密钥计算所述第二中间密钥；采用所述第三计算方式基于所述第一随机数和所述第一密钥计算所述第二中间密钥。

应理解的是，上述第二中间密钥在一些可能的示例中，还可以称为认证密钥。

一种可能的示例中，采用第三计算方式基于所述匿名密钥计算所述第二中间密钥，可以采用以下公式计算：$Ka = \mathrm{f3}\ (AK)$，Ka 表示第二中间密钥（或称为认证密钥）。另一些可能的示例中，采用第三计算方式基于所述第一随机数计算所述第二中间密钥，可以表示为 $Ka = \mathrm{f3}\ (RAND)$。应理解，以上仅为示例性说明，实际处理中，也可能采用第三计算方式基于匿名密钥和第一随机数共同计算第二中间密钥，比如 Ka=AK||RAND，这里不做穷举。

一种可能的示例中，第一密钥为物理层密钥。采用第三计算方式基于所述物理层密钥和所述匿名

密钥计算所述第二中间密钥，可以采用以下公式计算：$Ka = \text{f3}(AK, \text{物理层密钥})$，其中，Ka 表示第二中间密钥（或称为认证密钥），f3（）表示第三密钥生成函数，AK 表示匿名密钥。上述 Ka 的计算公式，还可以将 f3（）替换为异或，比如，表示为 $Ka = AK \oplus \text{物理层密钥}$；或者，还可以将 f3（）或异或计算替换为直连计算“||”，比如上述公式可以表示为 $Ka = AK \| \text{物理层密钥}$。或者，采用第三计算方式基于所述物理层密钥和所述第一随机数计算所述第二中间密钥。本示例的计算公式，可以将上述示例的计算公式中的匿名密钥（即 AK）替换为第一随机数（即 RAND），比如 $Ka = \text{f3}(RAND, \text{物理层密钥})$，其他可能的计算方式也与前述示例相同，不做一一赘述。由于物理层密钥是第二设备和第一设备之间的共享密钥，具有香农信息论安全性，因此第二中间密钥（或认证密钥）是安全的。

一种可能的示例中，第一密钥为第一中间密钥。采用第三计算方式基于所述第一中间密钥和所述匿名密钥计算所述第二中间密钥，可以采用以下公式计算：$Ka = \text{f3}(AK, Km)$；采用第三计算方式基于所述第一中间密钥和所述第一随机数计算所述第二中间密钥。本示例的计算公式，可以将上述示例的计算公式中的匿名密钥（即 AK）替换为第一随机数（即 RAND），比如 $Ka = \text{f3}(RAND, Km)$，其他可能的计算方式也与前述示例相同，不做一一赘述。

上述计算第二中间密钥的各个示例中，还可以增加第五随机数。比如，采用第三计算方式基于所述物理层密钥、第五随机数和所述匿名密钥计算所述第二中间密钥，上述处理可以表示为：$Ka = \text{f3}(AK, \text{物理层密钥}, \text{NONCE3})$，其中，NONCE3 表示第五随机数；该第五随机数可以是第一网络设备为第二设备和/或第一设备配置或发送的，本实施例不对其进行限定。又比如，采用第三计算方式基于所述匿名密钥和第五随机数计算所述第二中间密钥，可以采用以下公式计算：$Ka = \text{f3}(AK, NONCE3)$。关于上述各个示例中增加第五随机数之后的处理方式，这里不做穷举。

采用所述第二计算方式基于第二中间密钥和所述第三随机数计算所述完整性保护密钥，可以采用以下公式表示：$KI = Ka \oplus NONCE1$，其中，KI 表示完整性保护密钥，Ka 表示第二中间密钥，NONCE1 表示第三随机数。示例性的，上述 KI 的计算公式，还可以将异或计算替换为直连计算“||”，比如上述公式可以表示为 $KI = Ka \| \text{NONCE1}$。示例性的，上述 KI 的计算公式，还可以采用 KDF，比如，上述公式可以表示为 $KI = KDF(Ka, NONCE1)$。

可选地，所述第二设备采用第二计算方式基于第三中间密钥和所述第三随机数计算所述完整性保护密钥。

这种情况下，该第三中间密钥的计算方式可以包括以下之一：采用所述第三计算方式基于所述根密钥和所述第一随机数计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥和所述匿名密钥计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥、所述第一密钥和所述第一随机数计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥计算所述第三中间密钥；采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥、所述第一密钥计算所述第三中间密钥。

在计算第三中间密钥的处理中，与前述示例的区别在于，本示例中增加了根密钥来计算第三中间密钥。

在一种可能的示例中，第一密钥为物理层密钥，相应的，采用第三计算方式基于所述物理层密钥、所述根密钥和所述第一随机数计算所述第三中间密钥，可以采用以下公式计算：

$Ka' = f3(Kr, RAND, 物理层密钥)$，其中 Ka’表示第三中间密钥，上述公式中其他内容的含义与前述实施例相同，不做重复说明。示例性的，上述第三中间密钥的计算公式，还可以将 f3（）替换为异或，比如，表示为 $Ka' = Kr \oplus RAND \oplus 物理层密钥$；或者，还可以将 f3（）或异或计算替换为直连计算“||”，比如上述公式可以表示为 $Ka' = Kr \| RAND \| 物理层密钥$。

或者，第一密钥为第一中间密钥，则采用第三计算方式基于所述第一中间密钥、所述根密钥和所述第一随机数计算所述第三中间密钥，可以采用以下公式计算：$Ka' = f3(Kr, RAND, Km)$，上述公式中内容的含义与前述实施例相同，不做重复说明。示例性的，上述第三中间密钥的计算公式，还可以将 f3（）替换为异或，或者，还可以将 f3（）或异或计算替换为直连计算“||”，不再穷举。应理解，本示例中采用 Ka’来表示第三中间密钥，是为了与前述实施例中的 Ka 表示第二中间密钥进行区分，在一些其他可能的示例中，上述公式的 Ka’也可以直接表示为 Ka，这里不做穷举。

或者，采用第三计算方式基于所述根密钥和所述第一随机数计算所述第三中间密钥，可以采用以下公式计算：$Ka' = f3(Kr, RAND)$。上述第三中间密钥的计算公式，还可以将 f3（）替换为异或或直连计算等等其他方式，这里不做穷举。

或者，采用第三计算方式基于所述根密钥和所述匿名密钥计算所述第三中间密钥，可以采用以下公式计算：$Ka' = f3(Kr, AK)$，上述公式中内容的含义与前述实施例相同，不做重复说明。示例性的，上述第三中间密钥的计算公式，还可以将 f3（）替换为异或，或者，还可以将 f3（）或异或计算替换为直连计算“||”，不再穷举。应理解，本示例中采用 Ka’来表示第三中间密钥，是为了与前述实施例中的 Ka 表示第二中间密钥进行区分，在一些其他可能的示例中，上述公式的 Ka’也可以直接表示为 Ka，这里不做穷举。

相应的，所述第二设备采用第二计算方式基于第三中间密钥和所述第三随机数计算所述完整性保护密钥，可以表示为：$KI = Ka' \oplus NONCE1$。其中，KI 表示完整性保护密钥，NONCE1 表示第三随机数，该公式中其他内容的含义与前述实施例相同，不做赘述。上述公式中的异或计算还可以替换为直连计算或 KDF 计算，这里不做一一赘述。

在又一种可能的示例中，采用第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥。

其中，采用第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，可以表示为：$Ka'' = Kr \oplus RAND$，其中，Ka''表示第四中间密钥，公式中其他内容的含义与前述实施例相同，不做赘述。应理解的是，本示例中采用 Ka''来表示第四中间密钥，是为了与前述实施例中的 Ka 表示的第二中间密钥、以及 Ka’表示的第三中间密钥进行区分，在一些其他可能的示例中，上述公式的 Ka''也可以直接表示为 Ka，这里不做穷举。另外，上述公式中的异或计算也可以替换为 KDF、或直连计算，这里不做一一赘述。

以第一密钥为物理层密钥为例，采用第二计算方式基于所述第四中间密钥和所述物理层密钥计算所述第三中间密钥，可以表示为：$Kb = f2(物理层密钥, Ka'')$，其中，kb 为第三中间密钥，该公式中其他内容的含义与前述实施例相同，不做赘述。

以第一密钥为第一中间密钥为例，采用第二计算方式基于所述第四中间密钥和所述物理层密钥计算所述第三中间密钥，可以表示为：$Kb = f2(Km, Ka'')$，该公式中内容的含义与前述实施例相同，不做赘述。上述 f2（）也可以替换为前述第二计算方式中的其他计算方式，这里不做一一赘述。

采用所述第二计算方式基于所述第四中间密钥计算所述第三中间密钥，可以表示为：

$Kb = f2(Ka")$，上述各个示例中的 f2（）也可以替换为前述第二计算方式中的其他计算方式，这里不做一一赘述。

相应的，采用第二计算方式基于第三中间密钥和所述第三随机数计算所述完整性保护密钥，可以表示为：$KI = Kb \oplus NONCE1$。其中，KI 表示完整性保护密钥，NONCE1 表示第三随机数，该公式中其他内容的含义与前述实施例相同，不做赘述。上述公式中的异或计算还可以替换为直连计算或 KDF 计算，这里不做一一赘述。另外，本实施例中为了与前述实施例 Ka'表示的第三中间密钥进行区分，将第三中间密钥表示为 kb，实际处理中，上述 $Ka"$ 和 kb 也可以替换表示方式，只要计算方式为本示例所提供的计算方式，就在本实施例保护范围内。

需要指出，上述是以电子设备为执行主体为例，对生成完整性保护密钥进行的示例性说明。上述电子设备为第二设备的情况下，可以执行前述生成完整性保护密钥的任意一种或多种处理，不做赘述。上述电子设备为第一设备的情况下，该第一设备若能够得到根密钥，则可以由第一设备执行生成前述第三中间密钥的处理、以及生成第四中间密钥。并且，由于第一设备有物理层密钥，因此能够执行前述生成第二中间密钥的处理。

在有一些可能的示例中，上述第一设备还可以接收第一网络设备发来的第二中间密钥、第三中间密钥、第四中间密钥中至少之一。也就是所述第一消息还携带以下至少之一：所述第二中间密钥、所述第三中间密钥、所述第四中间密钥。

所述第一消息还携带以下至少之一：第二中间密钥、第三中间密钥、第四中间密钥；所述方法还包括以下之一：所述第一网络设备接收所述第二网络设备发来的所述第二中间密钥、所述第三中间密钥、所述第四中间密钥中至少之一；所述第一网络设备采用第三计算方式基于物理层密钥、所述根密钥、所述第一随机数计算所述第三中间密钥，所述物理层密钥为所述第二设备与所述第一设备之间共享的密钥；所述第一网络设备采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥；所述第一网络设备采用所述第二计算方式基于所述第四中间密钥和所述物理层密钥计算所述第三中间密钥；所述第一网络设备采用第三计算方式基于所述物理层密钥和所述匿名密钥计算所述第二中间密钥；所述第一网络设备采用所述第三计算方式基于所述物理层密钥和所述第一随机数计算所述第二中间密钥。

关于上述第一网络设备生成第二中间密钥、第三中间密钥、第四中间密钥的具体处理，与前述实施例中相同，不做重复说明。需要指出的是，第一消息可以仅携带第三中间密钥，也可以仅携带第四中间密钥，或者可以携带第三中间密钥和第四中间密钥，或者也可以上述密钥全都携带，本实施例不对其进行限定。

所述第一网络设备接收所述第二网络设备发来的所述第二中间密钥、所述第三中间密钥、所述第四中间密钥中至少之一，可以指的是，第一网络设备直接从第二网络设备获取所述第二中间密钥、所述第三中间密钥、所述第四中间密钥中至少之一。关于上述第二网络设备生成各个中间密钥的具体处理，与前述实施例相同，不做重复说明。

针对上述生成完整性保护密钥的处理，还需要说明的是，第二设备和第一设备需要采用相同的参数以及相同的计算公式来计算各自的完整性保护密钥，比如，均采用物理层密钥、匿名密钥和第三随机数进行异或计算得到各自的完整性保护密钥。

另外，以上仅为示例性说明，在实际生成完整性保护密钥的处理时，还可以增加其他参数，比如可以包括第二设备的标识，这里不对全部可能的参数进行穷举。

上述示例中，若使用物理层密钥，由于物理层密钥是第二设备和第一设备之间通过空口的信道信

源特征生成的共享密钥，具有香农信息论安全性，因此发送第三随机数（即 NONCE1）是安全的，使用第三随机数和物理层密钥生成的完整性保护密钥也是安全的。并且，由于物理层密钥是不需要密码学计算，因此具有低功耗的特点，更加适合 AIOT 设备使用。由于物理层密钥是第二设备和第一设备之间的共享密钥，因此只有特定的第一设备能够得到正确的完整性保护密钥进而验证消息完整性，攻击者获得了第三随机数也不能得到完整性保护密钥，因此完整性保护密钥具备安全性。

在一些可能的实施方式中，所述第二设备和第一设备进行加密密钥的协商。

在第二设备侧和第一设备侧需要分别生成各自的加密密钥以对两者之间传输的数据加密，第二设备和第一设备侧生成各自的加密密钥所使用的参数和计算方式应为相同的，，因此，本示例中，将第二设备和第一设备称为电子设备来进行加密密钥的生成方式的说明，应指出的是，本示例中的电子设备可以为第二设备也可以为第一设备，不做重复说明。

在本实施方式中，所述密钥生成参数的详细说明，与前述实施例相同，不做赘述。

所述计算加密密钥，可以包括以下之一：采用第二计算方式对第四随机数和所述匿名密钥计算所述加密密钥；采用所述第二计算方式基于所述第一随机数和所述第四随机数计算所述加密密钥；采用第二计算方式基于所述匿名密钥、所述第一密钥和所述第四随机数计算所述加密密钥；采用所述第二计算方式基于所述第一随机数、所述第一密钥和所述第四随机数计算所述加密密钥；采用所述第二计算方式基于第二中间密钥和所述第四随机数计算所述加密密钥，所述第二中间密钥与所述密钥生成参数相关；采用所述第二计算方式基于第三中间密钥和所述第四随机数计算所述加密密钥，所述第三中间密钥与所述根密钥和所述密钥生成参数相关。

上述第二中间密钥以及第三中间密钥的计算方式，与前述实施方式相同，因此本实施方式中不做重复说明。

可选地，所述采用第二计算方式基于所述匿名密钥和第四随机数计算所述加密密钥。举例来说，可以表示为：$Kc = AK \oplus NONCE2$，其中，Kc 表示加密密钥，NONCE2 表示第四随机数，AK 表示匿名密钥；或者可以表示为：$Kc = KDF(AK, NONCE2)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述；或者可以表示为：$Kc = AK \| NONCE2$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

可选地，采用第二计算方式基于所述匿名密钥、所述第一密钥和第四随机数计算所述加密密钥。

举例来说，上述第一密钥具体可以为物理层密钥，则采用第二计算方式对所述第四随机数、所述物理层密钥和所述匿名密钥计算所述加密密钥，可以表示为：

$Kc = 物理层密钥 \oplus AK \oplus NONCE2$，其中，Kc 表示加密密钥，NONCE2 表示第四随机数，AK 表示匿名密钥，该公式中其他内容的含义与前述实施例相同，不做赘述。再举例来说，采用第二计算方式对所述第四随机数、所述物理层密钥和所述匿名密钥计算所述加密密钥，可以表示为：

$Kc = KDF(物理层密钥, AK, NONCE2)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述。再举例来说，采用第二计算方式基于所述物理层密钥、所述匿名密钥和所述第三随机数计算所述完整性保护密钥，可以表示为：

$Kc = 物理层密钥 \| AK \| NONCE2$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

举例来说，上述第一密钥具体可以为第一中间密钥，则采用第二计算方式对所述第四随机数、所述第一中间密钥和所述匿名密钥计算所述加密密钥，可以表示为：$Kc = Km \oplus AK \oplus NONCE2$，其

中，Kc 表示加密密钥，NONCE2 表示第四随机数，AK 表示匿名密钥，Km 表示第一中间密钥。或者，可以表示为：$Kc = KDF(Km, AK, NONCE2)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述。或者可以表示为：$Kc = Km \| AK \| NONCE2$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

可选地，采用第二计算方式基于所述第一密钥、所述第一随机数和所述第四随机数计算所述加密密钥。也就是可以将上述 Kc 的计算公式中的 AK（匿名密钥）替换为第一随机数 RAND，其他计算公式也可以做相似的替换，这里不做一一赘述。

可选地，采用所述第二计算方式基于第二中间密钥和所述第四随机数计算所述加密密钥，所述第二中间密钥与所述物理层密钥和所述密钥生成参数相关。这里，第二中间密钥的生成方式与前述实施例相同，不做赘述，该第二中间密钥可以表示为 Ka。

所述第二设备采用所述第二计算方式基于第二中间密钥和所述第四随机数计算所述加密密钥，可以采用以下公式表示：$Kc = Ka \oplus NONCE2$，其中，Kc 表示加密密钥，Ka 表示第二中间密钥，NONCE2 表示第四随机数。示例性的，上述计算公式，还可以将异或计算替换为直连计算“||”，或还可以替换为 KDF 等等，这里不做赘述。

可选地，所述第二设备采用第二计算方式基于第三中间密钥和所述第四随机数计算所述加密密钥。

在一种可能的示例中，采用第二计算方式基于第三中间密钥和所述第四随机数计算所述加密密钥，可以表示为：$Kc = Ka' \oplus NONCE2$。其中，Kc 表示加密密钥，NONCE2 表示第四随机数，该公式中其他内容的含义与前述实施例相同，不做赘述。上述公式中的异或计算还可以替换为直连计算或 KDF 计算，这里不做一一赘述。

在又一种可能的示例中，采用第二计算方式基于第三中间密钥和所述第四随机数计算所述加密密钥，可以表示为：$Kc = Kb \oplus NONCE2$。该公式中各个内容的含义与前述实施例相同，不做赘述。上述公式中的异或计算还可以替换为直连计算或 KDF 计算，这里不做一一赘述。以上示例中，Ka’和 Kb 的计算方式以及生成参数与前述实施例相同，因此不做重复说明。

可选地，采用第二计算方式基于所述第一密钥、第三中间密钥和所述第三随机数计算所述加密密钥。这里，第三中间密钥可以是与根密钥相关的。

举例来说，第一网络设备可以是预先与第二设备协商，基于两者互相认证时基于共享的根密钥生成成对主密钥（PMK，Pairwise Master Key）作为共享密钥，将该共享密钥作为上述第三中间密钥。然后第一网络设备可以是通过第一消息将该第三中间密钥发送给第一设备，从而使得第二设备、第一设备共享该第三中间密钥。

举例来说，第一密钥为物理层密钥，采用第二计算方式基于所述第一密钥、第三中间密钥和所述第三随机数计算所述加密密钥，可以表示为：$Ks = 物理层密钥 \oplus PMK \oplus NONCE1$，其中，Ks 表示加密密钥，NONCE1 表示第三随机数，PMK 表示第三中间密钥。再举例来说，可以采用以下公式计算：$Ks = KDF(物理层密钥, PMK, NONCE1)$，其中，KDF（）为密钥派生函数，该公式中其他内容的含义与前述实施例相同，不做赘述。再举例来说，采用以下公式计算：$Ks = 物理层密钥 \| PMK \| NONCE1$，其中，“||”为直连计算，该公式中其他内容的含义与前述实施例相同，不做赘述。

还需要说明，上述生成完整性保护密钥、加密密钥、第一 RES、第二 RES、MAC、第一验证 RES、第二验证 RES、验证 MAC 的处理中，还可以增加第二设备的标识和/或第一设备的标识，比

如，可以在计算 MAC（或验证 MAC）的时候，增加第二设备的 ID、第一设备的 ID；比如，在计算加密密钥（或完整性保护密钥）的时候，采用物理层密钥（或第一中间密钥）、根密钥、随机数以及第二设备的 ID（和/或第一设备的 ID）进行异或计算等等，这里不对全部可能的情况进行穷举。

在一些可能的实施方式中，第二设备和第一设备在通信流程中还会使用各自的完整性保护密钥和/或加密密钥。

可选地，所述第三消息还携带第一完整性验证码。

可选地，所述第三消息还携带第三随机数和/或第四随机数。

可选地，所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息，所述响应消息携带以下至少之一：所述第三消息完整性验证通过的指示信息，第二完整性验证码，所述第四随机数，加密后的组密钥。

可选地，所述第一设备向所述第二设备发送响应消息，所述响应消息响应于所述第三消息，所述响应消息携带以下至少之一：所述第三消息完整性验证通过的指示信息，第二完整性验证码，所述第四随机数，加密后的组密钥。

可选地，所述第二消息还携带以下至少之一：所述第三随机数、第三完整性验证码、加密后的组密钥、所述第四随机数。

关于在上述各个消息中传输用于生成完整性保护密钥和/或加密密钥的随机数、以及得到完整性验证码等处理，具体说明如下。

在一些可能的示例中，所述第一设备向所述第二设备发送第二消息，可以包括：所述第一设备生成第三随机数；所述第一设备基于密钥生成参数和所述第三随机数生成完整性保护密钥；所述第一设备基于所述完整性保护密钥计算得到第三完整性验证码；所述第一设备向所述第二设备发送所述第二消息；所述第二消息携带第三随机数以及所述第三完整性验证码。

第二设备的处理可以包括：所述第二消息还携带第三随机数以及所述第三完整性验证码；所述第二设备基于所述认证参数和根密钥计算验证 MAC，包括：所述第二设备基于密钥生成参数和所述第三随机数生成完整性保护密钥；所述第二设备基于所述完整性保护密钥对所述第三完整性验证码进行验证，得到第二验证结果；所述第二设备在所述第二验证结果指示所述第二消息完整性验证通过的情况下，所述第二设备基于所述认证参数和根密钥计算所述验证 MAC。

也就是说，本示例中，第三随机数由第一设备生成，并在发送第二消息时，第一设备就进行了完整性保护处理。在第二设备侧先基于第二消息携带的第三随机数得到完整性保护密钥，然后对第二消息携带的所述第三完整性验证码进行验证，在第二消息完整性验证通过的时候，第二设备再执行前述计算验证 MAC 等处理。

上述第一设备基于所述完整性保护密钥计算得到所述第三完整性验证码，可以指的是：第一设备基于完整性保护密钥对第二消息的原始内容计算得到所述第三完整性验证码。该第二消息的原始内容可以指的是第二消息原始需要携带的内容，比如第一随机数、第三随机数、认证参数和 MAC 等等。

所述第二设备基于所述完整性保护密钥对所述第三完整性验证码进行验证，得到第三验证结果，可以指的是：第二设备基于所述完整性保护密钥对第二消息的原始内容计算得到第三待验证码，在第三待验证码和所述第三完整性验证码相同的情况下，得到第二验证结果用于指示第二消息完整性验证通过，在第三待验证码和所述第三完整性验证码不同的情况下，得到第二验证结果用于指示第二消息完整性验证不通过（或失败）。

进一步，所述第三消息还携带第一完整性验证码，第二设备在完成上述计算验证 MAC 等处理，

向第一设备发送第三消息时，第二设备可以基于完整性保护密钥对第三消息的原始内容计算得到第一完整性验证码，然后向第一设备发送携带该第一完整性验证码以及原始内容的第三消息。本示例中，上述第三消息的原始内容可以包括前述实施例所示意的内容，这里不做赘述。

相应的，第一设备接收来自第二设备的第三消息后，所述第一设备的处理还可以包括：所述第一设备基于所述完整性保护密钥对所述第一完整性验证码进行验证，得到第三验证结果；所述第一设备在所述第三验证结果指示所述第三消息完整性验证通过的情况下，所述第一设备向所述第二设备发送响应消息，所述响应消息响应于所述第三消息，所述响应消息还用于指示所述第三消息完整性验证通过。

上述第二设备基于完整性保护密钥对第三消息的原始内容计算得到第一完整性验证码，可以指的是：第二设备基于完整性保护密钥对第三消息的原始内容计算得到第一完整性验证码。该第三消息的原始内容可以指的是第二消息原始需要携带的内容，这里不对其进行穷举。

关于本示例中，上述第一设备确定所述第三消息完整性验证通过的同时，可以确定第三消息所携带的内容没有被篡改；同样的，第二设备在确定第二消息完整性验证通过的情况下，可以确定第二消息所携带的第三随机数没有被篡改。

在又一种示例中，所述第三消息携带所述第三随机数，进一步在第二设备侧的处理，可以包括：所述第二设备生成第三随机数；所述第二设备基于密钥生成参数和所述第三随机数生成所述完整性保护密钥。相应的，所述第三消息包括基于第一完整性验证码。

这里，所述第二设备可以是在确定核心网侧设备认证通过的情况下，执行生成第三随机数的处理。进一步，所述第二设备生成所述完整性保护密钥后，基于第三消息的原始消息以及完整性保护密钥计算得到第一完整性验证码，生成携带该原始消息以及第一完整性验证码的第三消息。其中，所述原始消息可以指的是该第三消息所需要携带的信息，比如，本示例中，该原始消息中至少可以携带上述第三随机数，关于该原始消息中可以携带的其他内容与前述实施例相同，不做重复说明。

在第一设备侧接收到第三消息之后的处理，包括：所述第一设备基于密钥生成参数和所述第三随机数生成完整性保护密钥；所述第一设备基于所述完整性保护密钥对所述第一完整性验证码验证，得到第四验证结果；所述第一设备在所述第四验证结果指示所述第三消息完整性验证通过的情况下，所述第一设备向所述第二设备发送响应消息，所述响应消息响应于所述第三消息，所述响应消息用于指示所述第三消息完整性验证通过，所述响应消息携带基于完整性保护密钥计算得到的第二验证码。

这里，所述第一设备基于所述完整性保护密钥对所述第三消息中的所述第一完整性验证码进行验证，得到第四验证结果，可以包括：第一设备基于所述完整性保护密钥对所述第三消息中包含的原始消息计算得到第一待验证码，基于所述第一待验证码和所述第一完整性验证码进行验证，得到第四验证结果。进一步，基于所述第一待验证码和所述第一完整性验证码进行验证，得到第四验证结果，可以包括以下之一：在所述第一待验证码和第一完整性验证码相同的情况下，得到指示所述第三消息完整性验证通过的第四验证结果；在所述第一待验证码和第一完整性验证码不同的情况下，得到指示所述第三消息完整性验证不通过的第四验证结果。所述第一设备基于所述完整性保护密钥对所述第三消息中包含的原始消息计算得到第一待验证码的具体处理，与前述第二设备基于完整性保护密钥对第三消息的原始消息计算得到第一完整性验证码的处理是相似的，不做重复说明。

也就是，由于第一设备和第二设备生成完整性保护密钥所使用的参数和计算方式为相同的，因此，该第一设备所得到的第一待验证码与第一完整性验证码应为相同的，进而第一设备可以确定完整性验证通过（或成功或完成）。

在第二设备侧的处理：所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息，所述响应消息携带指示所述第三消息完整性验证通过的指示信息，第二完整性验证码。进一步，所述第二设备基于所述完整性保护密钥对所述第二完整性验证码进行验证，得到第一验证结果。

这里，所述第二设备基于所述完整性保护密钥对所述第二完整性验证码进行验证，得到第一验证结果可以包括：第二设备基于所述完整性保护密钥对所述响应消息中包含的原始内容计算得到第二待验证码，基于所述第二待验证码和第二完整性验证码进行验证，得到第一验证结果。进一步，基于所述第二待验证码和所述第二完整性验证码进行验证，得到第一验证结果，可以包括以下之一：在所述第二待验证码和所述第二完整性验证码相同的情况下，得到指示所述响应消息完整性验证通过的验证结果；在所述第二待验证码和所述第二完整性验证码不同的情况下，得到指示所述响应消息完整性验证不通过的验证结果。关于上述计算得到第二待验证码的方式，与前述第二设备计算得到第一完整性验证码的方式相似，只是第二设备采用了响应消息中的原始内容计算第二待验证码，这里不做重复说明。响应消息中的原始内容，本实施例不做限定。这种情况下，该第二设备所得到的第二待验证码与第二完整性验证码应为相同的，进而第二设备可以确定完整性验证通过（或成功或完成）。

在一些可能的示例中，上述第三消息还可以直接由第二设备发送至第一网络设备；相应的，第一网络设备生成完整性保护密钥后，基于完整性保护密钥生成自身的待验证码，在自身生成的待验证码与该第三消息携带的第一完整性验证码相同的情况下，确认第三消息完整性验证通过，然后从第三消息中得到第一 RES，在第一 RES 与自身保存的第一验证 RES 相同的情况下，确定对第二设备验证通过。进而，第一网络设备还可以向第二设备发送响应消息，该响应消息响应于第三消息，且该响应消息可以携带基于完整性保护密钥生成的第二完整性验证码。第二设备在生成自身的第二待验证码之后，若第二待验证码与该第二完整性验证码相同，则确定两者之间完整性保护密钥协商完成。

需要指出，本示例中的上述第三消息可以是由第一设备转发给第一网络设备；响应消息可以由第一设备转发给第二设备。只是该第一设备不对第三消息进一步进行处理。关于第一网络设备生成第三完整性保护密钥的方式，与前述生成完整性保护密钥的方式可以相同，不做重复说明。

在一种可能的示例中，所述第二设备和第一设备分别基于各自的完整性保护密钥对接收到的消息进行完整性校验且校验通过的情况下，第二设备和第一设备可以进行加密密钥的协商。

可选地，第二设备可以在发送第三消息时，对该第三消息进行完整性保护，相应的，第一设备在对第三消息完整性验证通过的情况下，生成加密密钥，并将第四随机数携带在响应消息中发送给第二设备；第二设备根据响应消息中携带的第四随机数生成加密密钥。该第三消息可以用于指示第二设备对核心网侧设备完成认证。

所述第一设备执行的处理中，所述第一设备接收到第三消息之后，所述方法还可以包括：所述第一设备生成第四随机数；所述第一设备基于所述第四随机数和密钥生成参数，得到加密密钥；所述第一设备向所述第二设备发送响应消息，所述响应消息携带所述第四随机数。

所述第二设备执行的处理中，所述响应消息还携带第四随机数；所述方法还包括：所述第二设备在所述第一验证结果指示所述响应消息完整性验证通过的情况下，所述第二设备基于所述第四随机数和所述密钥生成参数计算加密密钥。

示例性的，该第一设备生成第四随机数的条件可以包括以下至少之一：第三消息完整性验证通过、所述第二设备认证通过。

比如，前述第三消息不携带第二 RES、第一 RES，则上述第一设备生成第四随机数，可以包括：

所述第一设备在所述第三消息完整性验证通过的情况下，第一设备生成第四随机数。也就是，上述第一设备是在对第三消息完整性校验通过的时候，才会生成加密密钥，本示例中，上述响应消息还可以用于指示所述第三消息完整性校验通过。比如，若第三消息携带第二 RES 和/或第一 RES、且第三消息携带第一验证码，则上述第一设备生成第四随机数，还可以包括：所述第一设备在确定所述第二设备认证通过、且所述第三验证结果指示所述第三消息完整性验证通过的情况下，生成第四随机数。这里，关于确定第二设备认证通过，可以包括第一设备接收到第一网络设备发来的第二设备认证通过的同时，和/或第一设备自身验证第二 RES 与第二验证 RES 相同的情况下确定第二设备认证通过。

可选地，第二设备对第二消息完整性验证通过的情况下，第二设备可以在发送第三消息时，就生成加密密钥，并在第三消息中携带第四随机数。相应的，第一设备在对第三消息完整性验证通过的情况下，根据第三消息中携带的第四随机数生成加密密钥。

这种示例中，第二设备的处理说明如下，所述第三消息携带第四随机数；所述方法还包括：所述第二设备生成第四随机数；所述第二设备基于所述第四随机数、密钥生成参数计算加密密钥。

第一设备侧的处理说明如下，所述第三消息携带第四随机数，所述方法还包括：所述第一设备基于所述第四随机数和密钥生成参数，得到加密密钥。

示例性的，该第二设备生成第四随机数的条件可以包括以下至少之一：第二消息完整性验证通过、对所述核心网侧设备完成认证。该第三消息可以用于指示第二设备对核心网侧设备完成认证，且上述第三消息还可以用于指示第二消息完整性验证通过。

示例性的，该第一设备基于所述第四随机数和密钥生成参数，得到加密密钥的条件可以包括以下至少之一：第三消息完整性验证通过、第一设备在确定所述第二设备认证通过。

比如，前述第三消息不携带第二 RES、第一 RES，则第一设备在所述第三验证结果指示所述第三消息完整性验证通过的情况下，得到加密密钥。比如，若第三消息携带第二 RES 和/或第一 RES、且第三消息携带第一验证码，则第一设备在确定所述第二设备认证通过、且所述第三验证结果指示所述第三消息完整性验证通过的情况下，得到加密密钥。

还应指出的是，在上述第一设备生成加密密钥之后，还可以向第二设备发送响应消息，该响应消息可以携带第三消息完整性验证通过的指示信息，还可以携带对第二设备认证通过的指示信息。

在一些可能的示例中，所述第二设备和第一设备之间不需要进行完整性校验，但第二设备和第一设备可以进行加密密钥的协商，以分别得到加密密钥，该加密密钥用于对第二设备和第一设备之间传输的数据加密。

可选地，所述第一设备执行的处理中，所述第一设备接收到第三消息之后，所述方法还可以包括：所述第一设备生成第四随机数；所述第一设备基于所述第四随机数、密钥生成参数，得到加密密钥；所述第一设备向所述第二设备发送响应消息，所述响应消息携带所述第四随机数。该第三消息可以仅用于指示第二设备对核心网侧设备完成认证。

所述第二设备执行的处理中，所述响应消息还携带第四随机数；所述方法还包括：所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息，所述响应消息携带第四随机数；所述第二设备基于所述第四随机数和密钥生成参数计算加密密钥。

示例性的，前述第三消息不携带第二 RES、第一 RES、且不携带第一验证码，则第一设备可以直接生成第四随机数。示例性的，若第三消息携带第二 RES 和/或第一 RES，则上述第一设备在确定所述第二设备认证通过的情况下，生成第四随机数。这里，关于确定第二设备认证通过说明与前述实施例相同，不做赘述。

可选地，第二设备的处理说明如下，所述第三消息携带第四随机数；所述方法还包括：所述第二设备生成第四随机数；所述第二设备基于所述第四随机数和密钥生成参数计算加密密钥。第一设备侧的处理说明如下，所述第三消息携带第四随机数，所述方法还包括：所述第一设备基于所述第四随机数和密钥生成参数，得到加密密钥。

示例性的，该第二设备生成第四随机数的条件可以包括对所述核心网侧设备完成认证。上述第三消息用于指示第二设备对核心网侧设备完成认证。

示例性的，前述第三消息不携带第二 RES、第一 RES，则第一设备直接计算加密密钥。若第三消息携带第二 RES 和/或第一 RES，则第一设备在确定所述第二设备认证通过的情况下，计算加密密钥。

在上述第一设备生成加密密钥之后，还可以向第二设备发送响应消息，该响应消息可以用于指示对第二设备认证通过。

在一些可能的实施方式中，该第一设备还可以向密钥管理功能实体（或网元）发送一个或多个密钥。

示例性的，上述第一设备可以向密钥管理功能实体发送上述完整性保护密钥和/或加密密钥。该密钥功能管理实体可以保存该完整性保护密钥和/或加密密钥，进而在第一设备和/或第二设备产生移动的情况下，不需要第一设备和/或第二设备或其他设备重新生成各自的完整性保护密钥以及加密密钥，提升系统的处理效率。

示例性的，上述第一设备可以向密钥管理功能实体发送上述第二中间密钥和/或第三中间密钥。该密钥功能管理实体可以保存该第二中间密钥和/或第三中间密钥，进而在第一设备和/或第二设备产生移动的情况下，不需要第一设备和/或第二设备或其他设备重新生成第二中间密钥和/或第三中间密钥，而直接基于第二中间密钥和/或第三中间密钥生成各自的完整性保护密钥以及加密密钥，从而提升系统的处理效率。

上述密钥管理功能实体可以为任意一个或多个网络侧的设备，比如可以是 AMF、接入网设备、SEAF、AUSF 等等，该接入网设备可以是基站、gNB、eNB 等等至少一种，这里不对各种可能的设备进行穷举。上述密钥管理功能实体可以是密钥管理服务(KMS，Key Management Service)实体，或密钥管理功能（KMF，Key Management Function）实体。

在一些可能的实施方式中，以上的认证方法的处理流程，可以是由第二设备触发的。

上述第二设备接收所述第一设备发送的第二消息之前，还可以包括：所述第二设备向所述第一设备发送认证请求，所述认证请求携带所述第二设备的标识。

所述第一设备的处理还可以包括：所述第一设备接收来自所述第二设备的认证请求，所述认证请求携带所述第二设备的标识；所述第一设备向所述第一网络设备转发所述认证请求。

所述第一网络设备的处理还可以包括：所述第一网络设备接收来自所述第一设备的认证请求，所述认证请求携带所述第二设备的标识。

在第一网络设备接收到所述认证请求之后，执行前述得到 MAC 和认证参数的处理，这里不做重复说明。然后第一网络设备向所述第一设备发送所述第一消息。

所述第一设备接收来自第一网络设备的第一消息后，向所述第二设备发送第二消息。

所述第二设备接收来自第一设备的第二消息后，执行前述计算验证 MAC 的处理，以及基于验证 MAC 和 MAC 对网络侧设备进行认证的处理，这里不做重复说明。

所述第二设备对所述核心网侧设备完成认证之后，所述方法还可以包括：所述第二设备向所述第

一设备发送第三消息，所述第三消息用于指示所述第二设备对所述核心网侧设备完成认证。相应的，第一设备的方法还可以包括：所述第一设备接收来自所述第二设备的第三消息，所述第三消息用于指示所述第二设备对所述核心网侧设备完成认证；所述第一设备向所述第一网络设备发送第四消息，所述第四消息用于指示所述第二设备对所述核心网侧设备完成认证。所述第一网络设备的处理方法还可以包括：所述第一网络设备接收来自所述第一设备的第四消息，其中，所述第四消息用于指示所述第二设备对所述核心网侧设备完成认证。

下面结合图 6，对前述实施例所提供的认证方法进行示例性说明。在图 6 中，以第二设备为 A-IoT 设备（图 6 中为了简洁示意为 A-IoT）、第一设备为 UE、第一网络设备为 AUSF、第二网络设备为 UDM 和/或 ARPF 为例，应理解，在图 6 中为了简洁将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF。图 6 的认证方法处理流程包括：

A-IoT 设备（即 A-IoT）和核心网侧设备共享唯一不重复的根密钥 Kr，作为 A-IoT 设备的安全凭证。应理解，这里 A-IoT 仅为一个 A-IoT 设备，在实际处理中，可以有多个 A-IoT 设备，由于每个 A-IoT 设备的处理均为相同的，因此不做一一赘述。

步骤 601，A-IoT 设备向 UE 发送认证请求，携带 A-IoT ID 。

步骤 602，UE 向 AUSF 转发认证请求，携带 A-IoT ID。

步骤 603，AUSF 向 UDM/ARPF 转发认证请求，UDM/ARPF 生成第一随机数 RAND，再根据 Kr 生成匿名密钥 AK、MAC、XRES（即前述第一验证 RES），将 AK、MAC 和 RES 发给 AUSF。

示例性的，合图 7a 来说，上述各个参数的生成架构可以包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND）。其中，f2 也可以由 HMAC-SHA-256，AES，ACSON，SNOW 3G, ZUC 等算法代替。由于 AK 需要发送，所以不能用异或等可以逆向推导的算法生成 MAC 和 XRES。由于 Kr 是仅在每个 A-IoT 设备和核心网共享唯一不重复的密钥，攻击者截获 AK 也不能得到 RAND 或 Kr，因此生成和发送 AK 是安全的，并且具有低功耗的特点。发送 MAC 也是安全的，并且由于 MAC 是基于 Kr 生成的，只有 AUSF 拥有 Kr，因此验证 MAC 可以验证核心网的身份。

示例性的，合图 7b 来说，上述各个参数的生成架构可以包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK，服务参数），XRES = f2（Kr, RAND，服务参数）。其中，f2 也可以由 HMAC-SHA-256，AES，ACSON，SNOW 3G, ZUC 等算法代替。

步骤 604，AUSF 向 UE 发送认证响应，携带 AK、MAC，该认证响应中还可以携带 A-IoT ID。该认证响应即前述实施例中的第一消息。

步骤 605，UE 向 A-IoT 设备转发认证响应，携带 AK、MAC。本步骤中的认证响应消息为前述实施例中的第二消息。

步骤 606，A-IoT 设备收到认证响应消息后，计算 MAC’， 基于 MAC’成功验证 MAC 后，确定成功验证 AUSF 身份，计算 RES。本步骤中的 RES 即前述实施例中的第一 RES。

示例性的，A-IoT 设备的计算方式可以包括：$RAND = Kr \oplus AK$，MAC’=f2（Kr，AK），RES=f2（Kr，RAND）。由于 RES 是基于 Kr 生成的，只有 A-IoT 设备拥有 Kr，因此核心网侧设备通过验证 RES 可以验证 A-IoT 设备的身份。

步骤 607，A-IoT 设备成功验证核心网身份后，计算完整性保护密钥 KI。

示例性的，本步骤的处理，可以包括：A-IoT 设备生成第三随机数即 NONCE1；然后基于公式 $KI = 物理层密钥 \oplus AK \oplus NONCE1$ 计算完整性保护密钥。其中 KI 生成使用的异或 $\oplus$ 算法也可以是直连||，KDF 算法如 HMAC-SHA-256 等，其他可选的 KI 生成参数包括 A-IoT ID 等。该完整性保护

密钥用于对 A-IoT 设备和网络实体的完整性保护。其中，网络实体可以包括但不限于以下至少之一：UE、其他网络设备；其他网络设备可以包括：AP、small cell、gNB、CPE、AMF、UPF、MEC 等。由于物理层密钥是 A-IoT 设备和 UE 之间通过空口的信道信源特征生成的共享密钥，具有香农信息论安全性，因此发送 NONCE1 是安全的，不会泄露 KI，使用 NONCE 1 和物理层密钥生成的 KI 也是安全的。并且，由于物理层密钥是不需要密码学计算，因此具有低功耗的特点。

步骤 608，A-IoT 设备向 UE 发送认证确认，该消息携带 RES，NONCE1（即前述实施例的第三随机数）。A-IoT 设备用 KI 对认证确认消息进行完整性保护后再发送。本步骤中的认证确认消息即前述实施例的第三消息。

步骤 609，UE 收到认证确认消息后，生成 KI' ，UE 用 KI' 对认证确认消息做完整性验证。

该 KI' 可以为 UE 侧的完整性保护密钥，理论上 KI' 与前述 KI 应为相同的，本示例为了区分表示不同设备生成的完整性保护密钥而采用了不同的符号来表示。本示例采用了物理层密钥来生成完整性保护密钥 KI，由于物理层密钥是 A-IoT 设备和 UE 之间通过空口的信道信源特征生成的共享密钥，具有香农信息论安全性，因此只有这个特定 UE 能够验证消息完整性。并且，只有特定的 UE 能够获得物理层密钥，因此即使攻击者获得了 NONCE1 也不能得到 KI，KI 具备安全性。

步骤 610，UE 完成完整性校验后，确认 RES 没有被篡改，向 AUSF 发送认证确认，该认证确认中携带 RES；并且生成第四随机数（NONCE 2），用 NONCE2 生成加密密钥（Kc），该加密密钥用于和 A-IoT 设备之间的消息加密保护。该认证确认可以是前述实施例中的第四消息。示例性的，$Kc = 物理层密钥 \oplus AK \oplus NONCE2$ 。

步骤 611，UE 向 A-IoT 设备发送认证响应，发送之前用 KI' 完整性保护的认证响应，认证响应携带 NONCE2。这里，该认证响应可以为前述实施例中的响应消息，即响应于第三消息的响应消息。由于物理层密钥是 A-IoT 设备和 UE 之间的共享密钥，具有香农信息论安全性，只有特定的 UE 能够获得物理层密钥，因此即使攻击者获得了 NONCE2 也不能得到物理层密钥，使用 NONCE2 和物理层密钥生成的 Kc 也是安全的。另，由于物理层密钥是不需要密码学计算，因此 Kc 生成具有低功耗的特点。

步骤 612，UE 向网络侧 KMS 实体发送 Kc 和 KI' 。

应理解的是，步骤 612 和步骤 611 的处理，可以不分先后顺序。

步骤 613，A-IoT 设备接收认证响应，用 KI 验证完整性，确认 NONCE2 没有被篡改，并且用 NONCE2 生成 Kc。该 Kc 的生成方式与前述示例相同，不做赘述。

另外，在 AUSF 侧还可以执行步骤 614，验证 RES，关于 AUSF 验证 RES 的具体方式与前述实施例相同，不做重复说明。

结合图 8，对密钥的生成架构进行示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，A-IoT 设备和 UE 侧采用相同的方式得到各自的 Kc 和 KI，其中，KI 是采用物理层密钥、AK 再结合第三随机数（即 NONCE1）得到的，Kc 采用物理层密钥、AK 再结合第四随机数得到的。最终 UE 会将 Kc 和 KI 发送给 KMS，从而使得 UE、A-IoT 设备和 KMS 共享相同的 Kc 和 KI。在图 8 中，物理层密钥为可选地，因此表示为虚线框，也就是在一些可能的示例中，KI 是采用 AK 再结合第三随机数（即 NONCE1）得到的，Kc 采用 AK 再结合第四随机数得到的。关于上述生成 KI 和 Kc 的各种可能的示例，与前述实施例相同，不做赘述。在图 8 中，没有区分 KI 和 KI'、且也没有区分不同设备生成的 Kc，原因是 KI 和 KI'理论上应为相同的，且不同设备采用相同方式以及算法得到的 Kc 也应为相同的，因此，在图 8 中不做区分表述。

结合图 8，对密钥的生成架构进行另一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，A-IoT 设备和接入网设备（比如图 8 中的 gNB）采用相同的方式得到各自的 Kc 和 KI，其中，KI 是采用物理层密钥（可选地）、AK 再结合第三随机数（即 NONCE1）得到的，Kc 采用物理层密钥（可选地）、AK 再结合第四随机数得到的。最终接入网设备会将 Kc 和 KI 发送给 KMS，从而使得接入网设备、A-IoT 设备和 KMS 共享相同的 Kc 和 KI。

结合图 8，对密钥的生成架构进行又一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，A-IoT 设备和第一核心网设备（比如前述实施例的各种第一核心网设备中任意之一，这里不做穷举）采用相同的方式得到各自的 Kc 和 KI，其中，KI 是采用物理层密钥（可选地）、AK 再结合第三随机数（即 NONCE1）得到的，Kc 采用物理层密钥（可选地）、AK 再结合第四随机数得到的。最终第一核心网设备会将 Kc 和 KI 发送给 KMS，从而使得第一核心网设备、A-IoT 设备和 KMS 共享相同的 Kc 和 KI。

上述认证方法的处理流程相比与现有技术的 AKA 流程更加简化，A-IoT 设备可以通过异或、f2 等简单的运算得到 RES 和 MAC，从而完成与网络之间的双向认证。另外，密钥协商过程也更加简化，上述认证方法中 A-IoT 设备和 UE（或其他认证代理设备，如 AP, small cell, CPE 等）基于物理层密钥和异或运算得到共享密钥（包括加密密钥和完整性保护密钥），如果需要，由 UE 把会话密钥共享给 KMS，供移动性或生成其他密钥使用。另外，上述示例中，UE 还可以替换为接入网设备，从而对 indirect（间接）和 direct（直接）模式均能够匹配，并且，上述 UE 或者 AUSF 验证 A-IoT 设备均可，比如 AUSF 可以将 XRES 发送给 UE，由 UE 执行 RES 的验证。以上示例，对 A-IoT 设备运算能力和功耗有一定要求，AUSF 可能需要执行简化的 MAC 计算，UE 不需要知道 A-IoT 设备的根密钥 Kr，安全性较强，A-IoT 设备不需要采用较为复杂的计算方式，比如 KDF 生成密钥，UE 可作为认证代理完成认证。

结合图 9，对前述实施例所提供的认证方法进行又一示例性说明。在图 9 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为 UE、第一网络设备为 AUSF、第二网络设备为 UDM 和/或 ARPF 为例，应理解，在图 9 中为了简洁将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF。图 9 的认证方法处理流程包括：

步骤 901~步骤 904 的处理，与前述图 6 示例中的步骤 601~步骤 604 处理相同，不做赘述。

步骤 905，UE 收到认证响应，计算认证密钥 Ka。

示例性的，Ka = f3 (AK,物理层密钥)，Ka 即前述实施例中的第二中间密钥。由于物理层密钥是 A-IoT 设备和 UE 之间通过空口的信道信源特征生成的共享密钥，具有香农信息论安全性，因此 Ka 是安全的。该 UE 收到的认证响应可以是前述实施例的第一消息。

示例性的，$Ka =$ f3 $(AK, NONCE3)$，也就是可以不采用物理层密钥得到 Ka，而是采用第五随机数 NONCE3 来计算认证密钥。

示例性的，$Ka =$ f3 $(AK,$物理层密钥$,$ NONCE3$)$，也就是可以采用 AK、物理层密钥以及第五随机数来计算认证密钥。

步骤 906，UE 向 A-IoT 设备转发认证响应，携带 AK、MAC。该 UE 向 A-IoT 设备发送的认证响应可以是前述实施例的第二消息。

步骤 907，A-IoT 设备收到认证响应后，计算 MAC’， 基于 MAC’成功验证 MAC 后，确定成功验证 AUSF 身份，计算 RES，并计算认证密钥 Ka。

示例性的，$RAND = Kr \oplus AK$，MAC’ = f2（Kr, AK），RES = f2（Kr, RAND），Ka = f3 (AK,物理

层密钥)，其中，MAC'即验证 MAC。因为需要 f3 功能，所以功耗较高。认证密钥 Ka 可以用于分享给其他网络实体（UE，或其他网络设备，如 AP, small cell, gNB, CPE，AMF,UPF,MEC 等）。可以基于 Ka 可以生成 Kc 和 KI，也可生成 A-IoT 设备和其他设备之间的密钥，因此灵活性较大。

步骤 908，A-IoT 设备成功验证 AUSF 身份后，计算 KI。

示例性的，A-IoT 设备生成随机数 NONCE1（即第三随机数），采用公式 $KI = Ka \oplus NONCE1$ 计算得到 KI。其中 KI 生成使用的异或算法也可以是直连||、KDF 算法如 HMAC-SHA-256 等，其他可选的 KI 生成参数还可以包括 A-IoT ID 等。

步骤 909，A-IoT 设备向 UE 发送认证确认，携带 RES，NONCE1。本步骤中，A-IoT 设备用 KI 对认证确认消息进行完整性保护后再发送。该认证确认可以是前述实施例的第三消息。

步骤 910，UE 收到认证确认后，生成 KI 并基于 KI 对认证确认消息进行完整性校验。

本步骤中 $KI = Ka \oplus NONCE1$，在本示例中不对 UE 生成的完整性保护密钥与 A-IoT 设备生成的完整性保护密钥进行区分表示。

步骤 911，UE 完成完整性校验后，确认 RES 没有被篡改，向 AUSF 发送认证确认，该认证确认中携带 RES；并且生成第四随机数（NONCE 2），用 NONCE2 生成加密密钥（Kc），该加密密钥用于和 A-IoT 设备之间的消息加密保护。该认证确认可以是前述实施例中的第四消息。示例性的，Kc = Ka ⊕NONCE2。

步骤 912，UE 向 A-IoT 设备发送认证响应，发送之前用 KI 完整性保护认证响应消息。认证响应消息携带 NONCE2。

步骤 913，UE 向网络侧密钥管理功能 KMF 实体发送 Ka。步骤 912 和步骤 913 的处理，可以不分先后顺序。

步骤 914，A-IoT 设备接收认证响应，用 KI 验证完整性，确认 NONCE2 没有被篡改，并且用 NONCE2 生成 Kc，该 Kc 的生成方式与步骤 911 相同，不做赘述。

另外，在 AUSF 侧还可以执行步骤 915，验证 RES，关于 AUSF 验证 RES 的具体方式与前述实施例相同，不做重复说明。

示例性的，结合图 10 来说，上述各个参数的生成架构可以包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND）。其中，f2 也可以由 HMAC-SHA-256，AES，ACSON，SNOW 3G, ZUC 等算法代替。由于 AK 需要发送，所以不能用异或等可以逆向推导的算法生成 MAC 和 XRES。由于 Kr 是仅在每个 A-IoT 设备和核心网共享唯一不重复的密钥，攻击者截获 AK 也不能得到 RAND 或 Kr，因此生成和发送 AK 是安全的，并且具有低功耗的特点。发送 MAC 也是安全的，并且由于 MAC 是基于 Kr 生成的，只有 AUSF 拥有 Kr，因此验证 MAC 可以验证核心网的身份。进一步，增加了认证密钥 Ka，Ka = f3 (AK,物理层密钥)。

结合图 11，对上述密钥的生成架构进行示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，首先基于 AK 和物理层密钥得到认证密钥 Ka，该 Ka 是 UE 和 A-IoT 设备各自采用相同的方式得到的；该 Ka 可以发送至 KMS，从而使得其他 A-IoT 以及其他网元共享该 Ka，密钥 Ka 可以用于分享给其他网元（UE，或其他网络设备，如 AP, small cell, gNB, CPE，AMF,UPF,MEC 等）。可以基于 Ka 可以生成 Kc 和 KI，也可生成 A-IoT 设备和其他设备之间的密钥，因此灵活性较大。进一步，UE 和 A-IoT 设备各自采用相同的方式计算 Kc 和 KI，其中，Kc 是采用 Ka 再结合第三随机数（即 NONCE1）得到的，Kc 采用 Ka 再结合第四随机数得到的。在图 11 中，物理层密钥为可选地，因此表示为虚线框，也就是在一些可能的示例中，Ka 可以是采用 AK 再结

合第五随机数得到的、而不采用物理层密钥，不做赘述。

结合图 11，对密钥的生成架构进行另一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，首先基于 AK 和物理层密钥（可选地）得到认证密钥 Ka，该 Ka 是 gNB 和 A-IoT 设备各自采用相同的方式得到的；该 Ka 可以发送至 KMS，从而使得其他 A-IoT 以及其他网元共享该 Ka，密钥 Ka 可以用于分享给其他网元（UE，或其他网络设备，如 AP, small cell, gNB, CPE，AMF,UPF,MEC 等）。可以基于 Ka 可以生成 Kc 和 KI，也可生成 A-IoT 设备和其他设备之间的密钥，因此灵活性较大。进一步，gNB 和 A-IoT 设备各自采用相同的方式计算 Kc 和 KI，其中，Kc 是采用 Ka 再结合第三随机数（即 NONCE1）得到的，Kc 采用 Ka 再结合第四随机数得到的。

结合图 11，对密钥的生成架构进行又一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr；在协商 KI 和 Kc 的处理中，首先基于 AK 和物理层密钥（可选地）得到认证密钥 Ka，该 Ka 是第一核心网设备和 A-IoT 设备各自采用相同的方式得到的；该 Ka 可以发送至 KMS，从而使得其他 A-IoT 以及其他网元共享该 Ka，密钥 Ka 可以用于分享给其他网元（UE，或其他网络设备，如 AP, small cell, gNB, CPE，AMF,UPF,MEC 等）。可以基于 Ka 可以生成 Kc 和 KI，也可生成 A-IoT 设备和其他设备之间的密钥，因此灵活性较大。进一步，第一核心网设备和 A-IoT 设备各自采用相同的方式计算 Kc 和 KI，其中，Kc 是采用 Ka 再结合第三随机数（即 NONCE1）得到的，Kc 采用 Ka 再结合第四随机数得到的。

结合图 12，对前述实施例所提供的认证方法进行再一示例性说明。在图 12 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为 UE、第一网络设备为 AUSF、第二网络设备为 UDM 和/或 ARPF 为例，应理解，在图 12 中为了简洁将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF。图 12 的认证方法处理流程包括：

步骤 1201~步骤 1205 的处理，与前述图 6 示例中的步骤 601~步骤 605 处理相同，不做赘述。

步骤 1206，A-IoT 设备收到认证响应消息后，计算 MAC’， 基于 MAC’成功验证 MAC 后，确定成功验证 AUSF 身份，计算 RES（即第一 RES）、以及 RES’（即前述第二 RES）。

示例性的，$RAND = Kr \oplus AK$，MAC’ = f2（Kr, AK），RES = f2（Kr, RAND）。

RES’ 的计算方式可以为以下之一：RES’= f2（物理层密钥，AK），RES’= f2（物理层密钥，RAND），RES’= f2（物理层密钥，RES）。

需要指出的是，图 12 中以第一设备为 UE 为例进行的说明，在实际场景中，图 12 中的 UE 还可以替换为核心网网元（即第一设备可以为第一核心网设备的场景），在第一设备为第一核心网设备的情况下，上述 RES’的计算方式，还可以替换为采用第一中间密钥（Km）来计算，比如，上述 Km 的计算方式如前述实施例，可以包括 Km=KDF（中间网元标识，第二随机数）、或 Km=KDF（AK，中间网元标识，第二随机数），这里不做重复说明；相应的，上述 RES’的计算方式可以替换为以下之一：RES’= f2（Km，RAND）、RES’= f2（Km，RAND），RES’= f2（Km，RES）。

步骤 1207 与前述图 6 的步骤 607 相同，不做赘述。

步骤 1208，A-IoT 设备向 UE 发送认证确认消息，携带 RES，RES’，NONCE1。本步骤中，A-IoT 设备用 KI 对认证确认消息进行完整性保护后再发送。在图 11 中为了简洁，将认证确认消息表示为认证确认。

步骤 1209，UE 收到认证确认消息后，生成 KI'，UE 用 KI' 对认证确认消息做完整性验证。

步骤 1210，UE 对认证确认消息完整性验证通过的情况下，UE 生成 XRES’，验证收到的 RES’和计算的 XRES’是否相同。

其中，XRES'的生成方式可以为以下之一：XRES'= f2（物理层密钥，AK），XRES'= f2（物理层密钥，RAND），XRES'= f2（物理层密钥，RES）。由于 RES'是基于物理层密钥生成的，只有 A-IoT 设备拥有物理层密钥，因此验证 RES'可以验证 A-IoT 设备的身份。

在收到的 RES'和计算的 XRES'相同的情况下，执行后续步骤 1211~步骤 1215，该步骤 1211~步骤 1215 的具体说明与前述示例图 6 中的步骤 610~步骤 614 相同，不做重复说明。

需要指出，上述图 6、图 9、图 12 分别对 Indirect mode 下第一设备为 UE 的场景进行的示例性说明。在一些可能的示例中，在 Direct mode 下，上述图 6、图 9、图 12 中的 UE 还可以替换为接入网设备，比如 gNB，或者，上述图 6、图 9、图 12 中的 UE 还可以替换为第一核心网设备，比如 AMF、SEAF、专用于 AIoT（或 IoT）的核心网网元等等任意之一，这里不对全部可能的示例进行穷举。

示例性的，结合图 13 来说，与图 12 所示例的认证方法处理流程中的上述各个参数的生成架构进行说明，可以包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND），XRES'= f2（物理层密钥，AK），或者 XRES'也可以基于 XRES 得到。其中，f2 也可以由 HMAC-SHA-256，AES，ACSON，SNOW 3G, ZUC 等算法代替。图 13 所提供的示例使用 XRES'（可替换理解为前述 RES'），增加 A-IoT 设备和 UE 之间的认证，由于 UE 没有 Kr，只有 AK 和 RES，因此 RES'（或 XRES'）的生成不能基于 Kr，而是基于 AK 和/或 RES。

结合图 14，对前述实施例所提供的认证方法进行再一示例性说明。在图 14 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为基站（该第一设备可以为基站也可以为 UE）、第一网络设备为 AUSF、第二网络设备为 UDM 和/或 ARPF 为例，应理解，在图 14 中为了简洁将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF。图 14 的认证方法处理流程包括：

步骤 1401~步骤 1402 与前述示例图 6 中的步骤 601~步骤 602 相同，不做赘述。

步骤 1403，AUSF 向 UDM/ARPF 转发认证请求，UDM/ARPF 生成第一随机数 RAND，再根据 Kr 生成匿名密钥 AK、MAC、XRES（即前述第一验证 RES）、Ka'，将 AK、MAC、XRES、Ka'发给 AUSF。

本示例采用前述实施例的第三中间密钥为例，将该第三中间密钥表示为 Ka'。示例性的，$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND）；本示例采用前述实施例的第三中间密钥为例，将该第三中间密钥表示为 Ka'。示例性的，$Ka' =$ f3 $(Kr, RAND, \text{物理层密钥})$。

另外，上述第三中间密钥，也可以不采用物理层密钥计算，比如 $Ka' =$ f3 $(Kr, RAND)$；又比如，上述第三中间密钥也可以将物理层密钥替换为第一中间密钥计算，比如 $Ka' =$ f3 $(Kr, RAND, Km)$。关于第三中间密钥的各种示例性计算方式在前述实施例已经详述，这里不做赘述。

步骤 1404，AUSF 向基站发送认证响应，携带 MAC，AK，Ka'。该认证响应可以是前面实施例中的第二消息。

步骤 1405，基站向 A-IoT 设备发送认证响应，携带 MAC，AK，不携带 Ka'。

步骤 1406，A-IoT 设备计算 MAC'，基于 MAC'成功验证 MAC 后，确定成功验证 AUSF 身份，计算 Ka'并计算完整性保护密钥 KI。另外，本步骤中 A-IoT 设备还可以生成 RES（即前述第一 RES）。

该密钥 Ka'或 KI 用于对 A-IoT 设备和网络实体（UE，或其他网络设备，如 AP, small cell, gNB, CPE，AMF,UPF,MEC 等）共享。

示例性的，A-IoT 设备执行的计算可以包括以下至少之一：$RAND = Kr \oplus AK$，MAC'=f2

（Kr，AK），RES=f2（Kr，RAND），$Ka' = \text{f3}\ (Kr, RAND, \text{物理层密钥})$。

进一步，A-IoT 设备生成随机数 NONCE1（即前述第三随机数），生成 Ka'后生成 KI 的方式可以为 $KI = Ka' \oplus NONCE1$。

示例性的，上述步骤 1403 中可以计算的为前述第四中间密钥 Ka''，即 $Ka'' = Kr \oplus RAND$。进一步地，基站以及 A-IoT 均可以采用以下公式基于第四中间密钥生成 Kb，$Kb = f2(\text{物理层密钥}, Ka'')$；基站以及 A-IoT 均可以基于 Kb 生成 KI，比如表示为 $KI = Kb \oplus NONCE1$。

上述示例中，Ka'、Ka''生成可替换的使用的异或⊕算法、直连算法||、KDF 算法如 HMAC-SHA-256、f3（）等，另外，其他可选的 Ka'生成参数包括 A-IoT ID，NONCE 等。

步骤 1407，A-IoT 设备向基站发送认证确认消息，该消息携带 RES。A-IoT 设备可以用 KI 对认证确认消息进行完整性保护后再发送。

步骤 1408，基站收到认证确认消息后，生成 KI 并用 KI 对认证确认消息进行完整性校验，向 AUSF 发送认证确认，该认证确认中携带 RES。在本步骤中，基站还可以生成 Kc，比如采用前述 Ka'生成 Kc，具体处理方式与前述实施例相同，步骤赘述。

步骤 1409，AUSF 验证 RES 通过后，对 A-IoT 设备完成验证。

示例性的，上述步骤 1407 中，AIOT 设备可以将认证确认消息直接发送至 AUSF，由 AUSF 根据前述 Ka'生成 KI，进而基于 KI 完整性校验通过之后，确认 RES 没有被篡改，对认证确认消息中的 RES 进行验证，通过后可以确定对 A-IoT 设备完成验证。

示例性的，AUSF 可以将 Ka'共享给服务器或者 KMS，KMS 和服务器可基于 Ka'进一步生成其他密钥。

示例性的，步骤 1404 中，基站收到 AUSF 的认证响应后生成 KI，在步骤 1405 中，基站基于 KI 对转发给 A-IoT 设备的认证响应消息进行完整性保护。在步骤 1406 中，A-IoT 设备收到认证响应消息后也生成 KI，对认证响应消息进行完整性校验，从而完成 KI 协商，并完整性保护认证响应消息。在步骤 1406 中，A-IoT 设备可以生成 Kc，执行步骤 1407 时在发送认证确认消息前，对消息进行完保和加密，并在认证确认消息中携带第四随机数。步骤 1408 中，基站收到认证确认消息后，根据第四随机数生成 Kc 对认证确认消息进行解密并基于 KI 进行完整性校验从而完成密钥协商。

图 14 的示例中，和之前的实施例不同，第三中间密钥 Ka'由网络侧生成发给基站或 UE，再由基站或 UE 使用物理层密钥生成 KI 和 Kc。AUSF 可以将 Ka 共享给服务器或者 KMS，KMS 和服务器可基于 Ka 进一步生成其他密钥。

需要指出，上述图 14 对 Direct mode 下第一设备为基站的场景进行的示例性说明。在一些可能的示例中，在 Direct mode 下，上述图 14 中的基站还可以替换为第一核心网设备，比如 AMF、SEAF、专用于 AIoT（或 IoT）的核心网网元等等任意之一。在一些可能的示例中，在 Indirect mode 下，上述图 14 中的基站还可以替换为 UE，这里不对全部可能的示例进行穷举。

示例性的，合图 15 来说，与图 14 所示例的认证方法处理流程中的上述各个参数的生成架构进行说明，可以包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND），$Ka' = \text{f3}\ (Kr, RAND, \text{物理层密钥})$。

结合图 16，对上述各个密钥的生成架构进行示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr，并可以基于根密钥得到 AK；在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧，均可以根据

Kr 和物理层密钥生成 Ka（即前述示例中的 Ka'）。A-IoT 设备侧与基站侧在协商 KI 和 Kc 的处理中，A-IoT 设备和基站采用相同的方式基于 Ka 得到各自的 Kc 和 KI。另外，基站会将 Ka 发送给 KMS，从而使得基站、A-IoT 设备、KMS 和其他网元（与前述示例相同不做赘述）共享相同的 Ka。在图 16 中，物理层密钥为可选地，因此表示为虚线框，也就是在一些可能的示例中，Ka 可以不采用物理层密钥进行计算，关于其各种计算方式与前述实施例相同，不做赘述。结合图 16，对上述各个密钥的生成架构进行又一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr，并可以基于根密钥得到 AK；在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧，均可以根据 Kr 和物理层密钥（可选地）生成 Ka（即前述示例中的 Ka'）。A-IoT 设备侧与 UE 在协商 KI 和 Kc 的处理中，A-IoT 设备和 UE 侧采用相同的方式基于 Ka 得到各自的 Kc 和 KI。另外，UE 会将 Ka 发送给 KMS，从而使得 UE、A-IoT 设备、KMS 和其他网元（与前述示例相同不做赘述）共享相同的 Ka。结合图 16，对上述各个密钥的生成架构进行又一示例性说明，在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧共享根密钥 Kr，并可以基于根密钥得到 AK；在 A-IoT 设备侧与 AUSF/UDM/ARPF 侧，均可以根据 Kr 和物理层密钥（可选地）生成 Ka（即前述示例中的 Ka'）。A-IoT 设备侧与第一核心网设备在协商 KI 和 Kc 的处理中，A-IoT 设备和第一核心网设备侧采用相同的方式基于 Ka 得到各自的 Kc 和 KI。另外，第一核心网设备会将 Ka 发送给 KMS，从而使得第一核心网设备、A-IoT 设备、KMS 和其他网元（与前述示例相同不做赘述）共享相同的 Ka。

结合图 17，对前述实施例所提供的认证方法进行再一示例性说明。在图 17 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为认证设备（Authenticator）、第一网络设备为 AS 为例，处理流程包括：

A-IoT 设备（即 A-IoT）和 AS 共享唯一不重复的根密钥 Kr，比如可以是 AS 和 A-IoT 互相认证后生成成对主密钥（PMK，Pairwise Master Key）。AS 在认证响应消息中将 PMK 发送给 Authenticator，A-IoT 和 Authenticator 共享 PMK（在前述实施例中将 PMK 称为第三中间密钥）。

步骤 1701，A-IoT 设备向认证设备（Authenticator）发送认证请求，携带 A-IoT ID 。

步骤 1702，认证设备（Authenticator）向 AS 转发认证请求，携带 A-IoT ID。

步骤 1703，AS 生成第一随机数 RAND，再根据 Kr 生成匿名密钥 AK、MAC、XRES（即前述第一验证 RES）。

示例性的，合图 17 来说，上述各个参数的生成方式包括：$AK = Kr \oplus RAND$，MAC = f2（Kr, AK），XRES = f2（Kr, RAND）。其中，f2 也可以由 HMAC-SHA-256，AES，ACSON，SNOW 3G, ZUC 等算法代替。

步骤 1704，AS 向 Authenticator 发送认证响应，携带 AK、MAC、PMK，该认证响应中还可以携带 A-IoT ID。该认证响应即前述实施例中的第一消息。

步骤 1705，Authenticator 向 A-IoT 设备转发认证响应，携带 AK、MAC。本步骤中的认证响应消息为前述实施例中的第二消息。

步骤 1706，A-IoT 设备收到认证响应消息后，计算 MAC'， 基于 MAC'成功验证 MAC 后，确定成功验证 AS 身份，计算 RES。本步骤中的 RES 即前述实施例中的第一 RES。

示例性的，AIOT 设备的计算可以包括：$RAND = Kr \oplus AK$，MAC'=f2（Kr，AK），RES=f2（Kr，RAND）。

步骤 1707，A-IoT 设备计算加密密钥 Ks。

示例性的，本步骤的处理，可以包括：A-IoT 设备生成第三随机数即 NONCE1；然后基于公式

Ks = 物理层密钥 $\oplus$ PMK $\oplus$ $NONCE1$ 计算完整性保护密钥。其中 Ks 生成使用的异或 $\oplus$ 算法也可以是直连||，KDF 算法如 HMAC-SHA-256 等，其他可选的 Ks 生成参数包括 A-IoT ID 等。

步骤 1708，A-IoT 设备向 Authenticator 发送认证确认，该消息携带 RES，NONCE1（即前述实施例的第三随机数）。本步骤中的认证确认消息即前述实施例的第三消息。

步骤 1709，Authenticator 收到认证确认消息后，生成 Ks 作为加密密钥。

步骤 1710，Authenticator 向 AS 发送认证确认，该认证确认中携带 RES。

步骤 1711，Authenticator 向 A-IoT 设备发送认证响应，该认证响应可以为前述实施例中的响应消息，即响应于第三消息的响应消息。

另外，在 AS 侧还可以执行步骤 1712，验证 RES，关于 AS 验证 RES 的具体方式与前述实施例相同，不做重复说明。

结合图 18，对上述图 17 中各个密钥的生成架构进行示例性说明，在 A-IoT 设备侧与 AS 侧共享根密钥 Kr；基于该 Kr 可以得到 AK。在协商 Ks 的处理中，A-IoT 设备和认证设备侧采用相同的方式结合物理层密钥以及 PMK 得到各自的 Ks。在图 18 中，物理层密钥为可选地，因此表示为虚线框，也就是在一些可能的示例中，Ks 可以不采用物理层密钥计算，不做赘述。

在一些可能的实施方式中，本实施例提供的认证方法还可以是由第一设备、或网络侧触发执行的。

可选地，可以由服务器触发认证处理。

该第一网络设备的处理，可以包括：所述第一网络设备接收来自服务器的触发消息，所述触发消息携带所述第二设备的标识和/或所述第二设备所在的设备组的标识。

上述服务器可以是具备 AIoT 服务功能的服务器，比如可以是 AF、或其他服务器、或称为 A-IoT 网元，这里不对其进行限定。

上述第一网络设备接收来自服务器的触发消息之后，可以执行前述实施例中发送第一消息的处理。

可选地，上述触发消息仅携带一个第二设备的标识，相应的，前述第一消息仅携带第二设备的标识，该第一消息也可以称为认证请求（或认证请求消息）。后续第二设备和第一设备可以执行与前述实施例中交互第二消息、第三消息等处理，这里不做重复说明。

可选地，上述触发消息携带第二设备所在的设备组标识。也就是该触发消息可以携带一个组 ID。这种情况下，前述第一消息携带前述第二设备所在的设备组的标识。本情况下，该第一消息也可以称为认证请求（或认证请求消息）。

进一步，所述第一消息还携带所述第二设备所在的设备组的标识，所述第二消息用于请求认证；上述第一设备接收到第一消息后，所述第一设备向所述第二设备发送第二消息。该第一设备向所述第二设备发送第二消息，可以包括：所述第一设备生成第四随机数；所述第一设备基于所述第四随机数、所述物理层密钥和密钥生成参数，得到加密密钥；所述第一设备基于所述加密密钥对组密钥加密，得到加密后的组密钥；所述第一设备向所述第二设备发送第二消息，所述第二消息还携带加密后的组密钥、第四随机数。

上述加密密钥的生成方式，与前述实施例相同，不做重复说明。

可选地，第一设备还可以生成上述组密钥，该组密钥的生成方式，可以包括以下之一：所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的第一密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的第一密钥、每个设备的标识、所述第三随机数计算所述组密钥。

上述第三计算方式与前述实施例相同，不做重复说明。在以下的示例中采用第三计算方式为 KDF 为例进行说明，不对第三计算方式可以包含的其他方式计算组密钥的处理进行穷举。上述第三随机数可以是第一设备生成的，不对其生成方式进行限定。

示例性的，上述每个设备的中间密钥，可以是每个设备的第二中间密钥、或每个设备的第三中间密钥、或每个设备的第四中间密钥，关于每个设备的第二中间密钥、第三中间密钥以及第四中间密钥的计算方式，均与前述第二中间密钥、第三中间密钥以及第四中间密钥的计算方式是相同的，因此本实施例中不做重复说明。

示例性的，上述每个设备的中间密钥也可以是每个设备的第四中间密钥，也就是采用与前述实施例不同的方式得到的中间密钥，该第四中间密钥可以采用第三计算方式基于密钥生成参数和设备的标识计算得到，且该密钥生成参数包括匿名密钥以及第一随机数，举例来说，上述任意一个设备的第四中间密钥可以采用以下公式计算：Ka=f3（AK, RAND，A-IOT ID），其中，A-IoT ID 即设备的标识。应理解，以上仅为示例性说明，这里不对每个设备的中间密钥的生成方式进行穷举。

可选地，以各个设备的第一密钥为各个设备的物理层密钥为例，所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的物理层密钥、所述每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$K-Group=KDF(AK_{A-IoT-1}\ominus\ldots\ominus AK_{A-IoT-i},\ \|PK_{A-IoT-1}\ominus\ldots\ominus \mathbf{PK}_{A-IoT-i},\ (A-IoTID-1,\ldots,A-IoTID-\mathbf{i}),UEID/\text{基站}ID,NONCE1)$$

；

其中，K-Group 表示组密钥，KDF（）表示 KDF 计算函数，$AK_{A-IoT-1}\sim AK_{A-IoT-i}$ 表示每个设备的匿名密钥，对上述每个设备的匿名密钥进行异或计算，其中 i 表示设备组中的第 i 个设备，i 为正整数，“||”表示直连计算，$PK_{A-IoT-1}\sim \mathbf{PK}_{A-IoT-i}$ 表示每个设备的物理层密钥，对上述每个设备的物理层密钥进行异或计算，$(A-IoTID-1,\ldots,A-IoTID-\mathbf{i})$ 表示每个设备的标识、UEID 为第一设备为 UE 的情况下该 UE 的标识，基站 ID 为第一设备为基站的情况下该基站的标识（在一些可能的示例中，还可以将该基站 ID 表示为基站 IE），NONCE1 表示第三随机数。可选地，上述公式中，异或计算可以替换为直连计算、直连计算也可以替换为异或计算；可选地，$(A-IoTID-1,\ldots,A-IoTID-\mathbf{i})$ 可以替换为对每个设备的标识采用异或计算或直连计算，以上各种可能的计算方式均在本实施例保护

范围内，不做穷举。

可选地，以各个设备的第一密钥为各个设备的第一中间密钥为例，所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一中间密钥、所述每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$K-Group=KDF(AK_{A-IoT-1}\oplus\ldots\oplus AK_{A-IoT-i},\ \|Km_{A-IoT-1}\oplus\ldots\oplus Km_{A-IoT-i},(A-IoTID-1,\ldots,A-IoTID-i),UEID/\text{基站}ID,NONCE1)$$

；

其中，$Km_{A-IoT-1}\sim Km_{A-IoT-i}$表示每个设备的第一中间密钥，其余参数内容含义与前述示例相同，不做穷举。

可选地，采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的标识、所述第三随机数计算所述组密钥，也就是不采用第一密钥进行组密钥的计算，可以采用以下公式表示：

$$K-Group=KDF(AK_{A-IoT-1}\oplus\ldots\oplus AK_{A-IoT-i},(A-IoTID-1,\ldots,A-IoTID-i),UEID/\text{基站}ID,NONCE1)$$

，公式中各个参数的含义与前述示例相同，不做赘述。

可选地，所述第一设备采用所述第三计算方式基于所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group=KDF}(\mathbf{AK_{A-IoT-1}}\oplus\ldots\oplus\mathbf{AK_{A-IoT-i}},\ \|\ \mathbf{Ka_{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka_{A-IoT-i}},(\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站}\mathbf{ID},\mathbf{nonce1})$$

；

其中，K-Group 表示组密钥，KDF（）表示 KDF 计算函数，$AK_{A-IoT-1}\sim AK_{A-IoT-i}$表示每个设备的匿名密钥，对上述每个设备的匿名密钥进行异或计算，其中 i 表示设备组中的第 i 个设备，i 为正整数，“‖”表示直连计算，$\mathbf{Ka_{A-IoT-1}}\sim\mathbf{Ka_{A-IoT-i}}$表示每个设备的中间密钥，对上述每个设备的中间密钥进行异或计算，公式中其他内容的含义与前述实施例相同，不做重复说明。

可选地，以各个设备的第一密钥为各个设备的物理层密钥为例，所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的物理层密钥、每个设备的标识和所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group=KDF}(\mathbf{Ka_{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka_{A-IoT-i}},\ \|\mathbf{PK_{A-IoT-1}}\oplus\ldots\oplus\mathbf{PK_{A-IoT-1}},(\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站}\mathbf{ID},\mathbf{nonce1})$$

；

其中，K-Group 表示组密钥，KDF（）表示 KDF 计算函数，$PK_{A-IoT-1}\sim\mathbf{PK}_{A-IoT-i}$表示每个设备的物理层密钥，对上述每个设备的物理层密钥进行异或计算，其中 i 表示设备组中的第 i 个设备，i 为正整数，“‖”表示直连计算，$\mathbf{Ka_{A-IoT-1}}\sim\mathbf{Ka_{A-IoT-i}}$表示每个设备的中间密钥，对上述每个设备的中间密钥进行异或计算，公式中其他内容的含义与前述实施例相同，不做重复说明。

可选地，以各个设备的第一密钥为各个设备的第一中间密钥为例，所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的第一中间密钥、每个设备的标识和所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group=KDF}(\mathbf{Ka_{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka_{A-IoT-i}},\ \|Km_{\mathbf{A-IoT-1}}\oplus\ldots\oplus Km_{\mathbf{A-IoT-1}},(\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站}\mathbf{ID},\mathbf{nonce1})$$

；

其中，公式各个内容的含义与前述实施例相同，不做重复说明。

可选地，以各个设备的第一密钥为各个设备的物理层密钥为例，所述第一设备采用所述第三计算

方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的物理层密钥、每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group=KDF}\left(\mathbf{AK}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{AK}_{\mathbf{A-IoT-i}},\|\mathbf{Ka}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka}_{\mathbf{A-IoT-i}},\ \|\mathbf{PK}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{PK}_{\mathbf{A-IoT-1}},\right.$$
$$\left.(\mathbf{A-IoT\ ID-1},\ldots,\ \mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站ID},\ \mathbf{nonce1}\right)$$

，公式中各个内容的含义与前述实施例相同，不做重复说明。

上述公式中，异或计算可以替换为直连计算、直连计算也可以替换为异或计算；可选地，$(A-IoTID-1,\ldots,\ A-IoTID-\mathbf{i})$可以替换为对每个设备的标识采用异或计算或直连计算，以上各种可能的计算方式均在本实施例保护范围内，不做穷举。

可选地，以各个设备的第一密钥为各个设备的第一中间密钥为例，所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的第一中间密钥、每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group=KDF}\left(\mathbf{AK}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{AK}_{\mathbf{A-IoT-i}},\|\mathbf{Ka}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka}_{\mathbf{A-IoT-i}},\ \|Km_{\mathbf{A-IoT-1}}\oplus\ldots\oplus Km_{\mathbf{A-IoT-1}},\right.$$
$$\left.(\mathbf{A-IoT\ ID-1},\ldots,\ \mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站ID},\ \mathbf{nonce1}\right)$$

，公式中各个内容的含义与前述实施例相同，不做重复说明。

可选地，第一设备计算该组密钥的方式，可以包括以下之一：所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的物理层密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的第一密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的第一密钥、每个设备的标识、所述第三随机数计算所述组密钥。

本示例主要是在前述各个生成组密钥的计算中增加了设备组的密钥，以下仅以部分公式的变形为例进行示例性说明，不再对上述各个上述进行一一穷举：

可选地，以第一密钥为物理层密钥为例，所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的物理层密钥、所述每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group}=\mathbf{KDF}(\text{匿名密钥}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\text{匿名密钥}_{\mathbf{A-IoT-i}},\ \|\mathbf{PK}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{PK}_{\mathbf{A-IoT-1}},\ (\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站ID},\mathbf{Group\ ID},\mathbf{nonce1});$$

其中，K-Group 表示组密钥，KDF（）表示 KDF 计算函数，$\text{匿名密钥}_{A-IoT-1}\sim\text{匿名密钥}_{A-IoT-i}$ 表示每个设备的匿名密钥，对上述每个设备的匿名密钥进行异或计算，其中 i 表示设备组中的第 i 个设备，i 为正整数，“||”表示直连计算，$PK_{A-IoT-1}\sim\mathbf{PK}_{A-IoT-i}$ 表示每个设备的物理层密钥，对上述每个设备的物理层密钥进行异或计算，$(A-IoTID-1,\ldots,A-IoTID-\mathbf{i})$ 表示每个设备的标识、UEID 为第一设备为 UE 的情况下该 UE 的标识，基站 ID 为第一设备为基站的情况下该基站的标识（在一些可能的示例中，还可以将该基站 ID 表示为基站 IE），Group ID 为设备组的标识，NONCE1 表示第三随机数。可选地，上述公式中，异或计算可以替换为直连计算、直连计算也可以替换为异或计算；可选地，$(A-IoTID-1,\ldots,A-IoTID-\mathbf{i})$ 可以替换为对每个设备的标识采用异或计算或直连计算，以上各种可能的计算方式均在本实施例保护范围内，不做穷举。

可选地，以第一密钥为第一中间密钥为例，所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一中间密钥、所述每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group}=\mathbf{KDF}(\text{匿名密钥}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\text{匿名密钥}_{\mathbf{A-IoT-i}},\ \|Km_{\mathbf{A-IoT-1}}\oplus\ldots\oplus Km_{\mathbf{A-IoT-1}},\ (\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站ID},\mathbf{Group\ ID},\mathbf{nonce1});$$

其中，公式中各个内容的含义与前述实施例相同，不再赘述。

可选地，所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥，可以采用以下公式计算：

$$\mathbf{K-Group}=\mathbf{KDF}(\text{匿名密钥}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\text{匿名密钥}_{\mathbf{A-IoT-i}},\ \|\ \mathbf{Ka}_{\mathbf{A-IoT-1}}\oplus\ldots\oplus\mathbf{Ka}_{\mathbf{A-IoT-i}},\ (\mathbf{A-IoT\ ID-1},\ldots,\mathbf{A-IoT\ ID-i}),\mathbf{UE\ ID}/\text{基站IE},\mathbf{Group\ ID},\mathbf{nonce1});$$

其中，K-Group 表示组密钥，KDF（）表示 KDF 计算函数，$\text{匿名密钥}_{A-IoT-1}\sim\text{匿名密钥}_{A-IoT-i}$ 表示每个设备的匿名密钥，对上述每个设备的匿名密钥进行异或计算，其中 i 表示设备组中的第 i 个设备，i 为正整数，“||”表示直连计算，$\mathbf{Ka}_{\mathbf{A-IoT-1}}\sim\mathbf{Ka}_{\mathbf{A-IoT-i}}$ 表示每个设备的中间密钥，对上述每个设备的中间密钥进行异或计算，公式中其他内容的含义与前述实施例相同，不做重复说明。

所述第二设备的处理说明如下，所述第二设备基于所述加密密钥对加密后的组密钥进行解密，得到所述组密钥，所述组密钥用于对所述第二设备与所述第一设备之间传输的数据加密。

进一步，所述第二消息用于请求认证，所述第二消息还携带加密后的组密钥、第四随机数；所述第二设备向所述第一设备发送第三消息，包括：所述第二设备基于所述第四随机数和密钥生成参数，得到加密密钥；所述第二设备基于所述加密密钥对所述加密后的组密钥进行解密，得到所述组密钥；所述第二设备向所述第一设备发送第三消息，所述第三消息为基于所述组密钥加密后的消息。

需要指出，前述第二设备接收到第二消息之后，仍然会执行前述计算验证 MAC 等处理，具体的

处理方式与前述实施例也是相同的。

可选地，该第二设备也可以进一步生成完整性保护密钥，对第三消息进行完整性保护处理，其处理方式也与前述实施例相同，这里不做重复说明。需要指出，本实施例中，生成完整性保护密钥也可以使用前述第四中间密钥，进而采用第二计算方式基于第二中间密钥、第三随机数和物理层密钥计算完整性保护密钥。在第一设备侧也会采用相同的处理方式生成完整性保护密钥，这里不做重复说明。

可选地，第一设备可以将上述每个设备的中间密钥以及组密钥发送至密钥管理功能实体，以使得密钥管理功能实体进行移动性管理使用。

结合图 19，对前述实施例所提供的认证方法进行一示例性说明。在图 19 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为 UE/基站、将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF 为例。图 19 的认证方法处理流程包括：

步骤 1901，服务器发送触发消息，该触发消息可以携带 AIoT ID 和/或 Group（组）ID。

步骤 1902，AUSF 收到触发消息后，向 UDM/ARPF 请求认证向量，UDM/ARPF 生成认证向量，UDM/ARPF 向 AUSF 发送认证向量，该认证向量可以包括 MAC、AK、XRES。

步骤 1903，AUSF 向 UE/基站发送认证请求，携带 MAC，AK，A-IoT ID，Group ID。

步骤 1904，UE/基站生成设备组中每个设备的 Ka 进而生成组密钥（K-Group）。

上述 Ka 可以指的是前述实施例中的每个设备的中间密钥，关于该中间密钥的详细说明与前述实施例相同，并且组密钥的生成也与前述实施例相同，均不再重复说明。

可选地，UE/基站向 KMS 发各个设备的 Ka 以及组密钥。

步骤 1905，UE/基站发送认证请求（可以携带 AK，MAC，加密后的 K-Group)。

步骤 1906，A-IoT 设备收到认证响应后，计算 MAC’， 基于 MAC’成功验证 MAC 后，确定成功验证 AUSF 身份，计算 RES，并计算 Ka 以及 KI。示例性的，$RAND = Kr \oplus AK$，MAC’ = f2（Kr, AK），RES = f2（Kr, RAND），Ka=f3（AK, RAND，A-IOT ID），$KI = KDF(Ka, NONCE1$，物理层密钥$)$，其中，MAC’即验证 MAC，Ka 为前述设备的中间密钥，KI 为 AIOT 设备生成的完整性保护密钥。

上述步骤 1905 中，认证请求还可以携带第四随机数，步骤 1906 中，A-IoT 设备还可以基于所述第四随机数、所述物理层密钥和密钥生成参数，得到加密密钥；所述第二设备基于所述加密密钥对所述加密后的组密钥进行解密，得到所述组密钥。

步骤 1907，A-IoT 设备发送认证响应(携带 RES)，该认证响应可以用 KI 完保。

本步骤中，认证响应还可以为基于所述组密钥加密后的消息。

步骤 1908，UE/基站生成 KI 后对认证响应验证完保，成功后向 AUSF 发送认证确认，该认证确认携带 RES。上述 UE/基站生成的 KI 可以称为完整性保护密钥，关于该 UE/基站生成 KI 的方式与前述 AIOT 设备相同，不做重复说明。本步骤中，若认证响应还为基于所述组密钥加密后的消息，则 UE/基站还可以使用组密钥对该认证响应解密之后，执行验证完保等处理，不做重复说明。

另外，在 AUSF 侧还可以执行步骤 1909，验证 RES，关于 AUSF 验证 RES 的具体方式与前述实施例相同，不做重复说明。

可选地，可以由第一设备触发认证处理。

所述第一设备的处理可以包括：所述第一设备向所述第一网络设备发送认证请求，所述认证请求携带所述第二设备的标识和/或所述第二设备所在的设备组的标识。相应的，所述第一网络设备的处理可以包括：所述第一网络设备接收来自所述第一设备的认证请求，所述认证请求携带所述第二设备的

标识和/或所述第二设备所在的设备组的标识。

进一步，第一网络设备获取到认证请求后，可以执行前述实施例中发送第一消息的处理。与前述实施例不同在于，本实施例中，该第一消息还可以携带第二设备所在的设备组的标识。另外，前述第一设备在向第一网络设备发送认证请求之前，还可以向第二设备（或第二设备所在的设备组中的每个设备）发送触发消息，该触发消息中可以携带该第二设备的标识和/或第二设备所在的设备组的标识。

这种情况下，前述第一设备接收到第一消息之后，向第二设备发送用于请求认证的第二消息。关于第二设备基于第二消息的处理与前述各个实施例均可以相同，并且第二设备向第一设备发送第三消息的处理也可以是相同的，不做赘述。

所述第一设备接收到第三消息之后的处理，还可以包括：所述第一设备生成第四随机数；所述第一设备基于所述第四随机数、所述物理层密钥和密钥生成参数，得到加密密钥；所述第一设备基于所述加密密钥对组密钥进行加密，得到加密后的组密钥；所述第一设备向所述第二设备发送响应消息，所述响应消息响应于所述第三消息，所述响应消息携带第四随机数、和所述加密后的组密钥，所述组密钥用于对所述第二设备与所述第一设备之间传输的数据加密。

关于上述加密密钥的生成方式、组密钥的生成方式，均与前述实施例相同，不做赘述。

第二设备的处理，可以包括：所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息；所述第二设备基于所述完整性保护密钥对所述响应消息进行验证，得到验证结果；所述第二设备在所述验证结果表示所述响应消息的完整性验证通过的情况下，所述第二设备从所述响应消息中获取第四随机数；所述第二设备基于所述第四随机数、物理层密钥和密钥生成参数，得到加密密钥；所述第二设备从所述响应消息中获取加密后的组密钥；所述第二设备基于所述加密密钥对所述加密后的组密钥进行解密，得到所述组密钥，所述组密钥用于对所述第二设备与所述第一设备之间传输的数据加密。

关于第二设备得到加密密钥的方式与前述实施例相同，在第二设备得到该组密钥之后，可以采用组密钥对发送的数据进行加密并对接收的数据进行解密，这里不再进行限定。

结合图 20，对前述实施例所提供的认证方法进行一示例性说明。在图 20 中，以第二设备为 A-IoT 设备（为了简洁示意为 A-IoT）、第一设备为 UE/基站、将第一网络设备和第二网络设备合并表示为 AUSF/UDM/ARPF 为例。图 20 的认证方法处理流程包括：

步骤 2001，UE/基站向 A-IoT 设备发送触发消息，该触发消息可以携带 AIoT ID 和/或 Group（组）ID。

步骤 2002，UE/基站向 AUSF 发送认证请求，该认证请求可以携带 AIoT ID 和/或 Group（组）ID。

步骤 2003~步骤 2005 的处理，与前述图 19 中的步骤 1902~步骤 1904 相同，不做重复说明。

步骤 2006，UE/基站发送认证请求（可以携带 AK，MAC)。

步骤 2007，A-IoT 设备收到认证响应后，计算 MAC’， 基于 MAC’成功验证 MAC 后，确定成功验证 AUSF 身份，计算 RES，并计算 Ka 以及 KI。示例性的，$RAND = Kr \oplus AK$ ，MAC’ = f2（Kr, AK），RES = f2（Kr, RAND），Ka=f3（AK, RAND，A-IOT ID），$KI = KDF(Ka, NONCE1, \text{物理层密钥})$，其中，MAC’即验证 MAC，Ka 为前述设备的中间密钥，KI 为 AIOT 设备生成的完整性保护密钥。

步骤 2008，A-IoT 设备发送认证响应(携带 RES)，该认证响应可以用 KI 完保。

步骤 2009，UE/基站生成 KI 后对认证响应验证完保，成功后向 AUSF 发送认证确认，该认证确认

携带 RES。上述 UE/基站生成的 KI 可以称为完整性保护密钥，关于该 UE/基站生成 KI 的方式与前述 AIOT 设备相同，不做重复说明。

另外，在 AUSF 侧还可以执行步骤 2010，验证 RES，关于 AUSF 验证 RES 的具体方式与前述实施例相同，不做重复说明。

步骤 2011，UE/基站向 A-IoT 设备发送响应消息，可以携带加密后的 K-Group（组密钥）。具体的，UE/基站还可以基于所述第四随机数、所述物理层密钥和密钥生成参数，得到加密密钥；基于所述加密密钥对组密钥加密得到加密后的组密钥。另外，上述响应消息中还可以携带第四随机数。

相应的，A-IoT 设备还可以基于所述第四随机数、所述物理层密钥和密钥生成参数，得到加密密钥；所述第二设备基于所述加密密钥对所述加密后的组密钥进行解密，得到所述组密钥。

需要指出，上述图 19、图 20 分别对 Indirect mode 或 Direct mode 下第一设备为 UE 或基站的场景进行的示例性说明。在一些可能的示例中，在 Direct mode 下，上述图 19、图 20 中的 UE/基站还可以替换为第一核心网设备，比如 AMF、SEAF、专用于 AIoT（或 IoT）的核心网网元等等任意之一，这里不对全部可能的示例进行穷举。

可见，通过采用上述认证方法，可以使得第二设备接收认证参数，进而直接根据认证参数和与核心网侧设备共享的根密钥计算得到验证 MAC，基于验证 MAC 对接收到的 MAC 对核心网设备进行认证。如此，在保证了第二设备与核心网侧设备的认证过程的安全性的同时，避免第二设备侧执行较为复杂的计算，提升了第二设备的处理效率，尤其适用于运算能力较低的设备。

图 21 是根据本申请一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S2110、第一设备接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；

S2120、第一设备向所述第二设备发送第二消息，所述第二消息携带认证参数；

S2130、所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

S2140、所述第一设备向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

图 22 是根据本申请另一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S2210、第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

S2220、所述第二设备基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

S2230、所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

图 23 是根据本申请另一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S2310、第一网络设备向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识。

S2320、所述第一网络设备接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备

与所以核心网侧设备共享的密钥。

S2330、所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

所述核心网侧设备、所述第一设备、所述一个或多个核心网设备、第一网络设备以及第二网络设备的定义，均与前述实施例相同，因此不做重复说明。

可选地，所述认证参数包括以下之一：匿名密钥、第一随机数；所述第二设备基于所述认证参数和根密钥计算第一 RES，包括以下之一：所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES；所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES。

相应的，第一网络设备的处理，还包括以下之一：所述第一网络设备接收第二网络设备发来的所述认证参数和所述第一验证 RES；所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES。

本实施例中，生成第一 RES 以及第一验证 RES 的方式，均与前述实施例相同，不做赘述。

可选地，所述方法还包括以下之一：所述第一网络设备接收第二网络设备发来的所述认证参数和所述第一验证 RES；所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES。

可选地，所述第三消息还携带第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备；所述方法还包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和物理层密钥计算所述第二 RES，所述物理层密钥为所述第二设备与所述第一设备之间共享的密钥；所述第二设备采用所述第一计算方式基于所述第一随机数和所述物理层密钥计算所述第二 RES；所述第二设备采用所述第一计算方式基于所述第一 RES 和所述物理层密钥计算所述第二 RES。

第一设备的处理，还包括：所述第一设备在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

所述方法还包括以下之一：所述第一设备采用第一计算方式对匿名密钥和物理层密钥计算所述第二验证 RES，所述物理层密钥为所述第二设备与所述第一设备之间共享的密钥；所述第一设备采用第一计算方式对第一随机数和物理层密钥计算所述第二验证 RES；所述第一设备采用第一计算方式对第一验证 RES 和物理层密钥计算所述第二验证 RES。其中，所述第一消息还携带所述第一验证 RES。

本实施例中，生成第二 RES 以及第二验证 RES 的方式，均与前述实施例相同，不做赘述。

本实施例提供的认证方法，与前述实施例不同之处在于，不执行 MAC 的验证。本实施例所提供的认证方法，除了不执行 MAC 和验证 MAC 的计算，关于上述第二消息、第三消息、第一消息以及第四消息的详细说明，以及第二设备和第一设备之间进行完整性保护密钥的协商、加密密钥的协商、组密钥的生成以及传输等等处理，均可以与前述实施例相同，因此不做重复说明。

可见，通过采用上述认证方法，可以由第一设备向第二设备发送认证参数，进而使得第二设备直接根据认证参数和与核心网侧设备共享的根密钥计算得到第一 RES，将该第一 RES 通过第一设备发送至第一网络设备，以使得核心网侧认证所述第二设备。如此，在保证了安全性的同时，避免第二设备侧执行较为复杂的计算，提升了第二设备的处理效率，尤其适用于运算能力较低的设备。

图 24 是根据本申请一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S2410、第一设备向第二设备发送第二消息，所述第二消息携带认证参数；

S2420、所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第

二 RES 与所述认证参数和第一密钥相关；

S2430、所述第一设备基于所述认证参数和所述第一密钥生成第二验证 RES；

S2440、所述第一设备在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

图 25 是根据本申请另一实施例的认证方法的示意性流程图。该方法包括以下内容的至少部分内容。

S2510、第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

S2520、所述第二设备基于认证参数和第一密钥计算第二 RES，所述第一密钥与所述第一设备相关；

S2530、所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

所述核心网侧设备、所述第一设备、所述一个或多个核心网设备、第一网络设备以及第二网络设备的定义，均与前述实施例相同，因此不做重复说明。

可选地，所述第二设备基于所述认证参数和物理层密钥计算第二 RES，包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和物理层密钥计算所述第二 RES，所述物理层密钥为所述第二设备与所述第一设备之间共享的密钥；所述第二设备采用所述第一计算方式基于所述第一随机数和所述物理层密钥计算所述第二 RES；所述第二设备采用所述第一计算方式基于所述第一 RES 和所述物理层密钥计算所述第二 RES。

所述第一设备生成第二验证 RES，包括以下之一：所述第二设备采用第一计算方式基于所述匿名密钥和物理层密钥计算所述第二 RES，所述物理层密钥为所述第二设备与所述第一设备之间共享的密钥；所述第二设备采用所述第一计算方式基于所述第一随机数和所述物理层密钥计算所述第二 RES；所述第二设备采用所述第一计算方式基于所述第一 RES 和所述物理层密钥计算所述第二 RES。

本实施例中，生成第二 RES 以及第二验证 RES 的方式，均与前述实施例相同，不做赘述。

本实施例提供的认证方法，与前述实施例不同之处在于，不执行 MAC 的验证、且不执行第一 RES 的验证，此外，关于上述第二消息、第三消息、第一消息以及第四消息的详细说明，以及第二设备和第一设备之间进行完整性保护密钥的协商、加密密钥的协商、组密钥的生成以及传输等等处理，均可以与前述实施例相同，因此不做重复说明。

可见，通过采用上述认证方法，可以使得第二设备接收认证参数，进而直接根据认证参数和与核心网侧设备共享的根密钥计算得到第一 RES，将该第一 RES 通过第一设备发送至第一网络设备，以使得核心网侧认证所述第二设备。如此，在保证了安全性的同时，避免第二设备侧执行较为复杂的计算，提升了第二设备的处理效率，尤其适用于运算能力较低的设备。

最后，结合相关技术来对本实施例提供的方案的有益效果进行说明。

Ambient IoT 是 3GPP R19 研究的新型 IoT 终端，是一种由能量收集供电的物联网设备，无电池或能量存储能力有限。设备成本极低，计算能力极为受限，网络架构目前业界有两种方式，可以总结为 Direct mode（直连模式）和 Indirect mode（非直连模式）。比如参见图 26 所示，图 26 上方所示为直连模式，即 AIOT 设备直接连接网络侧的接入网设备（如基站），然后由基站连接核心网进而连接至 AIOT AF；图 26 下方所示为非直连模式，即 AIOT 设备通过其他终端设备（比如中继 UE 或代理 UE）接入基站，然后再通过基站接入 5G 核心网以及 AIOT AF。

在相关技术中，UE 在接入到 5G 网络时必须进行认证和密钥协商过程，才能成功接入 5G 网络，

使用网络资源，网络根据认证结果，授权 UE 使用网络资源和服务。3GPP 安全系列标准定义了 5G AKA 过程、使用密码算法。UE 的 AKA 流程使用的认证和授权凭证是对称根密钥 K，在网络侧由核心网的 UDM/ARPF 网元用集中式的方式保存，每一次授权都需要在 UDM 完成授权凭证的获取，并由核心网完成相应的认证计算。

关于上述 AKA 流程，如图 27 所示，可以包括：

S2701、针对接收到的鉴权请求，UDM/ARPF 通过生成 AV（Authentication Vector，鉴权向量)。也就是 UDM/ARPF 创建一个 5G HE AV(Home Environment Authentication Vector，归属环境鉴权向量)，其中认证管理字段（AMF）分隔位设置为“1”。然后，UDM/ARPF 应推导出 KAUSF(Key Authentication Server Function，密钥鉴权服务功能)并计算 XRES*（Expected Response，预期用户响应)。最后，UDM/ARPF 应从 RAND（Random number，随机数)、AUTN（Authentication Token，鉴权标记)、XRES* 和 KAUSF 创建 5G HE AV。S2702，UDM 应将 5G HE AV 返回给 AUSF。S2703、AUSF 应存储 XRES*与接收到的 SUCI 或 SUPI 一起临时存储 XRES*。S2704、AUSF 应根据从 UDM/ARPF 接收的 5G HE AV 生成 5G AV，计算来自 XRES*的 HXRES*和来自 KAUSF 的 KSEAF，将 5G HE AV 中的 XRES*替换为 HXRES*，将 KAUSF 替换为 KSEAF。S2705、AUSF 移除 KSEAF，将 5G SE AV 返回给 SEAF。S2706、SEAF 向 UE 发送 RAND、AUTN。S2707、USIM 计算响应 RES。 USIM 应向 ME 返回 RES、CK、IK。然后 ME 应从 RES 计算 RES*。S2708、UE 向 SEAF 返回 RES*。S2709、SEAF 从 RES*计算 HRES*，并且比较 HRES*和 HXRES*。如果它们一致，则从服务网络的角度来看，SEAF 应认为认证成功。否则 SEAF 应认为认证失败，并向 AUSF 指示失败。S2710、SEAF 向 AUSF 发送从 UE 接收到的 RES*。S2711、AUSF 将接收到的 RES*与存储的 XRES*进行比较。如果 RES*和 XRES*相等，则 AUSF 应认为认证成功。AUSF 应将认证结果通知 UDM。S2712、AUSF 向 SEAF 指示从归属网络的角度验证是否成功。

图 28 为上述处理流程所对应的认证架构，结合图 28 可以看出上述处理流程中各个参数的计算方式可以包括：匿名密钥 AK = f5K (RAND) 、检索序列号 SQN = (SQN * AK) * AK、XMAC = f1K (SQN || RAND || AMF) 、RES = f2K (RAND)、CK = f3K (RAND)、IK = f4K (RAND)、AK = f5K (RAND)；函数 f1~f5 为 ETSI SAGE 组定义的 MILENAGE 密码算法。示例性的，生成上述过程中所使用的 KAUSF 的方式，可以使用以下参数来形成 KDF 的输入并计算 KAUSF：FC = 0x6A、P0 = serving network name（服务网络名称)，L0 = length of the serving network name 服务网络名称长度，P1 = SQN ⊕ AK。L1 = length of SQN ⊕ AK (i.e. 0x00 0x06)。输入密钥 KEY 应等于串联 CK || CK。可以看出，上述过程中的参数计算是较为复杂的。

结合图 29 来说，在上述处理流程中，UE 和网络侧需要经过 8 次 KDF 计算才能得到最终的加密密钥 KE2Menc 和完整性保护密钥 KE2Eint，因此，5G AKA 和密钥架构较复杂，不适合用于 A-IoT 设备的安全认证，也不支持 A-IoT 设备和 UE 之间进行认证和密钥协商。

在相关技术中，RFID 系统通常由读取器 Reader 和标签 Tag 构成，可工作于不同频段。其中，Tag 根据供电方式可分为无源、有源、半有源 Tag。对于无源标签，其与 Reader 的耦合方式分为近场耦合与远场耦合。近场耦合依靠感应，即 Reader 和 Tag 互感导致标签线圈电流变化可被 Reader 检测到；远场耦合依靠反向散射通信。

相关技术中，读写器和标签的双向认证可以包括：1、读写器生成随机数RN_r，并将RN_r发送给标签。2：标签收到RN_r后，本地也生成随机数RN_t。标签利用哈希函数和 PSK 对$RN_r||RN_t$计算得到MIC_1(消息完整性校验码)。最后将RN_r、RN_t、MIC_1发送给读写器。3：读写器将收到的RN_r与本地的

RN_r做比较，如果不相等，则忽略；如果相等，读写器利用哈希函数和 PSK 对$RN_r||RN_t$计算得到$MIC_1^{'}$，比较MIC_1与$MIC_1^{'}$，如果不相等，则忽略；如果相等，则读写器认证标签合法，且读写器继续利用哈希函数和 PSK 对RN_t计算MIC_2，最后将RN_t、MIC_2发送给标签。4：标签将收到的RN_t与本地的RN_t做比较，如果不相等，则忽略；如果相等，则利用哈希函数和 PSK 对RN_t计算$MIC_2^{'}$，将收到的MIC_2与本地计算的$MIC_2^{'}$做比较，如果不相等，则忽略；如果相等，则标签认证读写器合法，标签将返回鉴别结果给读写器。5：如果标签和读写器需要进行安全通信，则各自通过$KDH(PSK, TID||RID||RN_r||RN_t)$导出会话密钥，KDH()是一种密钥导出算法。

通过上述分析，可以看出，相关技术中 AKA 认证流程和密钥协商的流程所使用的 f1-f5 函数和 KDF 函数计算复杂度较高，密钥架构较复杂，不适合用于 A-IoT 设备的安全认证，也不支持 A-IoT 设备和 UE 之间进行认证和密钥协商。标签和读写器之间进行认证和密钥协商，又无法支持 A-IoT 设备和网络之间进行认证和密钥协商。相比于上述相关技术，本申请所提供的前述多种实施例，可以实现第二设备与核心网侧设备的相互认证，以及第二设备与第一设备之间的相互认证，并且第二设备可以直接使用网络侧发来的认证参数以及自身的根密钥来实现认证处理，保证了安全性的同时还可以减少第二设备侧的计算能力要求；另外，本申请所提供的多种实施例中，协商完整性保护密钥和加密密钥的处理中，不需要多次进行复杂计算，仅需要基于物理层密钥、匿名密钥、随机数等就可以实现，更加适用于运算能力较低的设备。

图 30 是根据本申请一实施例的第一设备的组成结构示意图，包括：

第一通信单元 3010，用于接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

图 31 是根据本申请一实施例的第二设备的组成结构示意图，包括：

第二通信单元 3110，用于接收来自第一设备的第二消息，所述第二消息携带消息认证码 MAC 和认证参数；

第二处理单元 3120，用于基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与核心网侧设备共享的密钥；在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

图 32 是根据本申请一实施例的第一网络设备的组成结构示意图，包括：

第三通信单元 3210，用于向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

图 33 是根据本申请一实施例的电子设备的组成结构示意图，包括：

第四处理单元 3310，用于计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

本申请实施例提供一种第一设备，包括：

第一通信单元，用于接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

本申请实施例提供一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备；

第二处理单元，用于基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

图 32 是根据本申请一实施例的第一网络设备的组成结构示意图，包括：

第三通信单元 3210，用于向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识；接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

第三处理单元 3220，用于在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

图 30 是根据本申请一实施例的第一设备的组成结构示意图，包括：

第一通信单元 3010，用于向第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第二 RES 与所述认证参数和第一密钥相关；

第一处理单元 3020，用于基于所述认证参数和所述第一密钥生成第二验证 RES；在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

本申请实施例提供一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备；

第二处理单元，用于基于认证参数和第一密钥计算第二 RES，所述第一密钥与所述第一设备相关。

本申请实施例的设备能够实现前述的认证方法实施例中的各个设备的对应功能。该第二设备、或第一设备、或第一网络设备、或电子设备中的各个模块（子模块、单元或组件等）对应的流程、功能、实现方式和有益效果，可参见上述方法实施例中的对应描述，在此不再赘述。需要说明，关于申请实施例的第二设备、或第一设备、或第一网络设备、或电子设备中的各个模块（子模块、单元或组件等）所描述的功能，可以由不同的模块（子模块、单元或组件等）实现，也可以由同一个模块（子模块、单元或组件等）实现。

图 34 是根据本申请实施例的通信设备 3400 示意性结构图。该通信设备 3400 包括处理器 3410，处理器 3410 可以从存储器中调用并运行计算机程序，以使通信设备 3400 实现本申请实施例中的方法。

在一种可能的实现方式中，通信设备 3400 还可以包括存储器 3420。其中，处理器 3410 可以从存储器 3420 中调用并运行计算机程序，以使通信设备 3400 实现本申请实施例中的方法。

其中，存储器 3420 可以是独立于处理器 3410 的一个单独的器件，也可以集成在处理器 3410 中。

在一种可能的实现方式中，通信设备 3400 还可以包括收发器 3430，处理器 3410 可以控制该收发器 3430 与其他设备进行通信，具体地，可以向其他设备发送信息或数据，或接收其他设备发送的信息或数据。

其中，收发器 3430 可以包括发射机和接收机。收发器 3430 还可以进一步包括天线，天线的数量可以为一个或多个。

在一种可能的实现方式中，该通信设备 3400 可为本申请实施例的第一设备、或第二设备、或第一网络设备，并且该通信设备 3400 可以实现本申请实施例的各个方法中由第一设备、或第二设备、或第一网络设备实现的相应流程，为了简洁，在此不再赘述。

图 35 是根据本申请实施例的芯片 3500 的示意性结构图。该芯片 3500 包括处理器 3510，处理器 3510 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

在一种可能的实现方式中，芯片 3500 还可以包括存储器 3520。其中，处理器 3510 可以从存储器 3520 中调用并运行计算机程序，以实现本申请实施例中由接入网设备、或第一核心网设备执行的方法。其中，存储器 3520 可以是独立于处理器 3510 的一个单独的器件，也可以集成在处理器 3510 中。

在一种可能的实现方式中，该芯片 3500 还可以包括输入接口 3530。其中，处理器 3510 可以控制该输入接口 3530 与其他设备或芯片进行通信，具体地，可以获取其他设备或芯片发送的信息或数据。在一种可能的实现方式中，该芯片 3500 还可以包括输出接口 3540。其中，处理器 3510 可以控制该输出接口 3540 与其他设备或芯片进行通信，具体地，可以向其他设备或芯片输出信息或数据。

在一种可能的实现方式中，该芯片可应用于本申请实施例中的第一设备、或第二设备、或第一网络设备、或电子设备，并且该芯片可以实现本申请实施例的各个方法中由第一设备、或第二设备、或第一网络设备、或电子设备实现的相应流程，为了简洁，在此不再赘述。

应理解，本申请实施例提到的芯片还可以称为系统级芯片，系统芯片，芯片系统或片上系统芯片等。

上述提及的处理器可以是通用处理器、数字信号处理器（digital signal processor，DSP）、现成可编程门阵列（field programmable gate array，FPGA）、专用集成电路（application specific integrated circuit，ASIC）或者其他可编程逻辑器件、晶体管逻辑器件、分立硬件组件等。其中，上述提到的通用处理器可以是微处理器或者也可以是任何常规的处理器等。

上述提及的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory，ROM）、可编程只读存储器（programmable ROM，PROM）、可擦除可编程只读存储器（erasable PROM，EPROM）、电可擦除可编程只读存储器（electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory，RAM）。

应理解，上述存储器为示例性但不是限制性说明，例如，本申请实施例中的存储器还可以是静态随机存取存储器（static RAM，SRAM）、动态随机存取存储器（dynamic RAM，DRAM）、同步动 态随机存取存储器（synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（synch link DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）等等。也就是说，本申请实施例中的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

图 36 是根据本申请实施例的通信系统 3600 的示意性框图。该通信系统 3600 包括第二设备 3610、

第一设备 3620、第一网络设备 3630。其中，第二设备 3610、第一设备 3620、第一网络设备 3630 可以分别用于实现上述方法中由第二设备、第一设备、第一网络设备、实现的相应的功能。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。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该计算机程序指令时，全部或部分地产生按照本申请实施例中的流程或功能。该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。该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，该计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（Digital Subscriber Line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该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。

应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

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。

以上所述仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以该权利要求的保护范围为准。

权 利 要 求

1.一种认证方法，包括：

第一设备接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二设备的标识；

所述第一设备向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

2.根据权利要求 1 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数。

3.根据权利要求 2 所述的方法，其中，所述方法还包括：

所述第一设备接收来自所述第二设备的第三消息，所述第三消息用于指示所述第二设备对所述核心网侧设备完成认证；

所述第一设备向所述第一网络设备发送第四消息，所述第四消息用于指示所述第二设备对所述核心网侧设备完成认证。

4.根据权利要求 3 所述的方法，其中，所述第三消息携带以下至少之一：

第一 RES，所述第一 RES 用于所述核心网侧设备认证所述第二设备；

第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

5.根据权利要求 4 所述的方法，其中，所述第四消息携带所述第一 RES。

6.根据权利要求 5 所述的方法，其中，所述第二消息还携带服务参数，所述服务参数包括以下至少之一：用于指示环境供能物联网 AIoT 服务类型的类型参数、具备 AIoT 服务功能的服务器的标识、用于指示 AIoT 认证类型的类型参数。

7.根据权利要求 5 所述的方法，其中，所述方法还包括：

所述第一设备在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

8.根据权利要求 7 所述的方法，其中，所述方法还包括以下之一：

所述第一设备采用第一计算方式对匿名密钥和第一密钥计算所述第二验证 RES，所述第一密钥与所述第一设备相关；

所述第一设备采用第一计算方式对第一随机数和第一密钥计算所述第二验证 RES；

所述第一设备采用第一计算方式对第一验证 RES 和第一密钥计算所述第二验证 RES。

9.根据权利要求 8 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

10.根据权利要求 8 所述的方法，其中，所述第一消息还携带所述第一验证 RES。

11.根据权利要求 3-10 任一项所述的方法，其中，所述方法还包括：

所述第一设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

12.根据权利要求 11 所述的方法，其中，所述第三消息还携带第一完整性验证码。

13.根据权利要求 11 或 12 所述的方法，其中，所述第三消息还携带所述第三随机数和/或第四随机

数。

14.根据权利要求 11 或 12 所述的方法，其中，所述方法还包括：

所述第一设备向所述第二设备发送响应消息，所述响应消息响应于所述第三消息，所述响应消息携带以下至少之一：所述第三消息完整性验证通过的指示信息，第二完整性验证码，所述第四随机数，加密后的组密钥。

15.根据权利要求 11 或 12 所述的方法，其中，所述第二消息还携带以下至少之一：所述第三随机数、第三完整性验证码、加密后的组密钥、所述第四随机数。

16.根据权利要求 1-15 任一项所述的方法，其中，所述方法还包括：

所述第一设备接收来自所述第二设备的认证请求，所述认证请求携带所述第二设备的标识；

所述第一设备向所述第一网络设备转发所述认证请求。

17.根据权利要求 1-15 任一项所述的方法，其中，所述方法还包括：

所述第一设备向所述第一网络设备发送认证请求，所述认证请求携带所述第二设备的标识和/或所述第二设备所在的设备组的标识。

18.根据权利要求 1-17 任一项所述的方法，其中，所述核心网侧设备包括核心网、或验证服务器；所述第一网络设备为 AUSF 或 AS；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

19.一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带消息认证码 MAC 和认证参数；

所述第二设备基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与核心网侧设备共享的密钥；

所述第二设备在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

20.根据权利要求 19 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数。

21.根据权利要求 20 所述的方法，其中，所述第二设备基于所述认证参数和所述根密钥计算验证 MAC，包括以下之一：

所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC；

所述第二设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC；

所述第二设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC；

所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC。

22.根据权利要求 21 所述的方法，其中，所述第二设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述验证 MAC，包括：所述第二设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所述验证 MAC；

和/或，所述第二设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述验证 MAC，包括：所述第二设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述验证 MAC。

23.根据权利要求 21 或 22 所述的方法，其中，所述方法还包括：

所述第二设备向所述第一设备发送第三消息，所述第三消息用于指示所述第二设备对所述核心网

侧设备完成认证。

24.根据权利要求 23 所述的方法，其中，所述第三消息携带以下至少之一：

第一 RES，所述第一 RES 用于所述核心网侧设备认证所述第二设备；

第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

25.根据权利要求 24 所述的方法，其中，所述方法还包括以下之一：

所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES；

所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES。

26.根据权利要求 25 所述的方法，其中，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES，包括：所述第二设备采用所述第一计算方式基于服务参数、所述第一随机数和所述根密钥计算第一 RES；

和/或，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES，包括：所述第二设备采用所述第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算第一 RES。

27.根据权利要求 24-26 任一项所述的方法，其中，所述方法还包括以下之一：

所述第二设备采用第一计算方式基于所述匿名密钥和第一密钥计算所述第二 RES，所述第一密钥与所述第一设备相关；

所述第二设备采用所述第一计算方式基于所述第一随机数和所述第一密钥计算所述第二 RES；

所述第二设备采用所述第一计算方式基于所述第一 RES 和所述第一密钥计算所述第二 RES。

28.根据权利要求 27 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

29.根据权利要求 22 或 26 所述的方法，其中，所述第二消息还携带所述服务参数，所述服务参数包括以下至少之一：用于指示环境供能物联网 AIoT 服务类型的类型参数、具备 AIoT 服务功能的服务器的标识、用于指示 AIoT 认证类型的类型参数。

30.根据权利要求 23-28 任一项所述的方法，其中，所述方法还包括：

所述第二设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

31.根据权利要求 30 所述的方法，其中，所述第三消息还携带第一完整性验证码。

32.根据权利要求 30 或 31 所述的方法，其中，所述第三消息还携带第三随机数和/或第四随机数。

33.根据权利要求 30 或 31 所述的方法，其中，所述方法还包括：

所述第二设备接收来自所述第一设备的响应消息，所述响应消息响应于所述第三消息，所述响应消息携带以下至少之一：所述第三消息完整性验证通过的指示信息，第二完整性验证码，所述第四随机数，加密后的组密钥。

34.根据权利要求 30 或 31 所述的方法，其中，所述第二消息还携带以下至少之一：所述第三随机数、第三完整性验证码、加密后的组密钥、所述第四随机数。

35.根据权利要求 33 或 34 所述的方法，其中，所述第二消息用于请求认证，所述方法还包括：

所述第二设备基于所述加密密钥对加密后的组密钥进行解密，得到所述组密钥，所述组密钥用于对所述第二设备与所述第一设备之间传输的数据加密。

36.根据权利要求 19-35 任一项所述的方法，其中，所述方法还包括：

所述第二设备向所述第一设备发送认证请求，所述认证请求携带所述第二设备的标识。

37.根据权利要求 21、22、25-27 任一项所述的方法，其中，所述第一计算方式包括以下之一：第二鉴权函数、哈希算法、AES、ACSON、SNOW 3G、ZUC。

38.根据权利要求 19-37 任一项所述的方法，其中，所述核心网侧设备包括：一个或多个核心网设备或验证服务器；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

39.一种认证方法，包括：

第一网络设备向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

40.根据权利要求 39 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数。

41.根据权利要求 40 所述的方法，其中，所述方法还包括以下之一：

所述第一网络设备接收来自第二网络设备的所述 MAC 和所述认证参数；

所述第一网络设备生成所述认证参数，所述第一网络设备基于所述根密钥和所述认证参数计算所述 MAC。

42.根据权利要求 41 所述的方法，其中，所述第一网络设备基于所述根密钥和所述认证参数计算所述 MAC，包括以下之一：

所述第一网络设备采用第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC；

所述第一网络设备基于所述第一随机数和所述根密钥异或计算所述匿名密钥，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC；

所述第一网络设备基于所述匿名密钥和所述根密钥异或计算所述第一随机数，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC；

所述第一网络设备采用第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC。

43.根据权利要求 42 所述的方法，其中，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算所述 MAC，包括：所述第一网络设备采用第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算所述 MAC；

和/或，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算所述 MAC，包括：所述第一网络设备采用第一计算方式基于所述服务参数、所述第一随机数和所述根密钥计算所述 MAC。

44.根据权利要求 43 所述的方法，其中，所述方法还包括：

所述第一网络设备接收来自所述第一设备的第四消息，其中，所述第四消息用于指示所述第二设备对所述核心网侧设备完成认证。

45.根据权利要求 44 所述的方法，其中，所述第四消息携带第一 RES；所述方法还包括：

所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定认证所述第二设备通过。

46.根据权利要求 45 所述的方法，其中，所述第一消息还携带所述第一验证 RES。

47.根据权利要求 45 或 46 所述的方法，其中，所述方法还包括以下之一：

所述第一网络设备接收来自第二网络设备的所述第一验证 RES；

所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES。

48.根据权利要求 47 所述的方法，其中，所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES，包括以下之一：

所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES；

所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES。

49.根据权利要求 48 所述的方法，其中，所述第一网络设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一验证 RES，包括：所述第一网络设备采用所述第一计算方式基于服务参数、所述第一随机数和所述根密钥计算第一验证 RES；

和/或，所述第一网络设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一验证 RES，包括：所述第一网络设备采用所述第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算第一验证 RES。

50.根据权利要求 43 或 49 所述的方法，其中，所述第一消息还携带所述服务参数，所述服务参数包括以下至少之一：用于指示环境供能物联网 AIoT 服务类型的类型参数、具备 AIoT 服务功能的服务器的标识、用于指示 AIoT 认证类型的类型参数。

51.根据权利要求 39-50 任一项所述的方法，其中，所述第一消息还携带以下至少之一：第二中间密钥、第三中间密钥、第四中间密钥；所述方法还包括以下之一：

所述第一网络设备接收所述第二网络设备发来的所述第二中间密钥、所述第三中间密钥、所述第四中间密钥中至少之一；

所述第一网络设备采用第三计算方式基于所述匿名密钥计算所述第二中间密钥；

所述第一网络设备采用所述第三计算方式基于所述第一随机数计算所述第二中间密钥；

所述第一网络设备采用第三计算方式基于所述匿名密钥和所述第一密钥计算所述第二中间密钥；

所述第一网络设备采用所述第三计算方式基于所述第一随机数和所述第一密钥计算所述第二中间密钥；

所述第一网络设备采用所述第三计算方式基于所述根密钥和所述第一随机数计算所述第三中间密钥；

所述第一网络设备采用所述第三计算方式基于所述根密钥和所述匿名密钥计算所述第三中间密钥；

所述第一网络设备采用所述第三计算方式基于所述根密钥、所述第一密钥和所述第一随机数计算所述第三中间密钥；

所述第一网络设备采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥计算所述第三中间密钥；

所述第一网络设备采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥、所述第一密钥计算所述第三中间密钥。

52.根据权利要求 39-51 任一项所述的方法，其中，所述第一消息还携带所述第二设备所在的设备组的标识；所述方法还包括以下之一：

所述第一网络设备接收来自所述第一设备的认证请求，所述认证请求携带所述第二设备的标识和/或所述第二设备所在的设备组的标识；

所述第一网络设备接收来自服务器的触发消息，所述触发消息携带所述第二设备的标识和/或所述第二设备所在的设备组的标识。

53.根据权利要求 39-52 任一项所述的方法，其中，所述核心网侧设备包括：一个或多个核心网设备或验证服务器；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备；所述第一网络设备为 AUSF 或验证服务器；所述第二网络设备包括以下至少之一：用户数据管理 UDM、认证凭据存储和处理功能 ARPF。

54.一种密钥生成方法，包括：

电子设备计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

55.根据权利要求 54 所述的方法，其中，所述电子设备为第一设备或第二设备；所述第二设备为 AIoT 设备，所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

56.根据权利要求 55 所述的方法，其中，所述计算完整性保护密钥包括以下之一：

采用第二计算方式基于所述匿名密钥和第三随机数计算所述完整性保护密钥；

采用所述第二计算方式基于所述第一随机数和所述第三随机数计算所述完整性保护密钥；

采用第二计算方式基于所述匿名密钥、所述第一密钥和第三随机数计算所述完整性保护密钥；

采用所述第二计算方式基于所述第一随机数、所述第一密钥和所述第三随机数计算所述完整性保护密钥；

采用所述第二计算方式基于第二中间密钥和所述第三随机数计算所述完整性保护密钥，所述第二中间密钥与所述密钥生成参数相关；

采用所述第二计算方式基于第三中间密钥和所述第三随机数计算所述完整性保护密钥，所述第三中间密钥与根密钥和所述密钥生成参数相关。

57.根据权利要求 55 所述的方法，其中，所述计算加密密钥包括以下之一：

采用第二计算方式对第四随机数和所述匿名密钥计算所述加密密钥；

采用所述第二计算方式基于所述第一随机数和所述第四随机数计算所述加密密钥；

采用第二计算方式基于所述匿名密钥、所述第一密钥和所述第四随机数计算所述加密密钥；

采用所述第二计算方式基于所述第一随机数、所述第一密钥和所述第四随机数计算所述加密密钥；

采用所述第二计算方式基于第二中间密钥和所述第四随机数计算所述加密密钥，所述第二中间密钥与所述密钥生成参数相关；

采用所述第二计算方式基于第三中间密钥和所述第四随机数计算所述加密密钥，所述第三中间密钥与所述根密钥和所述密钥生成参数相关。

58.根据权利要求 56 或 57 所述的方法，其中，所述方法还包括以下至少之一：

采用第三计算方式基于所述匿名密钥计算所述第二中间密钥；

采用所述第三计算方式基于所述第一随机数计算所述第二中间密钥；

采用第三计算方式基于所述匿名密钥和所述第一密钥计算所述第二中间密钥；

采用所述第三计算方式基于所述第一随机数和所述第一密钥计算所述第二中间密钥；

采用所述第三计算方式基于所述根密钥和所述第一随机数计算所述第三中间密钥；

采用所述第三计算方式基于所述根密钥和所述匿名密钥计算所述第三中间密钥；

采用所述第三计算方式基于所述根密钥、所述第一密钥和所述第一随机数计算所述第三中间密钥；

采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥计算所述第三中间密钥；

采用所述第三计算方式基于所述根密钥和所述第一随机数计算第四中间密钥，采用所述第二计算方式基于所述第四中间密钥、所述第一密钥计算所述第三中间密钥。

59.根据权利要求 55 所述的方法，其中，所述电子设备为所述第二设备，所述方法还包括：

所述第二设备基于所述加密密钥对加密后的组密钥进行解密，得到所述组密钥，所述组密钥用于对所述第二设备与所述第一设备之间传输的数据加密。

60.根据权利要求 55 所述的方法，其中，所述电子设备为所述第一设备，所述方法还包括：

所述第一设备基于所述加密密钥对组密钥进行加密，得到加密后的组密钥。

61.根据权利要求 60 所述的方法，其中，所述方法还包括以下之一：

所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的第一密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的第一密钥、每个设备的标识、所述第三随机数计算所述组密钥。

62.根据权利要求 60 所述的方法，其中，所述方法还包括以下之一：

所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的物理层密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述

组密钥；

所述第一设备采用第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、所述每个设备的第一密钥、所述每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、对所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的标识、所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的中间密钥、每个设备的第一密钥、每个设备的标识和所述第三随机数计算所述组密钥；

所述第一设备采用所述第三计算方式基于所述设备组的标识、所述第一设备的标识、所述第二设备所在组的每个设备的匿名密钥、每个设备的中间密钥、每个设备的第一密钥、每个设备的标识、所述第三随机数计算所述组密钥。

63.根据权利要求 56-58、61、62 任一项所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

64.一种认证方法，包括：

第一设备接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；

第一设备向所述第二设备发送第二消息，所述第二消息携带认证参数；

所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

所述第一设备向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

65.根据权利要求 64 所述的方法，其中，所述第三消息还携带第二 RES，所述方法还包括：

所述第一设备在第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

66.根据权利要求 65 所述的方法，其中，所述方法还包括以下之一：

所述第一设备采用第一计算方式对匿名密钥和第一密钥计算所述第二验证 RES，所述第一密钥与所述第一设备相关；

所述第一设备采用第一计算方式对第一随机数和第一密钥计算所述第二验证 RES；

所述第一设备采用第一计算方式对第一验证 RES 和第一密钥计算所述第二验证 RES。

67.根据权利要求 66 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

68.根据权利要求 66 所述的方法，其中，所述第一消息还携带所述第一验证 RES。

69.根据权利要求 64-68 任一项所述的方法，其中，所述核心网侧设备包括：一个或多个核心网设备或验证服务器；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

70.一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

所述第二设备基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

71.根据权利要求 70 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数；所述第二设备基于所述认证参数和根密钥计算第一 RES，包括以下之一：

所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES；

所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES。

72.根据权利要求 71 所述的方法，其中，所述第二设备采用所述第一计算方式基于所述第一随机数和所述根密钥计算第一 RES，包括：所述第二设备采用所述第一计算方式基于服务参数、所述第一随机数和所述根密钥计算第一 RES；

和/或，所述第二设备采用所述第一计算方式基于所述匿名密钥和所述根密钥计算第一 RES，包括：所述第二设备采用所述第一计算方式基于服务参数、所述匿名密钥和所述根密钥计算第一 RES。

73.根据权利要求 72 所述的方法，其中，所述第二消息还携带所述服务参数，所述服务参数包括以下至少之一：用于指示环境供能物联网 AIoT 服务类型的类型参数、具备 AIoT 服务功能的服务器的标识、用于指示 AIoT 认证类型的类型参数。

74.根据权利要求 70-73 任一项所述的方法，其中，所述第三消息还携带第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备；所述方法还包括以下之一：

所述第二设备采用第一计算方式基于所述匿名密钥和第一密钥计算所述第二 RES，所述第一密钥与所述第一设备相关；

所述第二设备采用所述第一计算方式基于所述第一随机数和所述第一密钥计算所述第二 RES；

所述第二设备采用所述第一计算方式基于所述第一 RES 和所述第一密钥计算所述第二 RES 。

75.根据权利要求 74 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

76.根据权利要求 75 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

77.根据权利要求 70-76 任一项所述的方法，其中，所述核心网侧设备包括：一个或多个核心网设备或验证服务器；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

78.一种认证方法，包括：

第一网络设备向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识；

所述第一网络设备接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

所述第一网络设备在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

79.根据权利要求 78 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数。

80.根据权利要求 79 所述的方法，其中，所述方法还包括以下之一：

所述第一网络设备接收第二网络设备发来的所述认证参数和所述第一验证 RES；

所述第一网络设备采用所述第一计算方式基于所述根密钥和所述认证参数计算所述第一验证 RES。

81.根据权利要求 80 所述的方法，其中，所述核心网侧设备包括：一个或多个核心网设备或验证服务器；所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备；所述第一网络设备为 AUSF 或验证服务器；所述第二网络设备包括以下至少之一：用户数据管理 UDM、认证凭据存储和处理功能 ARPF。

82.一种认证方法，包括：

第一设备向第二设备发送第二消息，所述第二消息携带认证参数；

所述第一设备接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第二 RES 与所述认证参数和第一密钥相关；

所述第一设备基于所述认证参数和所述第一密钥生成第二验证 RES；

所述第一设备在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

83.根据权利要求 82 所述的方法，其中，所述方法还包括：所述第一设备接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识。

84.根据权利要求 83 所述的方法，其中，所述第一设备基于所述认证参数和所述第一密钥生成第二验证 RES，包括以下之一：

所述第一设备采用第一计算方式对匿名密钥和第一密钥计算所述第二验证 RES，所述第一密钥与所述第一设备相关；

所述第一设备采用第一计算方式对第一随机数和第一密钥计算所述第二验证 RES；

所述第一设备采用第一计算方式对第一验证 RES 和第一密钥计算所述第二验证 RES。

85.根据权利要求 84 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

86.根据权利要求 84 所述的方法，其中，所述第一消息还携带所述第一验证 RES。

87.根据权利要求 82-86 任一项所述的方法，其中，所述第二设备为环境供能物联网 AIoT 设备；所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备、第一核心网设备。

88.一种认证方法，包括：

第二设备接收来自第一设备的第二消息，所述第二消息携带认证参数；

所述第二设备基于认证参数和第一密钥计算第二 RES，所述第一密钥与所述第一设备相关；

所述第二设备向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备。

89.根据权利要求 88 所述的方法，其中，所述认证参数包括以下之一：匿名密钥、第一随机数；所述第二设备基于所述认证参数和第一密钥计算第二 RES，包括以下之一：

所述第二设备采用第一计算方式基于所述匿名密钥和第一密钥计算所述第二 RES；

所述第二设备采用所述第一计算方式基于所述第一随机数和所述第一密钥计算所述第二 RES；

所述第二设备采用所述第一计算方式基于所述第一 RES 和所述第一密钥计算所述第二 RES。

90.根据权利要求 89 所述的方法，其中，所述第一密钥为以下至少之一：基于所述第一设备的标识和第二随机数计算得到的第一中间密钥、物理层密钥，所述物理层密钥为所述第二设备与所述第一设备共享的密钥。

91.根据权利要求 88-90 任一项所述的方法，其中，所述第一设备包括以下至少之一：终端设备、接入网设备、认证设备；所述第二设备为环境供能物联网 AIoT 设备。

92.一种第一设备，包括：

第一通信单元，用于接收来自第一网络设备的第一消息，所述第一消息携带 MAC、认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带所述 MAC 和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥。

93.一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带消息认证码 MAC 和认证参数；

第二处理单元，用于基于所述认证参数和根密钥计算验证 MAC，所述根密钥为所述第二设备与核心网侧设备共享的密钥；在所述验证 MAC 与所述 MAC 相同的情况下，所述第二设备对所述核心网侧设备完成认证。

94.一种第一网络设备，包括：

第三通信单元，用于向第一设备发送第一消息，其中，所述第一消息携带消息认证码 MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证 MAC，所述验证 MAC 用于所述第二设备结合所述 MAC 认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

95.一种电子设备，包括：

第四处理单元，用于计算完整性保护密钥和/或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密。

96.一种第一设备，包括：

第一通信单元，用于接收来自第一网络设备的第一消息，所述第一消息携带认证参数和第二设备的标识；向所述第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；向所述第一网络设备发送第四消息，所述第四消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备。

97.一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第一 RES，所述第一 RES 用于核心网侧设备认证所述第二设备；

第二处理单元，用于基于所述认证参数和根密钥计算第一 RES，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥。

98.一种第一网络设备，包括：

第三通信单元，用于向第一设备发送第一消息，所述第一消息携带认证参数和第二设备的标识；接收来自所述第一设备的第四消息，所述第四消息携带所述第一 RES，所述第一 RES 为所述第二设备基于所述认证参数和根密钥得到的，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥；

第三处理单元，用于在所述第一 RES 与第一验证 RES 相同的情况下，确定所述第二设备认证通过。

99.一种第一设备，包括：

第一通信单元，用于向第二设备发送第二消息，所述第二消息携带认证参数；接收来自所述第二设备的第三消息，所述第三消息携带第二 RES，所述第二 RES 与所述认证参数和第一密钥相关；

第一处理单元，用于基于所述认证参数和所述第一密钥生成第二验证 RES；在所述第二验证 RES 与所述第二 RES 相同的情况下，确定所述第二设备认证通过。

100.一种第二设备，包括：

第二通信单元，用于接收来自第一设备的第二消息，所述第二消息携带认证参数；向所述第一设备发送第三消息，所述第三消息携带所述第二 RES，所述第二 RES 用于所述第一设备认证所述第二设备；

第二处理单元，用于基于认证参数和第一密钥计算第二 RES，所述第一密钥与所述第一设备相关。

101.一种第一设备，包括：收发器、处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，以使所述第一设备执行如权利要求 1 至 18、或权利要求 64 至 69、或权利要求 82 至 87 中任一项所述的方法。

102.一种第二设备，包括：收发器、处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，以使所述第二设备执行如权利要求 19 至 38、或权利要求 70 至 77、或权利要求 88 至 91 中任一项所述的方法。

103.一种第一网络设备，包括：收发器、处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，以使所述第一网络设备执行如权利要求 39 至 53、或权利要求 78 至 81 中任一项所述的方法。

104.一种电子设备，包括：收发器、处理器和存储器，该存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，以使所述电子设备执行如权利要求 54 至 63 中任一项所述的方法。

105.一种芯片，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的设备执行如权利要求 1 至 18、或权利要求 19 至 38、或权利要求 39 至 53、或权利要求 54 至 63、或权利要求 64 至 69、或权利要求 70 至 77、或权利要求 78 至 81、或权利要求 82 至 87、或权利要求 88 至 91 中任一项所述的方法。

106.一种计算机可读存储介质，用于存储计算机程序，当所述计算机程序被设备运行时使得所述设备执行如权利要求 1 至 18、或权利要求 19 至 38、或权利要求 39 至 53、或权利要求 54 至 63、或权利要求 64 至 69、或权利要求 70 至 77、或权利要求 78 至 81、或权利要求 82 至 87、或权利要求 88 至 91 中任一项所述的方法。

107 一种计算机程序产品，包括计算机程序指令，该计算机程序指令使得计算机执行如权利要求 1 至 18、或权利要求 19 至 38、或权利要求 39 至 53、或权利要求 54 至 63、或权利要求 64 至 69、或权

利要求 70 至 77、或权利要求 78 至 81、或权利要求 82 至 87、或权利要求 88 至 91 中任一项所述的方法。

108.一种计算机程序，所述计算机程序使得计算机执行如权利要求 1 至 18、或权利要求 19 至 38、或权利要求 39 至 53、或权利要求 54 至 63、或权利要求 64 至 69、或权利要求 70 至 77、或权利要求 78 至 81、或权利要求 82 至 87、或权利要求 88 至 91 中任一项所述的方法。

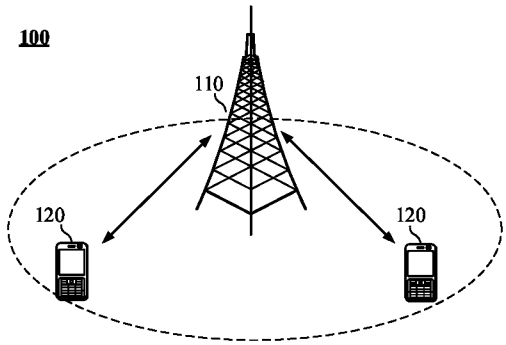
100
110
120
120

图 1

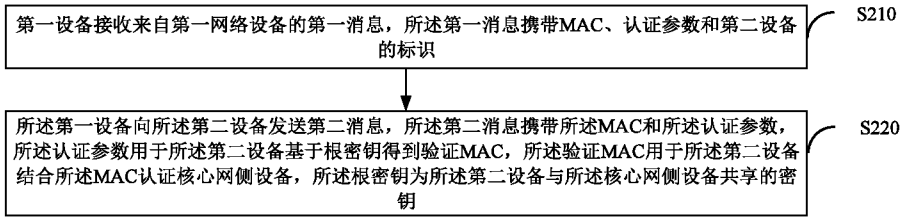
第一设备接收来自第一网络设备的第一消息，所述第一消息携带MAC、认证参数和第二设备的标识
S210
所述第一设备向所述第二设备发送第二消息，所述第二消息携带所述MAC和所述认证参数，所述认证参数用于所述第二设备基于根密钥得到验证MAC，所述验证MAC用于所述第二设备结合所述MAC认证核心网侧设备，所述根密钥为所述第二设备与所述核心网侧设备共享的密钥
S220

图 2

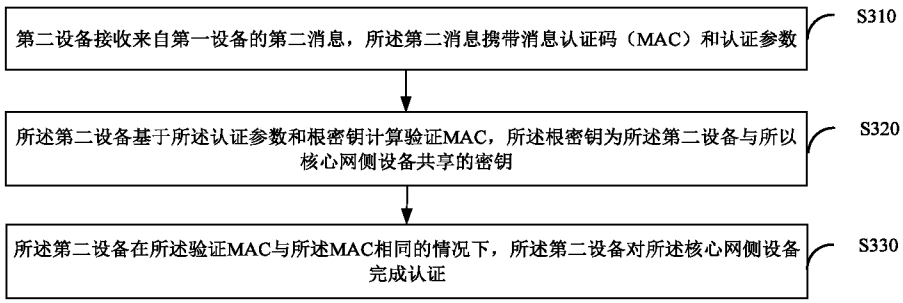
第二设备接收来自第一设备的第二消息，所述第二消息携带消息认证码（MAC）和认证参数
S310
所述第二设备基于所述认证参数和根密钥计算验证MAC，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥
S320
所述第二设备在所述验证MAC与所述MAC相同的情况下，所述第二设备对所述核心网侧设备完成认证
S330

图 3

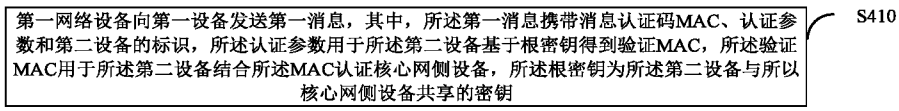
第一网络设备向第一设备发送第一消息，其中，所述第一消息携带消息认证码MAC、认证参数和第二设备的标识，所述认证参数用于所述第二设备基于根密钥得到验证MAC，所述验证MAC用于所述第二设备结合所述MAC认证核心网侧设备，所述根密钥为所述第二设备与所以核心网侧设备共享的密钥
S410

图 4

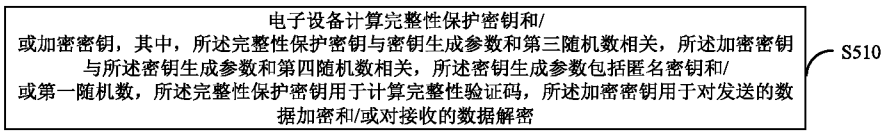
电子设备计算完整性保护密钥和/
或加密密钥，其中，所述完整性保护密钥与密钥生成参数和第三随机数相关，所述加密密钥与所述密钥生成参数和第四随机数相关，所述密钥生成参数包括匿名密钥和/
或第一随机数，所述完整性保护密钥用于计算完整性验证码，所述加密密钥用于对发送的数据加密和/或对接收的数据解密
S510

图 5

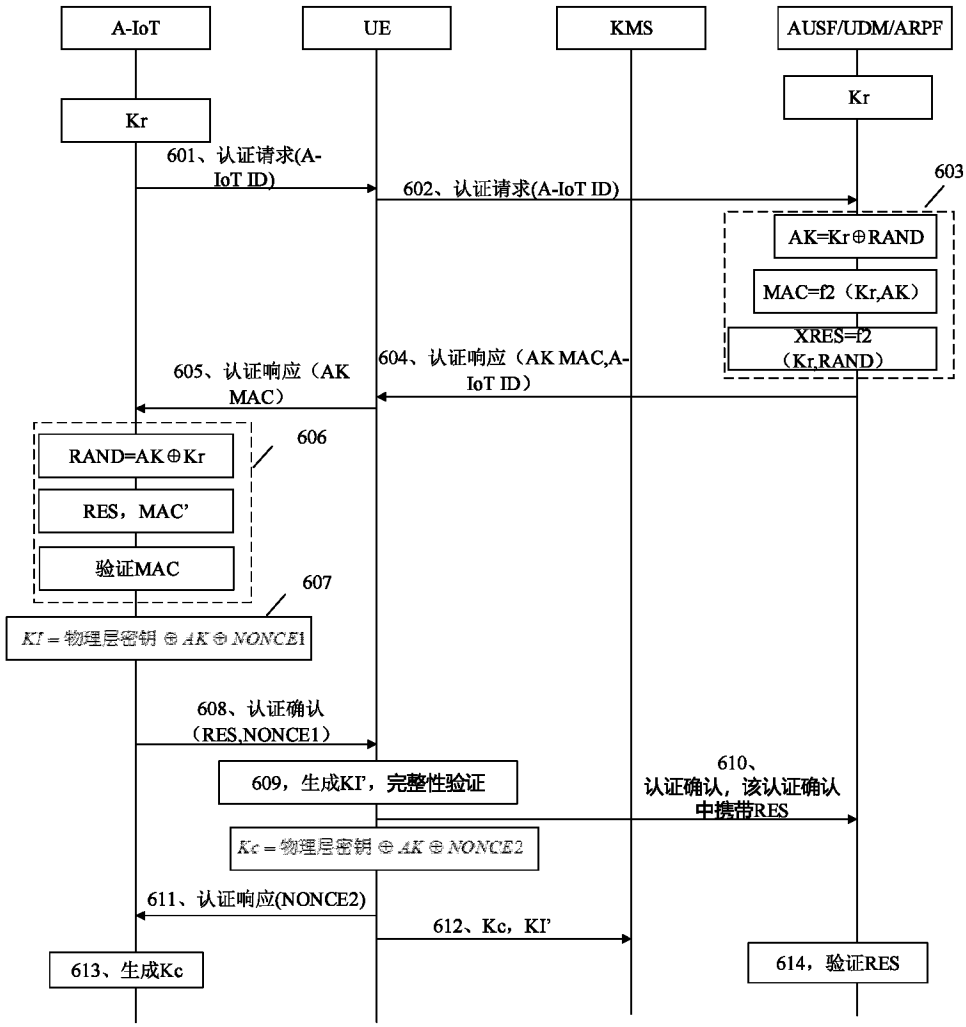
A-IoT
UE
KMS
AUSF/UDM/ARPF
Kr
Kr
601、认证请求(A-IoT ID)
602、认证请求(A-IoT ID)
603
AK=Kr⊕RAND
MAC=f2（Kr,AK）
XRES=f2（Kr,RAND）
604、认证响应（AK MAC,A-IoT ID）
605、认证响应（AK MAC）
606
RAND=AK⊕Kr
RES，MAC'
验证MAC
607
KI = 物理层密钥 ⊕ AK ⊕ NONCE1
608、认证确认（RES,NONCE1）
609，生成KI'，完整性验证
610、认证确认，该认证确认中携带RES
Kc = 物理层密钥 ⊕ AK ⊕ NONCE2
611、认证响应(NONCE2)
612、Kc，KI'
613、生成Kc
614，验证RES

图 6

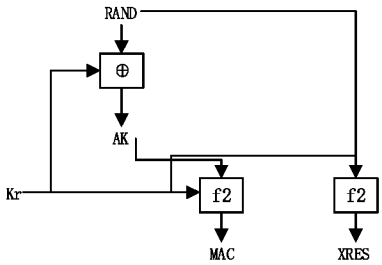
RAND
⊕
AK
Kr
f2
f2
MAC
XRES

图 7a

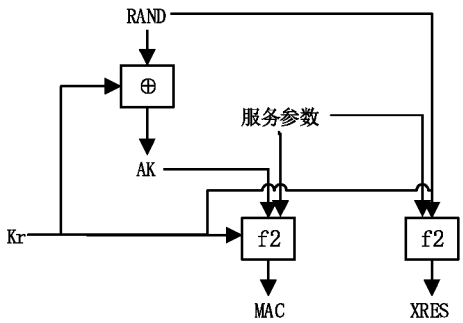
RAND
⊕
服务参数
AK
Kr
f2
f2
MAC
XRES

图 7b

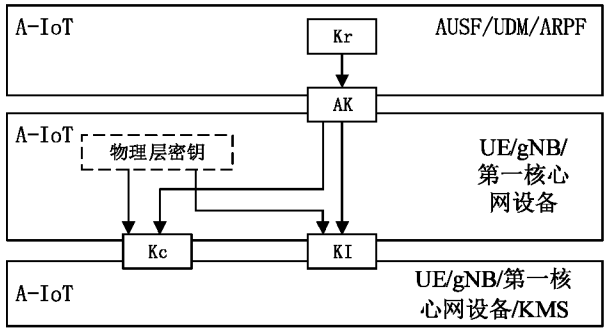
A-IoT
Kr
AUSF/UDM/ARPF
AK
A-IoT
物理层密钥
UE/gNB/
第一核心
网设备
Kc
KI
A-IoT
UE/gNB/第一核
心网设备/KMS

图 8

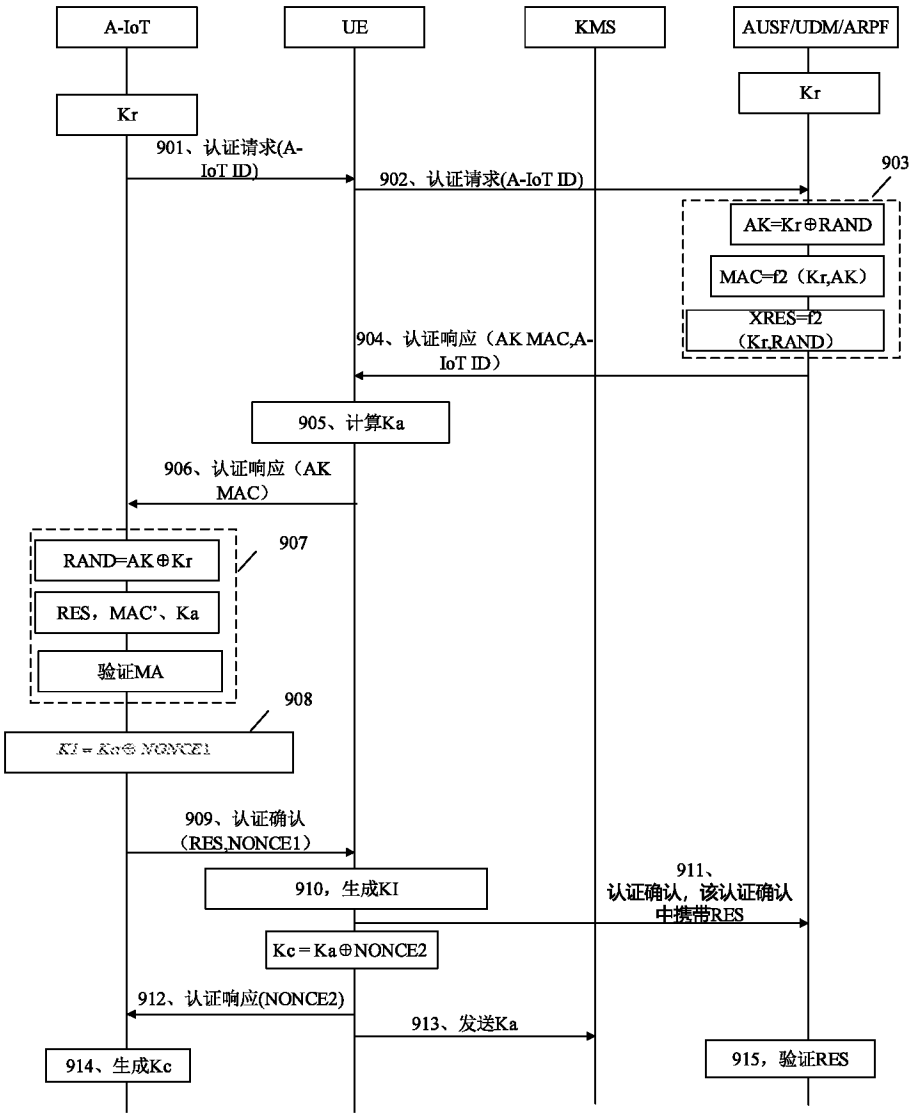
A-IoT
UE
KMS
AUSF/UDM/ARPF
Kr
Kr
901、认证请求(A-IoT ID)
902、认证请求(A-IoT ID)
903
AK=Kr⊕RAND
MAC=f2（Kr,AK）
XRES=f2（Kr,RAND）
904、认证响应（AK MAC,A-IoT ID）
905、计算Ka
906、认证响应（AK MAC）
907
RAND=AK⊕Kr
RES，MAC'、Ka
验证MA
908
KI＝Kr⊕ NONCE1
909、认证确认（RES,NONCE1）
910，生成KI
911、认证确认，该认证确认中携带RES
Kc＝Ka⊕NONCE2
912、认证响应(NONCE2)
913、发送Ka
914、生成Kc
915，验证RES

图 9

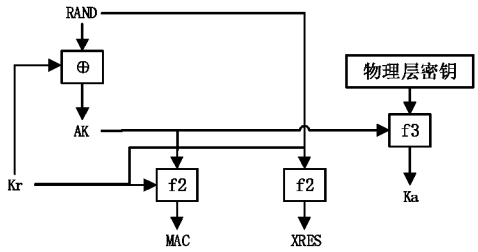
RAND
⊕
AK
Kr
f2
f2
f3
物理层密钥
MAC
XRES
Ka

图 10

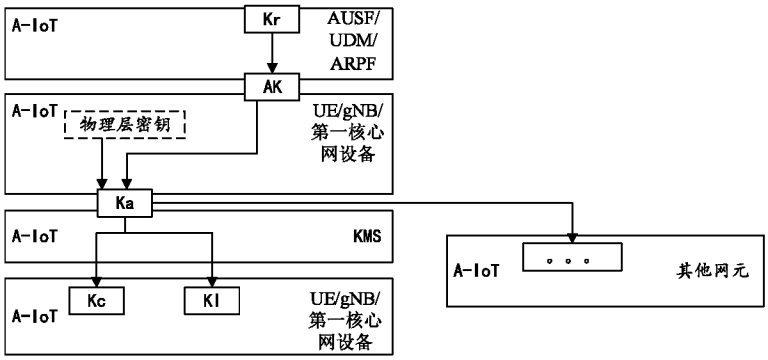
A-IoT
Kr
AUSF/
UDM/
ARPF
AK
A-IoT
物理层密钥
UE/gNB/
第一核心
网设备
Ka
A-IoT
KMS
A-IoT
。。。
其他网元
A-IoT
Kc
KI
UE/gNB/
第一核心
网设备

图 11

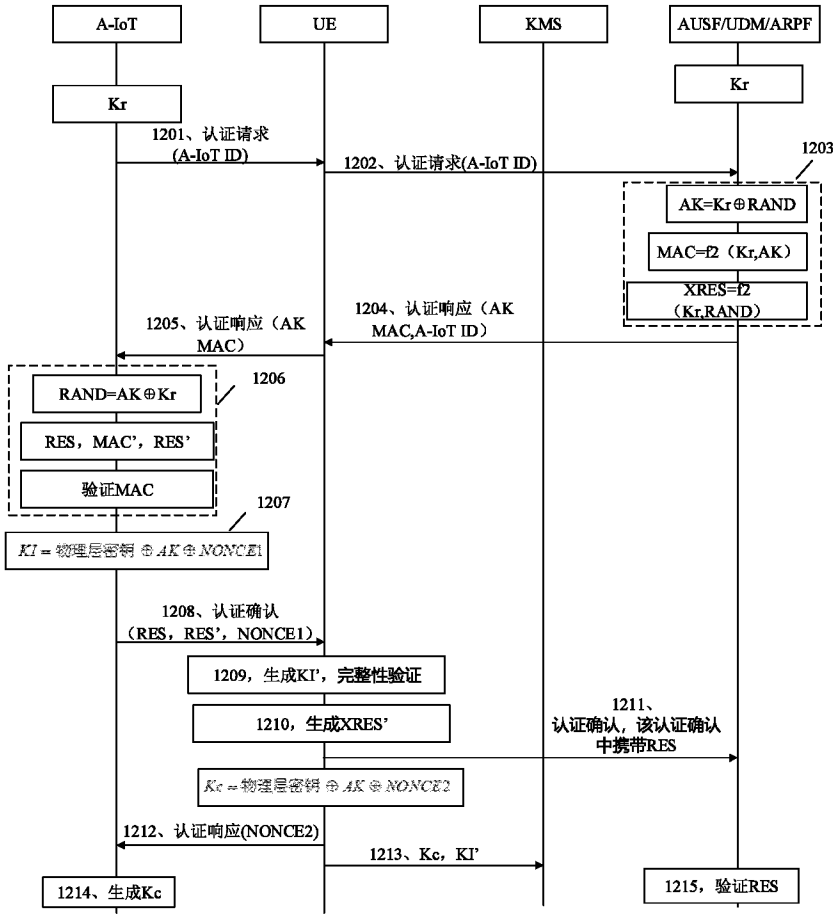
A-IoT
UE
KMS
AUSF/UDM/ARPF
Kr
Kr
1201、认证请求
(A-IoT ID)
1202、认证请求(A-IoT ID)
1203
AK=Kr⊕RAND
MAC=f2（Kr,AK）
XRES=f2
（Kr,RAND）
1204、认证响应（AK
MAC,A-IoT ID）
1205、认证响应（AK
MAC）
1206
RAND=AK⊕Kr
RES，MAC’，RES’
验证MAC
1207
KI＝物理层密钥⊕AK⊕NONCE1
1208、认证确认
（RES，RES’，NONCE1）
1209，生成KI’，完整性验证
1210，生成XRES’
1211、
认证确认，该认证确认
中携带RES
Kc＝物理层密钥⊕AK⊕NONCE2
1212、认证响应(NONCE2)
1213、Kc，KI’
1214、生成Kc
1215，验证RES

图 12

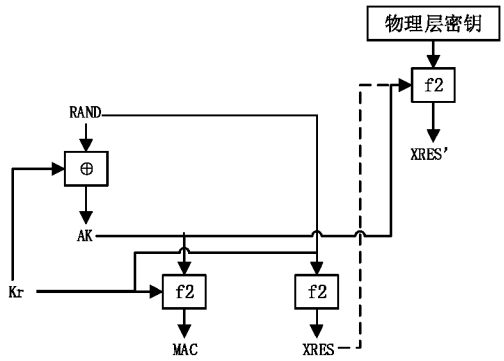
物理层密钥
f2
XRES'
RAND
⊕
AK
Kr
f2
f2
MAC
XRES

图 13

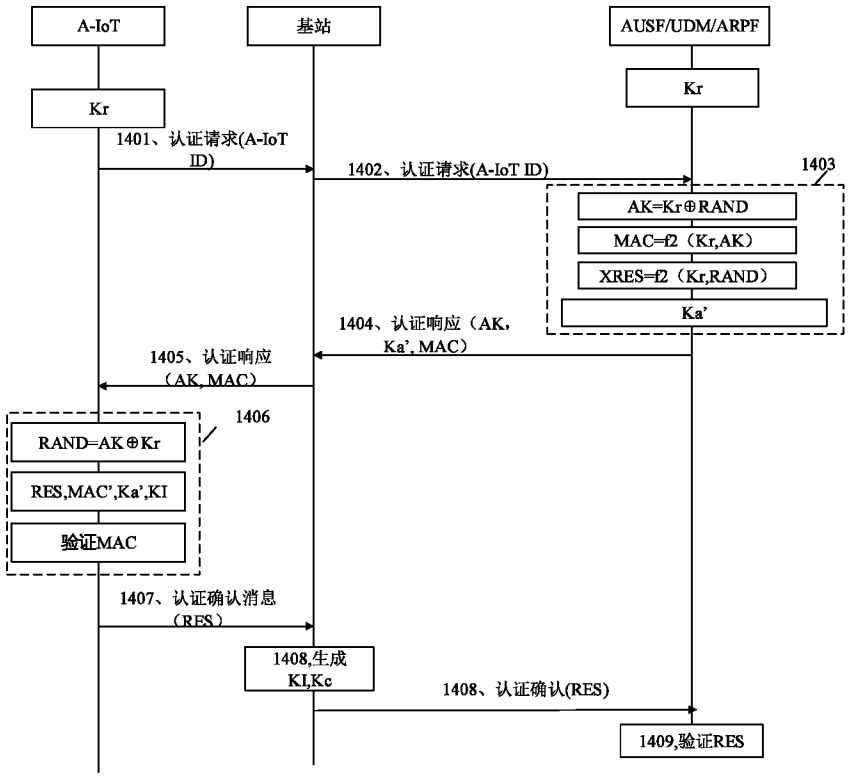
A-IoT
基站
AUSF/UDM/ARPF
Kr
Kr
1401、认证请求(A-IoT ID)
1402、认证请求(A-IoT ID)
1403
AK=Kr⊕RAND
MAC=f2（Kr,AK）
XRES=f2（Kr,RAND）
Ka'
1404、认证响应（AK，Ka', MAC）
1405、认证响应（AK, MAC）
1406
RAND=AK⊕Kr
RES,MAC',Ka',KI
验证MAC
1407、认证确认消息（RES）
1408,生成KI,Kc
1408、认证确认(RES)
1409,验证RES

图 14

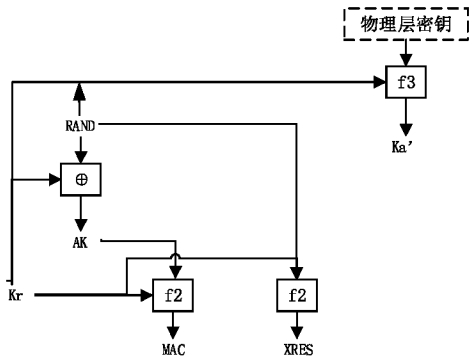
物理层密钥
f3
Ka'
RAND
⊕
AK
Kr
f2
f2
MAC
XRES

图 15

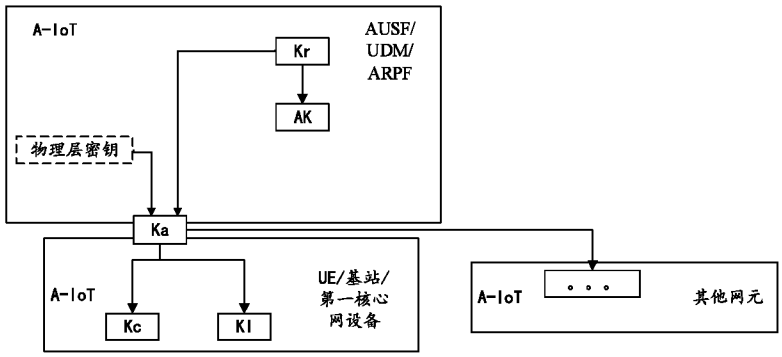
A-IoT
AUSF/
UDM/
ARPF
Kr
AK
物理层密钥
Ka
A-IoT
Kc
KI
UE/基站/
第一核心
网设备
A-IoT
。。。
其他网元

图 16

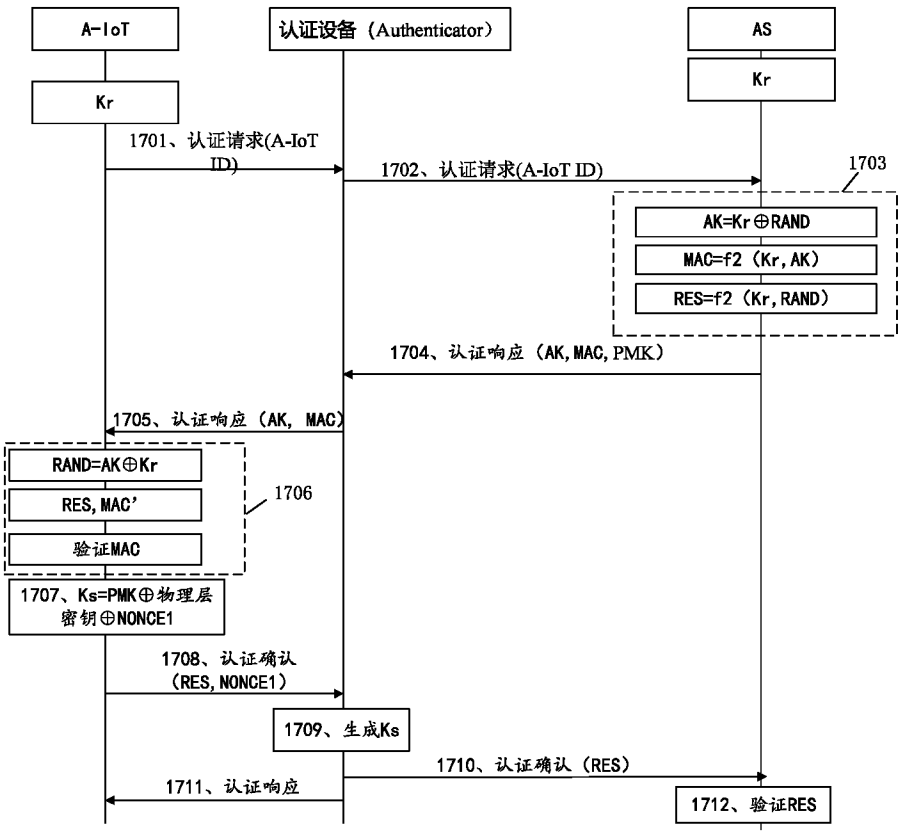
A-IoT
认证设备（Authenticator）
AS
Kr
Kr
1701、认证请求(A-IoT ID)
1702、认证请求(A-IoT ID)
1703
AK=Kr⊕RAND
MAC=f2（Kr,AK）
RES=f2（Kr,RAND）
1704、认证响应（AK,MAC,PMK）
1705、认证响应（AK, MAC）
RAND=AK⊕Kr
RES,MAC'
验证MAC
1706
1707、Ks=PMK⊕物理层密钥⊕NONCE1
1708、认证确认（RES,NONCE1）
1709、生成Ks
1710、认证确认（RES）
1711、认证响应
1712、验证RES

图 17

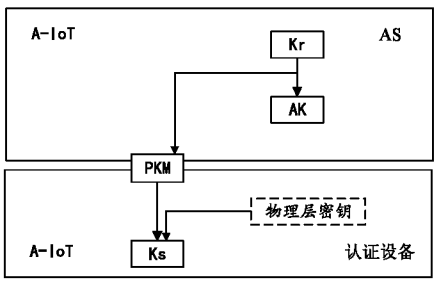
A-IoT
Kr
AS
AK
PKM
物理层密钥
A-IoT
Ks
认证设备

图 18

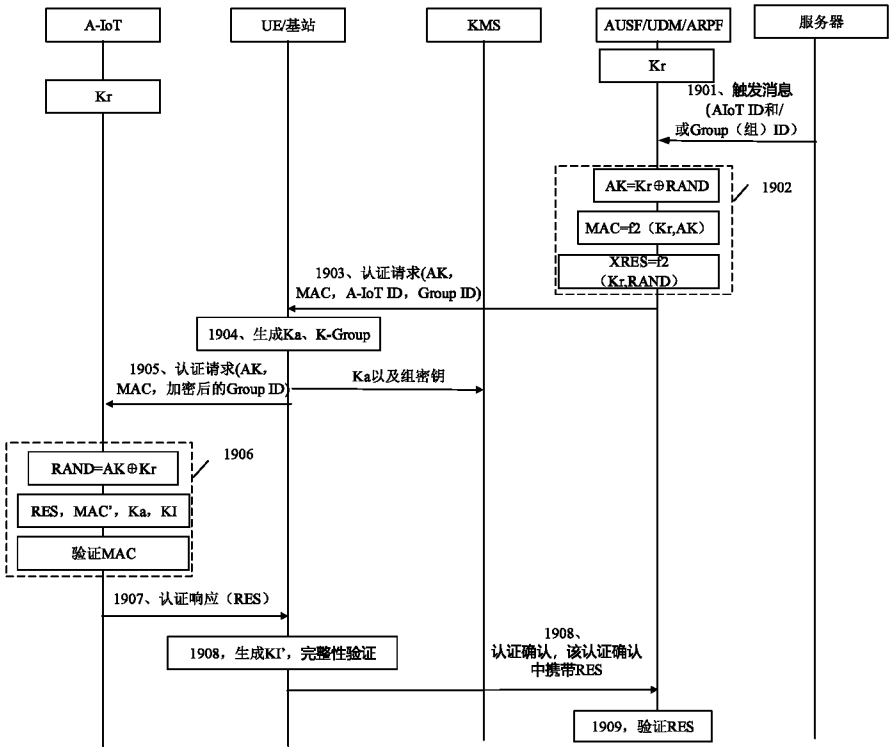
A-IoT
UE/基站
KMS
AUSF/UDM/ARPF
服务器
Kr
Kr
1901、触发消息
（AIoT ID和/
或Group（组）ID）
AK=Kr⊕RAND
1902
MAC=f2（Kr,AK）
XRES=f2
（Kr,RAND）
1903、认证请求(AK，
MAC，A-IoT ID，Group ID)
1904、生成Ka、K-Group
1905、认证请求(AK，
MAC，加密后的Group ID)
Ka以及组密钥
RAND=AK⊕Kr
1906
RES，MAC'，Ka，KI
验证MAC
1907、认证响应（RES）
1908，生成KI'，完整性验证
1908、
认证确认，该认证确认
中携带RES
1909，验证RES

图 19

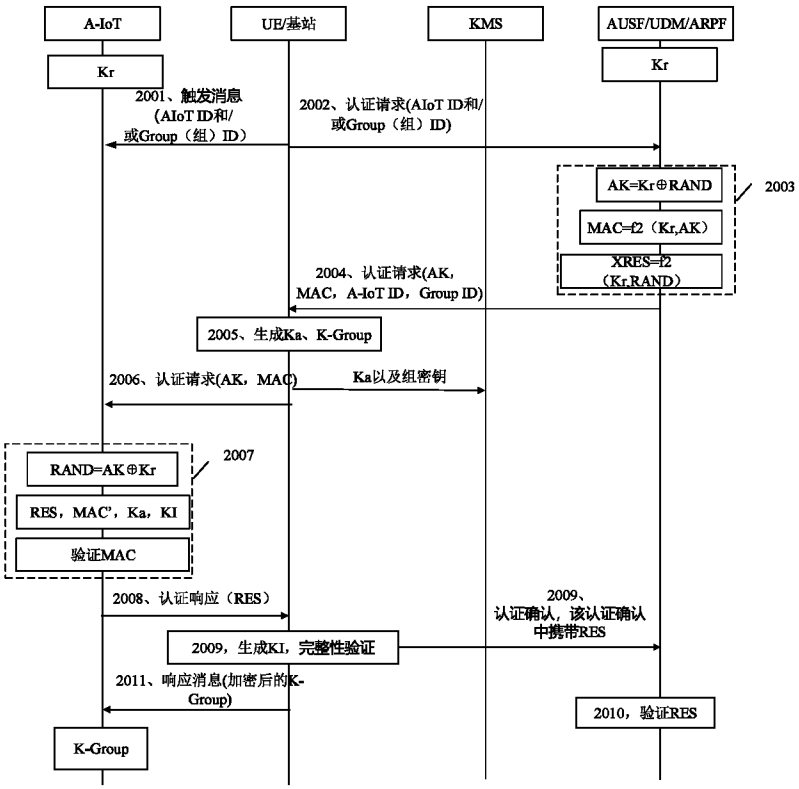
A-IoT
UE/基站
KMS
AUSF/UDM/ARPF
Kr
Kr
2001、触发消息
（AIoT ID和/
或Group（组）ID）
2002、认证请求(AIoT ID和/
或Group（组）ID)
AK=Kr⊕RAND
2003
MAC=f2（Kr,AK）
XRES=f2
（Kr,RAND）
2004、认证请求(AK，
MAC，A-IoT ID，Group ID)
2005、生成Ka、K-Group
2006、认证请求(AK，MAC)
Ka以及组密钥
RAND=AK⊕Kr
2007
RES，MAC'，Ka，KI
验证MAC
2008、认证响应（RES）
2009、
认证确认，该认证确认
中携带RES
2009，生成KI，完整性验证
2011、响应消息(加密后的K-
Group)
2010，验证RES
K-Group

图 20

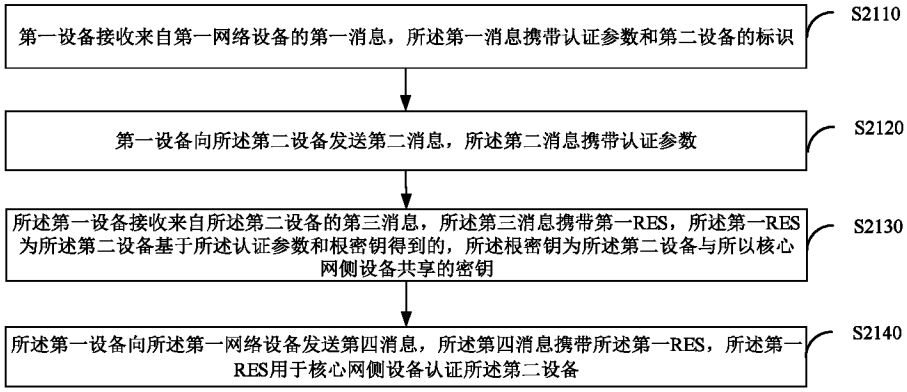

图 21

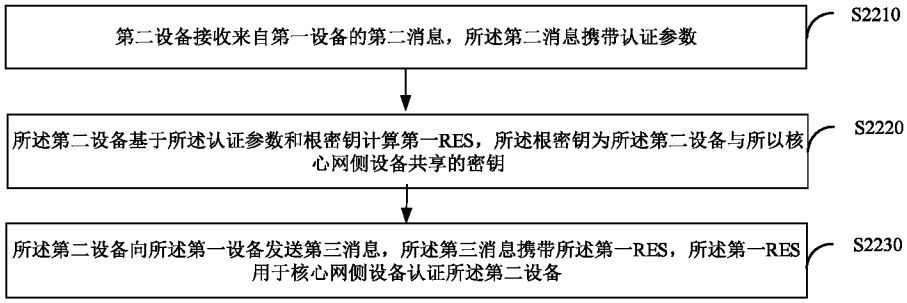

图 22

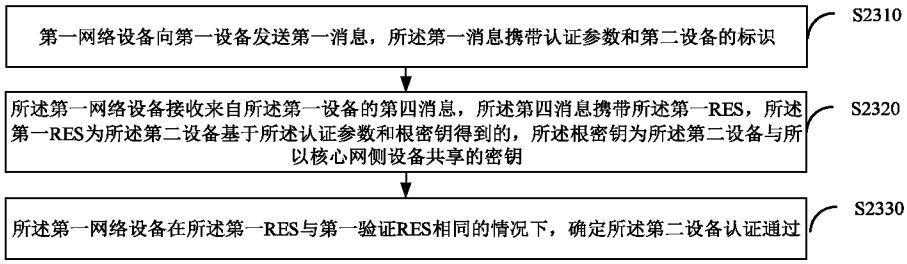

图 23

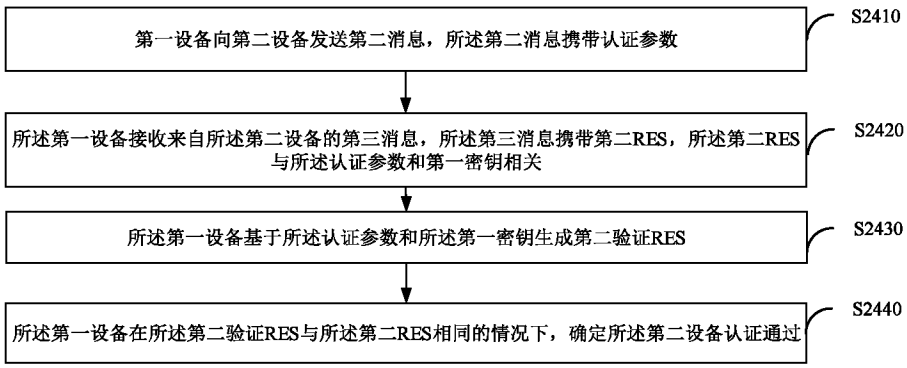

图 24

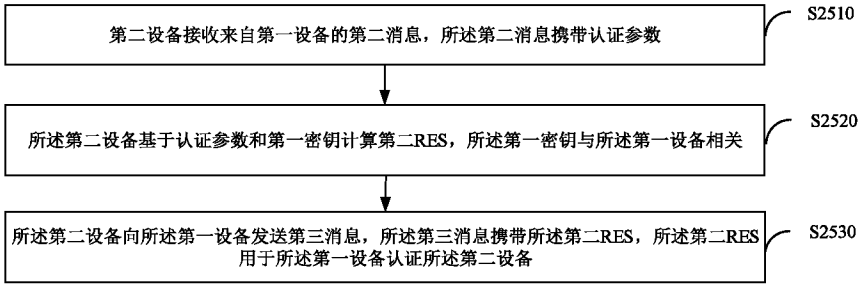

图 25

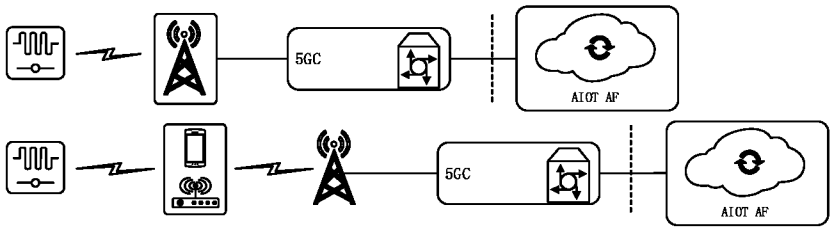

图 26

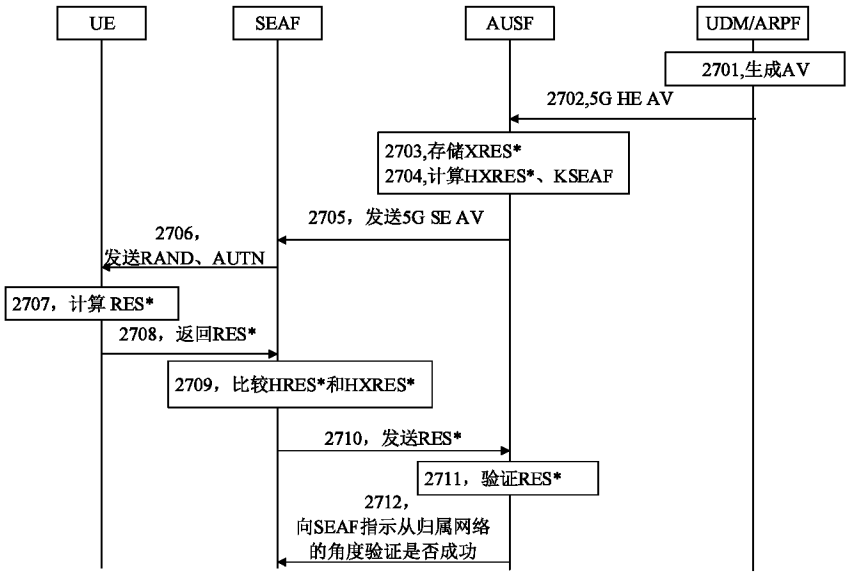

图 27

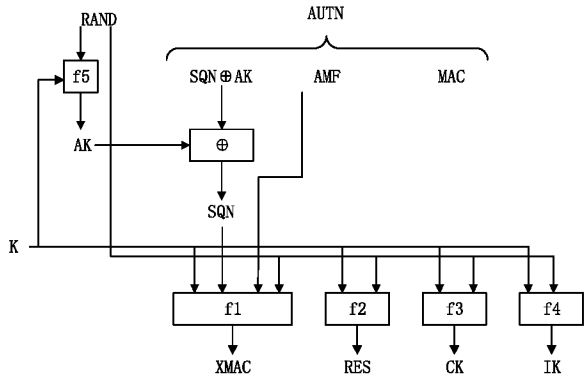

图 28

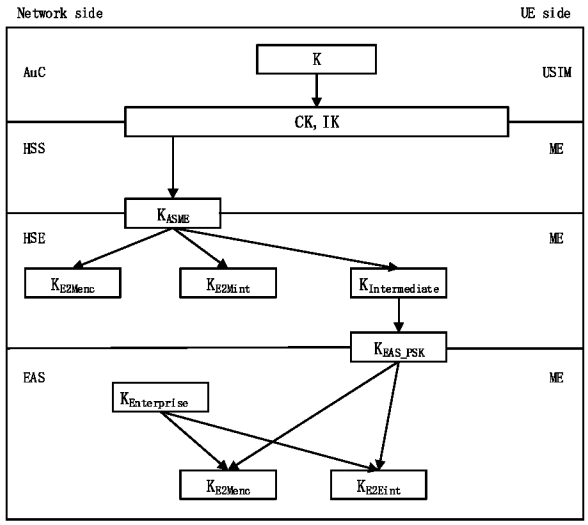

图 29

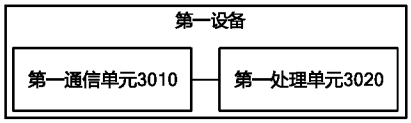

图 30

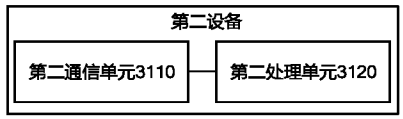

图 31

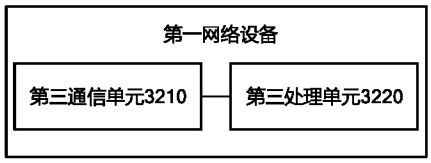

图 32

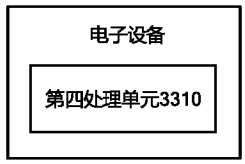

图 33

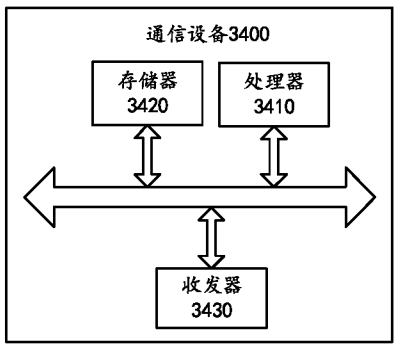

图 34

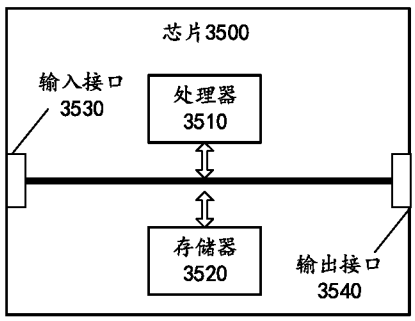

图 35

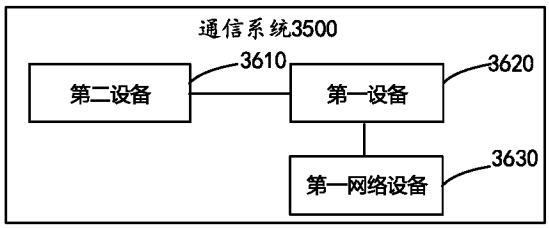

图 36

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/092602

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/06(2021.01)i; H04L9/14(2006.01)n

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)

IPC:H04W H04L

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)

3GPP, CNTXT, CNKI, ENTXT, VEN: 消息认证码, 密钥, 参数, 标识, 识别, 加密密钥, 完整性保护密钥, 随机数, MAC, key, parameter, ID, encryption key, integrity protection key, random, nonce

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111669276 A (HUAWEI TECHNOLOGIES CO., LTD.) 15 September 2020 (2020-09-15) description, paragraphs 0034, 0058-0085 and 0204-0234, and figure 2	1-10, 16-29, 36-53, 64-94, 96-103, 105-108
Y	CN 111669276 A (HUAWEI TECHNOLOGIES CO., LTD.) 15 September 2020 (2020-09-15) description, paragraphs 0034, 0058-0085 and 0204-0234, and figure 2	11-15, 30-35
X	CN 108293223 B (HUAWEI TECHNOLOGIES CO., LTD.) 17 November 2020 (2020-11-17) description, paragraphs 0114-0136 and 0234-0273	54-63, 95, 104-108
Y	CN 108293223 B (HUAWEI TECHNOLOGIES CO., LTD.) 17 November 2020 (2020-11-17) description, paragraphs 0114-0136 and 0234-0273	11-15, 30-35
A	CN 110012467 A (BEELINKER TECHNOLOGY (SUZHOU) CO., LTD.) 12 July 2019 (2019-07-12) entire document	1-108
A	CN 101039180 A (ZTE CORP.) 19 September 2007 (2007-09-19) entire document	1-108
A	CN 102625300 A (HUAWEI TECHNOLOGIES CO., LTD.) 01 August 2012 (2012-08-01) entire document	1-108

☐ 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
"D" document cited by the applicant in the international application
"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
25 January 2024	**26 January 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/092602

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The independent claims of the present application are divided into two groups, wherein independent claims 1, 19, 39, 64, 70, 78, 82, 88, 92-94 and 96-103 and corresponding claims 105-108 mainly relate to the authentication of a device, and independent claims 54, 95 and 104 and corresponding claims 105-108 mainly relate to the generation of a key. The two groups of independent claims do not have a same or corresponding special technical feature, do not have a technical relationship therebetween, do not belong to a single general inventive concept, and therefore lack unity of invention and do not comply with PCT Rule 13.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☑ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/092602

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111669276 A	15 September 2020	None	
CN 108293223 B	17 November 2020	WO 2017091959 A1	08 June 2017
CN 110012467 A	12 July 2019	None	
CN 101039180 A	19 September 2007	None	
CN 102625300 A	01 August 2012	US 2013310006 A1	21 November 2013
		US 9049594 B2	02 June 2015
		WO 2012100749 A1	02 August 2012
		EP 2663107 A1	13 November 2013
		EP 2663107 A4	26 February 2014
		EP 2663107 B1	20 November 2019

国际检索报告

国际申请号
PCT/CN2023/092602

A. 主题的分类

H04W12/06(2021.01)i；H04L9/14(2006.01)n

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)

IPC:H04W H04L

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））

3GPP,CNTXT,CNKI,ENTXT,VEN: 消息认证码，密钥，参数，标识，识别，加密密钥，完整性保护密钥，随机数，MAC，key，parameter，ID，encryption key，integrity protection key，random，nonce

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 111669276 A (华为技术有限公司) 2020年9月15日 (2020 - 09 - 15) 说明书第0034、0058-0085、0204-0234段，附图2	1-10，16-29，36-53，64-94，96-103，105-108
Y	CN 111669276 A (华为技术有限公司) 2020年9月15日 (2020 - 09 - 15) 说明书第0034、0058-0085、0204-0234段，附图2	11-15，30-35
X	CN 108293223 B (华为技术有限公司) 2020年11月17日 (2020 - 11 - 17) 说明书第0114-0136、0234-0273段	54-63，95，104-108
Y	CN 108293223 B (华为技术有限公司) 2020年11月17日 (2020 - 11 - 17) 说明书第0114-0136、0234-0273段	11-15，30-35
A	CN 110012467 A (苏州博联科技有限公司) 2019年7月12日 (2019 - 07 - 12) 全文	1-108
A	CN 101039180 A (中兴通讯股份有限公司) 2007年9月19日 (2007 - 09 - 19) 全文	1-108
A	CN 102625300 A (华为技术有限公司) 2012年8月1日 (2012 - 08 - 01) 全文	1-108

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2024年1月25日	2024年1月26日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 傅琦 电话号码 (+86) 010-62411842

第III栏　　缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明，即：

本申请的独立权利要求分为2组，独立权利要求1、19、39、64、70、78、82、88、92-94、96-103、及相应的105-108主要涉及设备的认证；独立权利要求54、95、104、及相应的105-108主要涉及密钥的生成。这2组独立权利要求之间都没有相同或相应的特定技术特征，技术上互不关联，不属于一个总的发明构思，因此不具备单一性，不符合PCT条约实施细则第13条的规定。

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。

2. ☑ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。

3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求：

4. ☐ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是：

对异议的意见

☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。

☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。

☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/092602

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	111669276	A	2020年9月15日	无			
CN	108293223	B	2020年11月17日	WO	2017091959	A1	2017年6月8日
CN	110012467	A	2019年7月12日	无			
CN	101039180	A	2007年9月19日	无			
CN	102625300	A	2012年8月1日	US	2013310006	A1	2013年11月21日
				US	9049594	B2	2015年6月2日
				WO	2012100749	A1	2012年8月2日
				EP	2663107	A1	2013年11月13日
				EP	2663107	A4	2014年2月26日
				EP	2663107	B1	2019年11月20日