

(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 12 月 5 日 (05.12.2024)



(10) 国际公布号
WO 2024/243748 A1

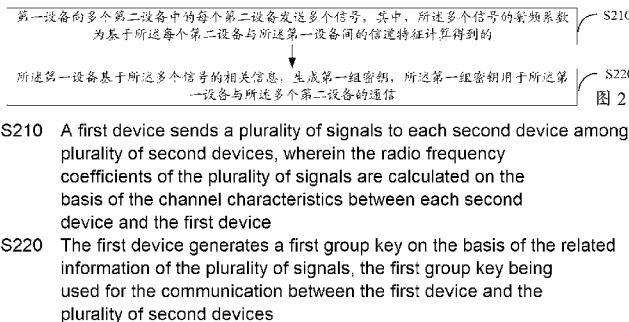
- (51) 国际专利分类号:
H04L 9/08 (2006.01)
- (21) 国际申请号: PCT/CN2023/096686
- (22) 国际申请日: 2023 年 5 月 26 日 (26.05.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: **OPPO 广东移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。
- (72) 发明人: 甘露 (**GAN, Lu**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。李猛 (**LI, Meng**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。王慧明 (**WANG, Huiming**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。赵斐斐 (**ZHAO, Feifei**); 中国广东省东莞市长安镇乌

沙海滨路 18 号, Guangdong 523860 (CN)。熊丽晖 (**XIONG, Lihui**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。石聪 (**SHI, Cong**); 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。

(54) Title: KEY GENERATION METHOD AND DEVICE

(54) 发明名称: 密钥生成方法和设备



(57) Abstract: The present application relates to a key generation method, a device, a computer readable storage medium, a computer program product, and a computer program. The method comprises: a first device sends a plurality of signals to each second device among a plurality of second devices, wherein the radio frequency coefficients of the plurality of signals are calculated on the basis of the channel characteristics between each second device and the first device; and the first device generates a first group key on the basis of the related information of the plurality of signals, the first group key being used for the communication between the first device and the plurality of second devices.

(57) 摘要: 本申请涉及一种密钥生成方法、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: 第一设备向多个第二设备中的每个第二设备发送多个信号, 其中, 所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的; 所述第一设备基于所述多个信号的相关信息, 生成第一组密钥, 所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

(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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

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。

5 背景技术

随着通信技术的发展，出现了非接触式的自动识别技术，这种技术通常是利用无线射频方式在零功耗设备和其他设备（比如读写器）之间进行非接触式数据传输。由于零功耗设备以及读写器之间的通信信道是不安全信道，因此为了保证零功耗设备的数据传输安全性，进一步提出零功耗设备和读写器之间可以采用密钥对两者之间传输的数据或信息进行加密的方案。上述方案也仅可以使得单个零功耗设备和读写器均使用相同的对密钥（或称为单播密钥或称为共享密钥），保证单个零功耗设备传输数据的安全性，而在存在多个零功耗设备的场景中，如何能够使得零功耗设备采用复杂度较低的方式生成组密钥、且保证组密钥的安全性，就成为需要解决的问题。

发明内容

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

15 本申请实施例提供一种密钥生成方法，包括：

第一设备向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的；

所述第一设备基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

20 本申请实施例提供一种密钥生成方法，包括：

目标第二设备接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；

所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

25 本申请实施例提供第一设备，包括：

第一通信单元，用于向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的；

30 第一处理单元，用于基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

本申请实施例提供目标第二设备，包括：

第二通信单元，用于接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；

35 第二处理单元，用于基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

40 本申请实施例提供一种第一设备，包括：处理器，与所述处理器通信的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，所述指令使所述第一设备执行：向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的；基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

45 本申请实施例提供一种目标第二设备，包括：处理器，与所述处理器通信的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，所述指令使所述目标第二设备执行：接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

本申请实施例提供一种芯片，用于实现上述方法。

50 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，由第一设备向每个第二设备发送多个信号，该多个信号的射频系数为基于第二设备与第一设备间的信道特征计算得到的，进而第一设备自身也会基于各个信号的相关信息生成用于与各个第二设备通信的组密钥。如此，通过对发送至不同第二设备的信号配置对应于不同第二设备的射频系数，能够准确的抵消该第二设备与第一设备之间的信道特征，即抵消该第二设备与第一设备的信道的损耗或干扰，并且仅需要基于信号的相关信息就可以生成组密钥，从而在保证降低生成组密钥的复杂度的同时，还保证了组密钥的安全性。

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密钥生成方法的示意性流程图。

图 3 是根据本申请另一实施例的密钥生成方法的示意性流程图。

图 4 是根据本申请一实施例的密钥生成方法的一种场景示意图。

图 5 是根据本申请一实施例密钥生成方法的一种示意性流程图。

图 6 是根据本申请实施例提供的密钥生成方法的仿真结果示意图。

图 7~图 8 是根据本申请一实施例密钥生成方法的另外两种示意性流程图。

图 9 是根据本申请的一实施例的第一设备的示意性框图。

图 10 是根据本申请的一实施例的目标第二设备的示意性框图。

图 11 是根据本申请实施例的通信设备示意性框图。

图 12 是根据本申请实施例的芯片的示意性框图。

图 13 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 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，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。

为了便于理解本申请实施例，下面对本申请实施例所涉及到的基本流程以及基本概念进行简单说明。应理解，下文所介绍的基本流程以及基本概念并不对本申请实施例产生限定。

图 2 是根据本申请一实施例的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。

5 S210、第一设备向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的；

S220、所述第一设备基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

10 图 3 是根据本申请另一实施例的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。

S310、目标第二设备接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；

15 S320、所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

所述第一设备为以下之一：终端设备、网络设备。该第一设备可以具备一个或多个天线，在一种优选的示例中，该第一设备可以具备多个天线。应理解的是，本实施例所提供的方案也可以应用于仅具备一个天线的设备，这里不做限定。

20 在一些实施例中，上述第一设备为终端设备，这种实施例中，第一设备和第二设备（任意一个第二设备）之间可以通过侧行链路消息进行通信。

在一些实施例中，上述第一设备可以为网络设备，比如，该网络设备可以为接入网设备（比如基站、gNB、eNB 等等任意一种），这种实施例中，该第一设备和第二设备之间可以通过 AS（接入层，Access Stratum）消息进行通信。

25 在一些实施例中，上述第一设备可以为网络设备，比如，该网络设备可以为核心网设备，这种实施例中，该第一设备和第二设备之间可以通过 NAS（非接入层，Non-Access Stratum）消息进行通信；或者，这种实施例中，该第一设备和第二设备之间可以通过接入网设备进行消息转发，本实施例不对其全部可能的消息传输方式进行穷举。另外，所述核心网侧设备包括以下至少之一：认证服务器功能（AUSF，Authentication Server Function）、统一数据管理功能（UDM，Unified Data Management）、环境供能物联网（AIoT，Ambient Power-enabled IoT）网元。在一些其他的示例中，该一个或多个核心网设备中除了上述 AUSF、UDM 和 AIoT 网元之外，还可以包括以下至少之一：

30 ARPF（Authentication credential Repository and Processing Function 认证凭证存储库和处理功能）、AMF（Access and Mobility Management Function，接入和移动性管理功能）、UPF（User Plane Function，用户平面功能）、SEAF（Security Anchor Function，安全锚点功能）等等。应理解，这里仅为示例性说明，实际处理中，核心网侧设备还可以包括核心网的其他设备，只是这里不做穷举。示例性的，上述 AIOT 网元可以指的是具备 AIOT 功能的网元，或具备零功耗相关功能的网元；该具备 AIoT 功能的网元（或具备零功耗相关功能的网元）可以是具备 AIOT 功能（或具备零功耗设备相关服务供能）的核心网网元，或者服务于 AIOT 功能（或服务于零功耗设备）的核心网网元，或者至少具备 AIoT 功能（比如至少具备 AIOT（或零功耗设备）组密钥生成供能）的核心网网元等等任意之一。应理解的是，该 AIOT 网元可以是单独设置的专门用于服务 AIOT 的网元（或专门服务于零功耗设备的网元），

40 也可能是已有的核心网网元中添加了 AIOT 相关功能（或服务于零功耗设备的相关功能），本实施例不对全部可能的情况进行穷举。

在一些实施例中，所述第一设备可以称为读写器（Reader）、或阅读器、或标签阅读器、或标签读写器等等，关于该第一设备全部可能的名称或可能的设备，这里不做穷举。

45 所述第二设备为零功耗设备。在一些实施例中，该零功耗设备可以为环境供能物联网（AIoT，Ambient Power-enabled IoT）设备。在一些实施例中，所述零功耗设备可以为有源零功耗设备、或无源零功耗设备、或半无源零功耗设备等等。在一些实施例中，该第二设备还可以为运算能力较低的终端。在一些可能的实施例中，该第二设备可以称为标签（Tag），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。

50 前述多个第二设备可以组成一个设备组。目标第二设备同样为零功耗设备，该目标第二设备可以为该多个第二设备中任意之一，也就是该目标第二设备可以为该多个第二设备所组成的设备组中的任意一个第二设备。

在一些可能的实施方式中，前述每个第二设备与第一设备间的信道特征，可以是在第一设备向每

个第二设备发送多个信号之前计算得到的。

在第一设备侧的处理中，先计算每个第二设备与第一设备间的信道特征。所述方法还包括：所述第一设备向所述每个第二设备发送组密钥生成信令；所述第一设备接收来自所述每个第二设备的导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号；所述第一设备基于所述每个第二设备的导频信号，计算所述每个第二设备与所述第一设备间的信道特征。其中，所述每个第二设备与所述第一设备间的信道特征可以组成信道特征矩阵。

以多个第二设备中任意一个第二设备为目标第二设备来说，该目标第二设备的处理中，所述方法还包括：所述目标第二设备接收来自所述第一设备的组密钥生成信令；所述目标第二设备向所述第一设备发送导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号，所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。需要指出，这里仅是以目标第二设备进行说明，实际处理中，多个第二设备中每个第二设备均执行与目标第二设备相同的处理，本实施方式为了简洁，不对每个第二设备的处理进行一一赘述。

上述信道特征可以用于表示信号在信道的传输损耗、和/或用于表示信号在信道的传输衰减等等，比如该信道特征可以包括信道的噪声等相关参数，这里不对该信道特征所可能包含的全部可能的参数进行穷举。该信道特征，可以指的是信道还可以替换性的称为信道估计值、或替换性的称为信道估计等等，这里不对其全部可能的名称进行穷举。

该组密钥生成信令的功能可以是用于触发第二设备发送导频信号。应理解的是，该组密钥生成信令也可以具备其他功能，只是在本实施例中不对该组密钥生成信令的其他功能进行穷举以及限定。另外，该组密钥生成信令所可能携带的信息内容，本实施例不做限定。

在一些实施例中，前述第一设备可以仅具备一个天线，这种情况下，该组密钥生成信令直接由该天线发射。

在一些实施例中，前述第一设备可以具备多个天线，该组密钥生成信令可以通过该第一设备的指定天线发送的，该指定天线可以根据实际情况预先配置或预先设置，比如将该第一设备的多个天线按照位置或处理顺序或逻辑顺序或其他顺序排列为第一根天线~第M根天线（M为大于或等于2的整数），该指定天线可以根据实际情况指定为第一根天线，也就是组密钥生成信令可以由该第一设备的第一根天线发射的；这里仅为示例性说明，实际处理中只要指定M根天线中任意一个天线发送该组密钥生成信令就在本实施例保护范围内，这里不做全部可能情况的穷举。

在一些实施例中，组密钥生成信令可以是广播或组播发送的，也就是该第一设备向多个第二设备广播或组播该组密钥生成信令，以使得每个第二设备均可以收到该组密钥生成信令。在一些实施例中，组密钥生成信令可以是单播发送的，也就是该第一设备向每个第二设备分别发送该组密钥生成信令。

以多个第二设备中任意一个第二设备为目标第二设备来说，该目标第二设备向所述第一设备发送导频信号可以为：目标第二设备将导频信号调制至该组密钥生成信令对应的连续载波并反射至第一设备。组密钥生成信令对应的连续载波，可以指的是：该组密钥生成信令为连续载波，或者该组密钥生成信令由连续载波的形式发送的，或该组密钥生成信令由连续载波承载的。

在一些实施例中，前述多个第二设备中每个第二设备可以按照防碰撞机制向第一设备发送导频信号。该防碰撞机制可以是预先在每个第二设备中配置的。该防碰撞机制可以为时隙防碰撞机制、或时间单元防碰撞机制、或频域防碰撞机制等等。举例来说，该防碰撞机制可以使得每个第二设备确定在接收到组密钥生成信令后的延时时间单元，该延时时间单元用于各个第二设备确定发送导频信号的发送时间单元、且不同的第二设备所对应的延时时间单元可能相同也可能不同。该时间单元可以是时隙、符号、毫秒、微秒等等任意一种时间单元，这里不做穷举。还应指出，以上仅为示例性说明，实际处理中，该防碰撞机制还可以使得每个第二设备确定导频信号的发送频率范围，且不同的第二设备对应的发送频率范围可能相同或不同；另外，该防碰撞机制也可以使得每个第二设备确定对应的延时时间单元和/或导频信号的发送频率范围，只要使得不同第二设备所发送的导频信号可以在时域和/或频域上避免相互干扰，就在本实施例保护范围内，这里不对该防碰撞机制的全部可能的内容进行穷举。

在一些实施例中，前述第一设备具备多个天线。

所述第一设备接收来自所述每个第二设备的导频信号，可以指的是第一设备通过多个天线中的每个天线接收来自每个第二设备的导频信号。所述第一设备基于所述每个第二设备的导频信号，计算所述每个第二设备与所述第一设备间的信道特征，指的是：所述第一设备基于所述每个第二设备的导频信号，计算所述每个第二设备与所述第一设备的每个天线之间的信道特征。

以任意一个第二设备为目标第二设备为例，该第一设备通过多个天线中的每个天线接收来自每个

第二设备的导频信号,指的是:第一设备通过多个天线中的每个天线接收来自目标第二设备的导频信号。所述第一设备基于所述每个第二设备的导频信号,计算所述每个第二设备与所述第一设备的每个天线之间的信道特征,指的是:所述第一设备基于多个天线中的每个天线所接收的来自目标第二设备的导频信号,计算所述目标第二设备与所述第一设备的每个天线之间的信道特征。

以多个第二设备为多个 tag、目标第二设备为多个 tag 中的 tag1,第一设备为 reader、且 reader 具备 M 个天线为例,该 reader 的 M 个天线中每个天线接收到 tag1 反射的导频信号,可以表示为:
 $[y_1^1 \cdots y_M^1] = ref * s[h_1^1 h_1^1 \cdots h_1^1 h_M^1]$,其中, ref 为 tag 反射系数, ref 的具体取值在 reader 端已知; s 表示 tag 发出的导频信号(比如可以是 reader 和 tag 双方已知内容和/或格式的导频信号), y_m^n 表示 reader 的第 m 根天线(或第 m 个天线)接收的第 n 个 tag 反射的导频信号; h_m^n 表示 reader 第 m 个(或第 m 根)天线与第 n 个 tag 之间的信道特征; $1 \leq m \leq M$ 、 $1 \leq n \leq N$, N 为设备组中全部 tag 的数量, N 为大于或等于 2 的整数, M 为前述 reader 的天线的数量, M 为大于或等于 2 的整数。上述公式中 n 等于 1,也就是 s 表示 tag1 发出的导频信号, y_m^1 表示 reader 的第 m 根天线接收的第 1 个 tag 反射的导频信号; h_m^1 表示 reader 第 m 个(或第 m 根)天线与第 1 个 tag 之间的信道特征。本示例中,该 reader 可以首先通过第 1 根天线(即第 1 根天线为前述指定天线)发送前述组密钥生成信令、且导频信号是在组密钥生成信令对应的连续载波上调制至并反射的,因此该第 1 根天线与第 1 个 tag 之间的信道特征,会对 reader 的每根天线接收到的第 1 个 tag 反射的导频信号产生影响,基于此,上述公式中, h_1^1 (即 reader 的第 1 根天线与第 1 个 tag 之间的信道特征)需要与每个 h_m^1 相乘。

进一步,由于 reader 侧上述公式中的 ref 已知, s 可以是 reader 和 tag 双方已知内容和/或格式的导频信号,因此 reader 可以通过上述公式计算得到 tag_1 与 reader 的每个天线之间的信道特征,比如可以表示为 $[h_1^1 \ h_2^1 \ \cdots \ h_M^1]$ 。

以上仅是以一个 tag1 为例进行的示例性说明, reader 可以对每个 tag 均执行上述处理,最终该 reader 可以得到每个 tag 与 reader 间的信道特征,然后该 reader 可以将每个 tag 与 reader 间的信道特征

组成信道特征矩阵,比如可以表示为以下矩阵形式: $H = \begin{bmatrix} h_1^1 & \cdots & h_M^1 \\ \vdots & \vdots & \vdots \\ h_1^N & \cdots & h_M^N \end{bmatrix}$,其中, H 表示 reader 得到

的全部 tag 中每个 tag 与 reader 的多个天线之间的信道特征矩阵,关于该信道特征矩阵中的 h_m^n 的说明,与前述实施例相同,不做重复说明。

应理解的是,以上是以第一设备具备多个天线为例进行的示例性说明,在一些可能的实施例中,前述第一设备仅具备一个天线,这种情况下,所述第一设备接收来自所述每个第二设备的导频信号,可以指的是第一设备通过该天线接收来自每个第二设备的导频信号。比如,以第二设备为 tag、目标第二设备为多个 tag 中的 tag1,第一设备为 reader、且第一设备具备 1 个天线为例,该 reader 的 1 个天线接收到 tag1 反射的导频信号,可以表示为: $[y_1^1] = ref * s[h_1^1 h_1^1]$,其中, ref 和 s 的说明与前述实施例相同,不做赘述; y_1^n 表示 reader 的 1 根天线接收的第 n 个 tag 反射的导频信号; h_1^n 表示 reader 的 1 根天线与第 n 个 tag 之间的信道特征; $1 \leq n \leq N$, N 为大于或等于 2 的整数,上述公式中 n 等于 1,也就是 s 表示 tag1 发出的导频信号,关于该公式中各个内容的含义与前述示例相似,不做重复说明。在这种实施例中,所述第一设备基于所述每个第二设备的导频信号,计算所述每个第二设备与所述第一设备间的信道特征,可以指的是:所述第一设备基于所述每个第二设备的导频信号,计算所述每个第二设备与所述第一设备的一个天线之间的信道特征;进而第一设备可以将所述每个第二设备与所述第一设备的一个天线之间的信道特征组成信道特征矩阵,比如该信道特征矩阵可以表示为: $H = \begin{bmatrix} h_1^1 \\ \vdots \\ h_1^N \end{bmatrix}$,

其中, H 表示 reader 得到的全部 tag 中每个 tag 与 reader 间的信道特征矩阵,关于该信道特征矩阵中的 h_1^n 的说明,与前述实施例相同,不做重复说明。

第一设备在得到上述信道特征之后,可以计算射频系数。所述方法还包括:所述第一设备基于所述每个第二设备与所述第一设备间的信道特征,计算一个或多个射频系数,其中,所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

任意一个射频系数的作用可以是用于抵消对应的信道特征(比如用于抵消信号在信道中的传输衰减或传输损耗等等),进而使得在该信道上传输至对应的第二设备的信号与第一设备所发出的信号相同或基本相同,这里不对该射频系数全部可能的作用或功能进行穷举。示例性的,射频系数还可以称为天线权系数、或天线系数、或天线射频发射系数、或射频发送系数、或增益系数、或发射权重系数等等,这里不对其全部可能的名称进行穷举。

在一些实施例中，设备组中的多个第二设备可以划分为一个或多个分组。所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备。

本实施例中，第一设备会计算每个分组（即每组第二设备）对应的射频系数。关于不同分组所对应的射频系数是否相同，本实施例不做限定。在下文中，任意一个分组、第二设备的任意一个分组、任意一组第二设备、任意一个分组中的第二设备均表示相同的含义，不做重复说明。需要注意的是，任意一组第二设备与设备组含义不同，设备组（或设备组中的多个第二设备）表示设备组中的全部第二设备，而任意一组第二设备则为该设备组内的任意一个分组、或设备组内的任意一个分组中的每个第二设备，也就是在下文中涉及到组的概念时，只要没有强调为设备组，均表示分组（即设备组内的第二设备分组），下文不做重复解释。

以任意一个分组为第 k 组第二设备（ k 为正整数）为例，所述第一设备基于所述每个第二设备与所述第一设备间的信道特征，计算一个或多个射频系数，可以为：该第一设备基于第 k 组第二设备中每个第二设备与第一设备间的信道特征组成第 k 组信道矩阵，计算该第 k 组信道矩阵的右逆矩阵，基于该第 k 组信道矩阵的右逆矩阵计算一个或多个射频系数中的第 k 个射频系数，该第 k 个射频系数对应于第 k 组第二设备。

关于前述设备组中的全部第二设备所能够得到的分组的数量，可以是等于设备组中第二设备的数量与第一设备的天线数量相除后向上取整；比如，可以表示为 $K = \text{ceil}(N/M)$ ，或者，

$K = \lceil N/M \rceil$ ，其中， $\text{ceil}()$ 表示向上取整， $\lceil \cdot \rceil$ 也表示向上取整，两者只是在不同计算工具中使用，公式中 N 和 M 的含义与前述实施例相同，不做赘述， K 表示分组的数量， K 为大于或等于 1 的整数。前述一个或多个射频系数的数量，与前述分组的数量相同均可以为 K 。也就是说，第 k 个射频系数可以与第 k 组第二设备具备对应关系，且 k 大于等于 1 且小于等于 K 。

该第一设备基于第 k 组第二设备中每个第二设备与第一设备间的信道特征组成第 k 组信道矩阵，可以是，将前述每个第二设备与第一设备间的信道特征矩阵中的第 k 组第二设备中每个第二设备对应的信道特征提取出来，组成第 k 组信道矩阵。

其中，第 k 组信道矩阵可以包括：第 $(k-1)M+1$ 个第二设备至第 $(k-1)M+M$ 个第二设备的信道特征。

$$H_k = \begin{bmatrix} H((k-1)M+1) \\ \vdots \\ H((k-1)M+M) \end{bmatrix};$$

举例来说，第 k 组信道矩阵可以表示为 $(1 \leq k \leq K)$ ：表示 H （信道特征矩阵）中的第 x 行， x 等于 $(k-1)M+1$ 时为 H 中的第 $(k-1)M+1$ 行，即第 $(k-1)M+1$ 个第二设备对应的信道特征， x 等于 $(k-1)M+M$ 时为 H 中的第 $(k-1)M+M$ 行，也就是第 $(k-1)M+M$ 个第二设备对应的信道特征。

$$H = \begin{bmatrix} h_1^1 & h_2^1 \\ \vdots & \vdots \\ h_1^4 & h_2^4 \end{bmatrix}$$

再举例来说，假设 N 等于 4， M 等于 2，则

下，第 1 组信道矩阵 $H_1 = \begin{bmatrix} H(1) \\ H(2) \end{bmatrix}$ ，其中， $H(1) = [h_1^1 \ h_2^1]$ ， $H(2) = [h_1^2 \ h_2^2]$ ，以此类推可以得到

$H_2 = \begin{bmatrix} H(3) \\ H(4) \end{bmatrix}$ ，不再对其进行重复说明。

所述计算该第 k 组信道矩阵的右逆矩阵可以采用以下公式计算： $H_k^{inv} = H_k^H (H_k H_k^H)^{-1}$ ，其中，

H_k^{inv} 表示第 k 组信道矩阵的右逆矩阵， H_k 表示第 k 组信道矩阵， H_k^H 则表示第 k 组信道矩阵的转置矩阵。

所述基于该第 k 组信道矩阵的右逆矩阵计算一个或多个射频系数中的第 k 个射频系数，可以指的是：将该第 k 组信道矩阵的右逆矩阵的所有列相加，得到一个或多个射频系数中的第 k 个射频系数。举例来说，得到第 k 个射频系数可以采用以下公式表示： $w_k = \text{sum_column}(H_k^{inv})$ ，其中， w_k 表示第 k 个射频系数， $\text{sum_column}()$ 表示将矩阵 H_k^{inv} 的所有列相加。

5 在一些实施例中，所述第一设备向多个第二设备中的每个第二设备发送多个信号，可以指的是：所述第一设备基于所述一个或多个射频系数中的第 k 个射频系数，向第 k 组第二设备中的每个第二设备发送所述多个信号，其中，所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备，所述第 k 组第二设备为所述多个第二设备的一个或多个分组之一， k 为正整数。也就是，第一设备将该多个信号中的第 i 个信号依次采
10 用 K 组第二设备中的每个第二设备分组分别对应的射频系数，依次向每组第二设备发送第 i 个信号， i 为正整数。比如，多个第二设备为 N 个， N 个第二设备划分成 K 组，则第一设备在生成多个信号中的第 i 个信号的情况下，依次采用 K 组第二设备中每组第二设备分别对应的射频系数，向每组第二设备发送该第 i 个信号；然后第一设备生成多个信号的第 $i+1$ 个信号的情况下，同样依次采用 K 组第二设备中每组第二设备分别对应的射频系数，向每组第二设备发送该第 $i+1$ 个信号。也就是在第一设备侧
15 第 i 个信号会发送 K 次、且不同次会发向不同组的每个第二设备，从而使得每个第二设备均可以接收到相同的第 i 个信号；相应的，在任意一个第二设备侧接收一次第 i 个信号。

以任意一个第二设备为目标第二设备、目标第二设备为 tag_n 来说，该 tag_n 接收到的第 i 个信号，可以表示为 $r_i H_k w_k$ ，其中， r_i 为第 i 个信号，其他内容的含义与前述实施例相同；由于通过射频系数 w_k 可以抵消掉 H_k ，因此在 tag_n 接收到的信号应为 r_i ，也就是 6，其中， $I_{k \times n \times 1}$ 表示 $k \times n$ 行 1 列的单位
20 向量， $k \times n$ 表示 H_k 的行数，即第 k 组 tag 中 tag 的个数，也就是第 k 组 tag 中所有的 tag （每个 tag ）都会接收到 r_i 。

在一些实施例中，若相干时间很长、即信道环境处于静态环境，则第一设备无需重复执行前述第一设备向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、和计算每组第二设备对应的射频系数的处理。也就是第一设备计算得到每个射频系数之后，可以
25 执行向每组第二设备内的第二设备发送多个信号的处理，并且针对相同组的第二设备采用相同的射频系数发送多个信号中的不同信号。

若相干时间较短、也就是信道环境时变，则第一设备可以重复前述处理。比如，若要执行发送第 i 个信号的处理，则第一设备需要执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每组第二设备对应的射频系数（即每个射频系数）的处理，然
30 后基于每组第二设备对应的射频系数，向每组第二设备发送第 i 个信号；若要执行发送第 $i+1$ 个信号的处理，则第一设备再次执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、和计算每组第二设备对应的射频系数的处理，然后基于每组第二设备对应的射频系数，向每组第二设备发送第 $i+1$ 个信号。

若相干时间较短、也就是信道环境时变，则第一设备还可以根据具体的相干时长，来确定何时重复执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每组第二设备对应的射频系数的处理。比如，相干时长内可以向每组第二设备分别发送 A 个
35 信号（ A 可以为大于或等于 1 的整数），则在完成发送第 1~第 A 个信号之后、向每组第二设备发送第 $A+1$ 个信号之前，再次执行向所述每组第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每组第二设备对应的射频系数的处理，然后基于每组第二设备对应的射频系数，向每组第二设备分别发送第 $A+1$ 个信号，下一次循环依此类推，在向每组第二设备发送第
40 $2A+1$ 个信号之前，再次执行前述计算每个射频系数的处理，依此类推不做赘述。

该相干时间较长或相干时间较短，可以是基于预先设置的时长门限值来确定的，比如，该相干时间大于时长门限值的情况下，该相干时间较长，即信道环境处于静态环境，该相干时间小于或等于时长门限值的情况下，该相干时间较短，即信道环境时变。该时长门限值可以根据实际情况配置，比
45 如，可以与设备组中实际包含的第二设备的数量相关、和/或与发送一次信号所需的时长相关等等，这里不对确定该时长门限值的全部可能的参数以及其确定方式进行限定。

另外，前述相干时间也可以称为相干时长，该相干时间可以根据实际情况确定的，本实施例不对该相干时间的获取或确定方式进行限定，只要在执行本实施例提供的全部方案之前，在第一设备侧可以预先得到该相干时间，就在本实施例保护范围内。

50 在一些实施例中，第一设备会计算每个第二设备对应的一个射频系数。关于不同第二设备所对应的射频系数是否相同，本实施例不做限定。

以任意一个第二设备为目标第二设备为例, 该第一设备可以是对目标第二设备与第一设备间的信道特征求右逆矩阵, 基于该右逆矩阵计算该目标第二设备所对应的射频系数。其中, 基于该右逆矩阵计算该目标第二设备所对应的射频系数, 可以指的是: 将该右逆矩阵的所有列相加得到该目标第二设备所对应的射频系数。

比如, 以目标第二设备为 tag_n (或第 n 个 tag)、第一设备为 reader 为例, 对 tag_n 与第一设备间的信道特征求右逆矩阵可以采用以下公式计算: $H_n^{inv} = H_n^H (H_n H_n^H)^{-1}$, 其中, n 表示 tag 的编号或序号, 在本示例中 n 可以等于 1, H_n^{inv} 表示右逆矩阵, H_n 表示第 n 个 tag 与 reader 间的信道特征矩阵, H_n^H 则表示第 n 个 tag 与 reader 间的信道特征矩阵的转置矩阵。以前述 n 具体取值为 1 为例, 也就是 tag₁ 与 reader 间的信道特征可以表示为 H_1 , 具体的 $H_1 = [h_1^1 \ h_1^2 \ \dots \ h_1^M]$, 或者, $H_1 = [h_1^1]$, 关于前述公式中包含的各个内容的含义与前述实施例相同, 不做赘述。

进一步, 将该右逆矩阵的所有列相加得到该 tag_n 所对应的射频系数, 可以表示为: $w_n = \text{sum_column}(H_n^{inv})$, 其中, w_n 表示 tag_n 所对应的射频系数, $\text{sum_column}()$ 表示将矩阵 H_n^{inv} 的所有列相加。

在一些实施例中, 所述第一设备向多个第二设备中的每个第二设备发送多个信号, 可以指的是: 第一设备将该多个信号中的第 i 个信号依次采用每个第二设备分别对应的射频系数, 依次向每个第二设备发送第 i 个信号, i 为正整数。比如, 多个第二设备为 N 个 (N 为大于或等于 2 的整数), 则第一设备在生成多个信号中的第 i 个信号的情况下, 依次采用 N 个第二设备中每个第二设备分别对应的射频系数, 向每个第二设备发送该第 i 个信号; 然后第一设备生成多个信号的第 i+1 个信号的情况下, 同样依次采用 N 个第二设备中每个第二设备分别对应的射频系数, 向每个第二设备发送该第 i+1 个信号。也就是在第一设备侧第 i 个信号会发送 N 次、且不同次会发向不同的第二设备, 从而使得每个第二设备均可以接收到相同的第 i 个信号; 相应的, 在任意一个第二设备侧接收一次第 i 个信号。

以任意一个第二设备为目标第二设备、目标第二设备为 tag_n 来说, 该 tag_n 接收到的第 i 个信号, 可以表示为 $r_i H_n w_n$, 其中, r_i 为第 i 个信号, 其他内容的含义与前述实施例相同; 由于通过射频系数 w_n 可以抵消掉 H_n , 因此在 tag_n 接收到的信号应为 r_i , 也就是 $r_i H_n w_n = r_i I_{n \times 1}$, 其中, $I_{n \times 1}$ 表示 $n \times 1$ 行 1 列的单位向量, $n \times 1$ 表示 H_n 的行数, 即 tag 的个数, 在本实施例中 $n \times 1$ 为 1, 因为本实施例中一个 tag 对应一个 H_n 。

在一些实施例中, 若相干时间很长、即信道环境处于静态环境, 则第一设备无需重复执行前述第一设备向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、和计算每个第二设备对应的射频系数的处理。也就是第一设备计算得到每个第二设备对应的射频系数之后, 可以执行向多个第二设备中的每个第二设备发送多个信号的处理, 针对相同的第二设备采用相同的射频系数发送多个信号中的不同信号。

若相干时间较短、也就是信道环境时变, 则第一设备可以重复前述处理。比如, 若要执行发送第 i 个信号的处理, 则第一设备需要执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每个第二设备对应的射频系数的处理, 然后基于每个第二设备对应的射频系数, 向每个第二设备发送第 i 个信号; 若要执行发送第 i+1 个信号的处理, 则第一设备再次执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、和计算每个第二设备对应的射频系数的处理, 然后基于每个第二设备对应的射频系数, 向每个第二设备发送第 i+1 个信号。

若相干时间较短、也就是信道环境时变, 则第一设备还可以根据具体的相干时长, 来确定何时重复执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每个第二设备对应的射频系数的处理。比如, 相干时长内可以向每个第二设备发送 B 个信号 (B 可以为大于或等于 1 的整数), 则在完成发送第 1~第 B 个信号之后、向每个第二设备发送第 B+1 个信号之前, 再次执行向所述每个第二设备发送组密钥生成信令至计算所述每个第二设备与所述第一设备间的信道特征、计算每个第二设备对应的射频系数的处理, 然后基于每个第二设备对应的射频系数, 向每个第二设备发送第 A+1 个信号, 下一次循环以此类推, 不做赘述。

关于该相干时间的说明与前述实施例为相同, 不做重复说明。

在一些可能的实施方式中, 所述第一设备基于所述多个信号的相关信息, 生成第一组密钥, 包括: 所述第一设备基于所述多个信号的相关信息, 得到多个第一量化结果; 所述第一设备基于所述多个第一量化结果, 生成所述第一组密钥。

在前述实施例所说明的第一设备向每个第二设备发送多个信号的处理中, 以任意一个信号为第 i 个信号为例, 第一设备可以是基于不同的第二设备的射频系数向不同的第二设备发送第 i 个信号, 也

可以是基于不同组对应的射频系数向不同组的每个第二设备发送第 i 个信号, 关于第 i 个信号发送的次数取决于第二设备的数量、或分组的数量, 但是无论哪种方式, 第一设备自身均可以得到第 i 个信号的相关信息, 也就是第一设备自身可以得到每个信号的相关信息。

仍然以任意一个信号为第 i 个信号为例, 所述第一设备基于所述多个信号的相关信息, 得到多个第一量化结果, 包括: 所述第一设备基于所述多个信号中第 i 个信号的相关信息, 确定所述第 i 个信号对应的第一量化范围, 将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第 i 个第一量化结果, 其中, 所述第一量化范围为多个第一候选量化范围中之一, 所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值, i 为正整数。

需要指出, 第一设备针对每个信号都执行与第 i 个信号相同的处理, 最终可以得到多个量化结果, 本实施例以第 i 个信号进行详述, 不再对每个信号进行一一赘述。

在一些实施例中, 所述第一设备的处理还可以包括: 所述第一设备可以基于多个信号的相关信息, 确定相关信息取值范围的最大值和最小值; 基于量化阶数 Q , 将相关信息取值范围划分为 Q 个第一候选量化范围, 并确定 Q 个第一候选量化范围中每个第一候选量化范围对应的第一候选量化值, Q 为大于或等于 2 的整数。

这里, 所述量化阶数 Q 可以根据实际情况设置, 比如可以是 16、32、8、4、5、21 或更大或更小, 这里不对 Q 全部可能的取值进行穷举。前述每个第一候选量化范围对应的第一候选量化值可以根据实际情况设置, 任意一个第一候选量化值可以为二进制的, 且第一候选量化值的长度可以与量化阶数相关, 比如第一候选量化值的长度可以等于 $\log_2 Q$ 个比特 (bit)。示例性的, 第一候选量化值可以为长度为 $\log_2 Q$ 的格雷码。

所述第一设备基于所述多个信号中第 i 个信号的相关信息, 确定所述第 i 个信号对应的第一量化范围, 将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第 i 个第一量化结果, 可以指的是: 所述第一设备确定所述多个信号中第 i 个信号的相关信息, 在 Q 个第一候选量化范围中所对应的第一量化范围, 将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第 i 个第一量化结果。应理解的是, 前述确定 Q 个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值可以仅执行一次, 然后可以基于前述 Q 个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值, 分别确定每个信号的相关信息所对应的量化结果, 这里不做一一赘述。

在一些实施例中, 为了减少量化边界左右微小误差导致的量化结果的不同, 第一设备还可以对所有获取的信号的相关信息就近取整, 再确定前述 Q 个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值; 和/或, 在对每个信号进行量化的处理时, 也可以对每个信号的相关信息就近取整, 然后进行量化。

需要指出, 前述实施例仅为对多个信号的相关信息进行量化的一种示例性说明, 实际处理中, 本实施例可以使用的量化方法可以不局限于此处所述的方法, 比如还可以采用奇异值分解的方法、还可以为其他量化方法, 本实施例不对其进行限定和穷举。

在一些实施例中, 所述多个信号的相关信息, 包括以下至少之一: 所述多个信号中每个信号的强度、所述每个信号的相位。

需要指出, 每个信号的强度也可以替换性描述为每个信号的幅度。

举例来说, 前述多个信号的相关信息包括每个信号的强度。则所述第一设备的处理还可以包括: 所述第一设备基于每个信号的强度 P , 确定全部信号的强度取值范围 (即 P 的取值范围) 的最大值 ($P_{\max}$) 和最小值 ($P_{\min}$), 也就是 $P_{\min} \leq P \leq P_{\max}$; 然后基于量化阶数 Q , 将 P 的取值范围划分为 Q 个第一候选量化范围, 并确定 Q 个第一候选量化范围中每个第一候选量化范围对应的长度为 $\log_2 Q$ 的格雷码。为了减少量化边界左右微小误差导致的量化结果的不同, 第一设备还可以对所有获取的信号强度 P 就近取整, 再确定前述 Q 个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值; 和/或, 在对每个信号进行量化处理时, 也可以对每个信号的强度 P 就近取整, 然后进行量化。这种示例中, Q 个第一候选量化范围还可以称为 Q 个第一候选强度量化范围。在一些可能的示例中, 所述第一设备发送每个信号时, 发送的可以是每个信号的强度的相关值, 比如, 可以是信号的强度的开平方值、或信号的强度的原值、或信号的强度的开多次方值等等, 这里不对其全部可能的情况进行穷举。

举例来说, 前述多个信号的相关信息包括每个信号的相位。则所述第一设备的处理还可以包括: 所述第一设备基于每个信号的相位 φ , 确定全部信号的相位取值范围 (即 φ 的取值范围) 的最大值

($\varphi_{\max}$) 和最小值 ($\varphi_{\min}$), 也就是 $\varphi_{\min} \leq \varphi \leq \varphi_{\max}$; 然后基于量化阶数 Q , 将 φ 的取值范围划分为 Q 个第一候选量化范围, 并确定 Q 个第一候选量化范围中每个第一候选量化范围对应的长度为 $\log_2 Q$

的格雷码。为了减少量化边界左右微小误差导致的量化结果的不同，第一设备还可以对所有获取的信号相位 φ 就近取整，再确定前述Q个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值；和/或，在对每个信号进行量化处理时，也可以对每个信号的相位 φ 就近取整，然后进行量化。这种示例中，Q个第一候选量化范围还可以称为Q个第一候选相位量化范围。

5 应理解，以上仅为示例性说明，实际处理中，可以将每个信号的强度和相位结合使用，比如可以既得到Q个第一候选强度量化范围又得到Q个第一候选相位量化范围，然后第q个第一候选强度量化范围和第q个第一候选相位量化范围对应于同一个量化值，其中，q为大于等于1且小于等于Q的整数，或者q为大于等于0且小于等于Q-1个整数。在对第i个信号进行量化的时候，可以根据第i个信号的强度和相位中任意之一，来确定对应的第一量化范围，进而确定量化结果，又或者，可以将第i个信号的强度和相位均对应的第一强度量化范围和第一相位量化范围，若两者一致，则确定任意一种第一量化范围对应的第一量化值为量化结果，若两者不一致，则可以指定以其中任意之一为准，比如统一指定以信号的强度为准，这里不对全部可能的示例进行穷举。

10 在一些实施例中，所述第一设备基于所述多个第一量化结果，生成所述第一组密钥，可以为：所述第一设备基于指定顺序将所述多个第一量化结果合并，得到所述第一组密钥。

15 其中，所述指定顺序可以根据实际情况设置。在一些实施例中，该指定顺序可以是正序，也就是第一组密钥可以是“第1个第一量化结果、第2个第一量化结果...最后一个第一量化结果”这样排列后合并组成的。在一些实施例中，该指定顺序可以是倒序，也就是第一组密钥可以是“最后一个第一量化结果、倒数第2个第一量化结果...第1个第一量化结果”这样排列后合并组成的。在一些实施例中，该指定顺序可以是乱序的，比如一共有4个第一量化结果，指定顺序可以为2、4、3、1，也就是第一组密钥可以是“第2个第一量化结果、第4个第一量化结果、第3个第一量化结果、第1个第一量化结果”这样排列后合并组成的，关于这种实施例下该指定顺序可以根据实际情况来设置，这里不做穷举。应理解，以上也仅为示例性说明，只要保证每个第二设备和第一设备均采用相同的指定顺序，就在本实施例保护范围内。

25 在一些实施例中，所述第一设备基于所述多个第一量化结果，生成所述第一组密钥，可以为：所述第一设备基于预设计算方式对所述多个第一量化结果计算得到所述第一组密钥。

本实施例中，该预设计算方式可以根据实际情况设置，比如可以是异或计算、直连计算、函数等等任意一种或多种的组合。举例来说，可以采用异或计算，也就是将全部第一量化结果进行异或计算得到第一组密钥。再举例来说，可以采用函数计算，比如函数为密钥派生函数（KDF，Key Derivation Function），则可以将多个第一量化结果均作为KDF的输入，通过KDF计算得到第一组密钥。需要指出，以上也仅为示例性说明，只要保证每个第二设备和第一设备均采用相同的预设计算方式，就在本实施例保护范围内。

30 在一些可能的实施方式中，所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，包括：所述目标第二设备基于所述多个信号的相关信息，得到多个第二量化结果；所述目标第二设备基于所述多个第二量化结果，生成所述第二组密钥。

35 在前述实施例已经说明，目标第二设备为设备组中的全部第二设备中任意之一，关于设备组中每个第二设备的处理与目标第二设备相同，因此这里不做一一赘述。

这里将目标第二设备生成的组密钥称为第二组密钥，原因是目标第二设备基于接收到的多个信号进行第二组密钥的生成，与第一设备的执行主体不同，可能会使得目标第二设备与第一设备所得到的组密钥相同或不同，还需要进一步校验才可以确定目标第二设备生成的第二组密钥是否与第一设备生成的第一组密钥相同，因此，本实施例将目标第二设备（也就是任意一个第二设备）所生成的组密钥、与第一设备所生成的组密钥，区分表示。应理解的是，在理想状态下，目标第二设备（也就是任意一个第二设备）所生成的组密钥、与第一设备所生成的组密钥应为相同的，也就是理想状态下，第一组密钥可以等于第二组密钥。

40 在一些实施例中，所述目标第二设备基于所述多个信号的相关信息，得到多个第二量化结果，包括：所述目标第二设备基于所述多个信号中第i个信号的相关信息，确定所述第i个信号对应的第二量化范围，将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第i个第二量化结果，其中，所述第二量化范围为多个第二候选量化范围中之一，所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值，i为正整数。需要指出，目标第二设备针对每个信号都执行与第i个信号相同的处理，最终可以得到多个量化结果，本实施例以第i个信号进行说明，不再对每个信号进行一一赘述。

50 在一些实施例中，所述目标第二设备的处理还可以包括：所述目标第二设备可以基于多个信号的相关信息，确定相关信息取值范围的最大值和最小值；基于量化阶数Q，将相关信息取值范围划分为

Q 个第二候选量化范围, 并确定 Q 个第二候选量化范围中每个第二候选量化范围对应的第二候选量化值, Q 为大于或等于 2 的整数。

关于该目标第二设备确定 Q 个第二候选量化范围, 并确定 Q 个第二候选量化范围中每个第二候选量化范围对应的第二候选量化值的具体处理方式, 与前述第一设备确定 Q 个第一候选量化范围, 并确定 Q 个第一候选量化范围中每个第一候选量化范围对应的第一候选量化值的具体处理方式是相同的, 因此不做重复说明。

所述目标第二设备基于所述多个信号中第 i 个信号的相关信息, 确定所述第 i 个信号对应的第二量化范围, 将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第 i 个第二量化结果, 可以指的是: 所述目标第二设备确定所述多个信号中第 i 个信号的相关信息, 在 Q 个第二量化范围中所对应的第二量化范围, 将所述第二量化范围对应的第二量化值, 作为所述多个第二量化结果中的第 i 个第二量化结果。关于目标第二设备得到第 i 个第二量化结果的处理, 也与前述第一设备得到第 i 个第一量化结果的方式相同, 不做赘述。

在一些实施例中, 所述多个信号的相关信息, 同样包括以下至少之一: 所述多个信号中每个信号的强度、所述每个信号的相位。关于信号的相关信息为强度和/或相位的不同情况下, 目标第二设备确定 Q 个第二候选量化范围、以及每个第二候选量化范围对应的第二候选量化值的具体说明, 与前述第一设备确定 Q 个第一候选量化范围、以及每个第一候选量化范围对应的第一候选量化值的具体说明是相似的, 不做赘述。

在一些可能的示例中, 信号的相关信息为信号的强度的情况下, 目标第二设备接收每个信号时, 可以是接收每个信号的强度的相关值, 比如, 可以是信号的强度的开平方值、或信号的强度的原值、或信号的强度的开多次方值等等, 这里不对其全部可能的情况进行穷举; 相应的, 目标第二设备可以是对该每个信号的强度的相关值的平方、或原值、或多次方值, 然后再确定 Q 个第二候选量化范围、以及每个第二候选量化范围对应的第二候选量化值, 关于确定 Q 个第二候选量化范围、以及每个第二候选量化范围对应的第二候选量化值的具体处理不做赘述。

在一些实施例中, 所述目标第二设备基于所述多个第二量化结果, 生成所述第二组密钥, 可以为: 所述目标第二设备基于指定顺序将所述多个第二量化结果合并, 得到所述第二组密钥。关于其中的指定顺序的说明, 以及具体的合并处理, 均与前述第一设备基于指定顺序将所述多个第一量化结果合并, 得到所述第一组密钥的处理是相同的, 不做赘述。

在一些实施例中, 所述目标第二设备基于所述多个第二量化结果, 生成所述第二组密钥, 可以为: 所述目标第二设备基于预设计算方式对所述多个第二量化结果计算得到所述第二组密钥。关于预设计算方式的具体说明也与前述第一设备的相关说明相同, 不做重复说明。

需要指出, 无论采用前述指定顺序还是预设计算方式, 第一设备和每个第二设备均需要采用相同的方式分别生成各自的组密钥, 这里不做重复说明。

在一些可能的实施方式中, 所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列; 所述第一设备基于所述多个信号的相关信息, 生成第一组密钥, 包括: 所述第一设备基于所述多个信号中每个信号携带的密钥序列, 生成所述第一组密钥。

这里, 不同信号所携带的密钥序列, 可以是第一设备随机生成的, 关于第一设备生成每个密钥序列的方式, 本实施例不做限定。

所述多个信号中第 j 个信号携带一个或多个数据段, 所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的, j 为正整数。

在一些实施例中, 所述多个信号指的是发送至每个第二设备的多个信号。

一种情况下, 该第一设备可以是分别基于每个第二设备对应的射频系数向每个第二设备发送信号的, 也就是同一个信号内容在这种情况下会分别向每个第二设备发送, 最终发送多次。

这种情况下, 若第一设备要发送内容为第 j 个密钥序列的信号, 则需要分别发送给 N 个第二设备, N 的取值定义与前述实施例相同, 不做赘述。在发送至第 n 个第二设备的第 j 个信号中可以携带一个数据段, 该数据段为基于第 n 个第二设备的标识和第 j 个密钥序列计算的; 依次类推, 发送至第 n+1 个第二设备的第 j 个信号可以携带一个数据段, 该数据段为基于第 n+1 个第二设备的标识和第 j 个密钥序列计算的, 这里不做穷举。

其中, 计算的方式可以根据实际情况设置, 比如可以是直连计算、异或计算、函数计算中一种或多种方式。举例来说, 计算的方式为异或计算, 发送至第 n 个第二设备的第 j 个信号表示为 r_{jn} , r_{jn} 的帧结构 (也就是 r_{jn} 的数据段) 设计为: $[ID_n^k \oplus k_j]$, 其中, $\oplus$ 表示异或运算, ID_n^k 表示第 n 个 tag 的 ID 号, k_j 为 reader 端随机生成的第 j 个密钥序列。

一种情况下,该第一设备可以是分别基于每组第二设备对应的射频系数向每组第二设备中的每个第二设备发送信号的,也就是同一个信号内容在这种情况下会以分组为单位发送多次。

这种情况下,若第一设备要发送内容为第 j 个密钥序列的信号,则需要分别发送给 K 组第二设备,也就是发送 K 次,关于 K 的取值定义与前述实施例相同,不做赘述。在发送至第 k 组第二设备的第 j 个信号中可以携带一个或多个数据段,其中数据段的数量取决于第 k 组第二设备中包含的第二设备的数量;该一个或多个数据段为基于第 k 组第二设备中每个第二设备的标识分别和第 j 个密钥序列计算的。同样的,在发送至第 $k+1$ 组第二设备的第 j 个信号中也可以携带一个或多个数据段,其中数据段的数量取决于第 $k+1$ 组第二设备中包含的第二设备的数量;该一个或多个数据段为基于第 $k+1$ 组第二设备中每个第二设备的标识分别和第 j 个密钥序列计算的,依次类推,不做一一赘述。

其中,计算的方式与前述示例的说明相同,不做赘述。举例来说,计算的方式为异或计算,不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的,可以指的是,第 k 组第二设备中每个第二设备所对应的数据段为分别采用每个第二设备的标识和第 j 个密钥序列异或计算得到的。比

如,第 k 次发送第 j 个密钥序列的时候,第 k 组第二设备对应的第 j 个信号可以表示为 r_{jk} , r_{jk} 的帧结构(也就是 r_{jk} 的一个或多个数据段)设计为: $[ID_1^k \oplus k_j, ID_2^k \oplus k_j, \dots, ID_n^k \oplus k_j]$ 。其中, $\oplus$ 表示异或运算, ID_n^k 表示第 k 组 tag 中第 n 个 tag 的 ID 号(即标识), k_j 为 reader 端随机生成的第 j 个密钥序列。

在一些实施例中,所述第一设备基于所述多个信号中每个信号携带的密钥序列,生成所述第一组密钥,可以指的是:所述第一设备基于指定顺序将所述每个信号携带的密钥序列合并,得到所述第一组密钥。关于该指定顺序可以与前述实施例为相同的,不做赘述。

在一些实施例中,所述第一设备基于所述多个信号中每个信号携带的密钥序列,生成所述第一组密钥,可以指的是:所述第一设备基于预设计算方式对所述每个信号携带的密钥序列计算得到所述第一组密钥。关于该预设计算方式可以与前述实施例为相同的,不做赘述。

在一些实施方式中,所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列;所述目标第二设备基于所述多个信号的相关信息,生成第二组密钥,包括:所述目标第二设备基于所述多个信号中每个信号携带的密钥序列,生成所述第二组密钥。

其中,所述多个信号中第 j 个信号携带一个或多个数据段,所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的;所述方法还包括:所述目标第二设备从所述第 j 个信号中,提取所述目标第二设备对应的目标数据段, j 为正整数;所述目标第二设备基于所述目标第二设备的标识和所述目标数据段,计算所述第 j 个信号携带的第 j 个密钥序列。其中,计算的方式应与第一设备的计算方式相同,这里不做重复说明。

一种情况下,该第一设备可以是分别基于每个第二设备对应的射频系数向每个第二设备发送信号的。这种情况下,在第一设备发送至目标第二设备的第 j 个信号中可以携带一个数据段,该数据段为基于目标第二设备的标识和第 j 个密钥序列计算的,则目标第二设备可以从该第 j 个信号中直接提取该数据段作为目标数据段,然后基于自身的标识与目标数据段进行计算,可以得到第 j 个密钥序列。举例来说,计算的方式为异或计算,目标第二设备为第 n 个 tag,则其提取的数据段可以为

$[ID_n^k \oplus k_j]$,则第 n 个 tag 仍采用自身的 ID 与上述数据段再次进行异或,就可以得到 k_j (第 j 个密钥序列),关于上述表达式中各个内容的含义与前述示例相同,不做赘述。

一种情况下,该第一设备可以是分别基于每组第二设备对应的射频系数向每组第二设备中的每个第二设备发送信号的。这种情况下,若目标第二设备为第 k 组第二设备中之一,则目标第二设备仅会接收到第一设备第 k 次发送的第 j 个信号(即携带第 j 个密钥序列的信号),在第 k 次发送的第 j 个信号中可以携带一个或多个数据段,目标第二设备可以从该第 j 个信号中直接提取自身对应的数据段作为目标数据段,然后基于自身的标识与目标数据段进行计算,可以得到第 j 个密钥序列。

关于这种情况中,目标第二设备所对应的数据段的位置,可以是根据实际情况设置的,比如目标第二设备为第 k 组第二设备中的第 n 个第二设备,其对应的数据段的位置可以是第 n 个位置处、或者也可以是其他指定位置处,本实施例不对其进行限定,只要保证第 k 组第二设备中不同的第二设备对应的数据段的位置不同,就在本实施例保护范围内。

举例来说,计算的方式为异或计算,第一设备第 k 次发送第 j 个密钥序列的时候,第 k 组第二设备对应的第 j 个信号可以表示为 r_{jk} , r_{jk} 的帧结构(也就是 r_{jk} 的一个或多个数据段)为: $[ID_1^k \oplus k_j, ID_2^k \oplus k_j, \dots, ID_n^k \oplus k_j]$ 。假设目标第二设备为第 n 个 tag、且其对应的数据段的位置为第 n 个位置,则可以从 r_{jk} 中提取第 n 个数据段,即“ $ID_n^k \oplus k_j$ ”作为目标数据段,然后基于自身的标识 ID_n^k 与

“ $ID_n^k \oplus k_j$ ”再次进行异或计算,即可得到 k_j (第j个密钥序列),关于上述表达式中各个内容的含义与前述示例相同,不做赘述。

在一些可能的实施方式中,所述多个信号用于所述每个第二设备生成第二组密钥,所述方法还包括:所述第一设备基于所述第一组密钥,计算组密钥校验信息,其中,所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性;所述第一设备向所述每个第二设备发送第一消息,其中,所述第一消息携带所述组密钥校验信息。

以设备组中的任意一个第二设备为目标第二设备为例,该目标第二设备的处理中,所述方法还包括:所述目标第二设备接收来自所述第一设备的第一消息,其中,所述第一消息携带组密钥校验信息,所述组密钥校验信息为所述第一设备基于第一组密钥计算的,所述第一组密钥为所述第一设备基于所述多个信息生成的;所述目标第二设备基于所述第二组密钥计算验证信息;所述目标第二设备基于所述组密钥校验信息和所述验证信息,校验所述第二组密钥与所述第一组密钥的一致性。

关于每个第二设备生成第二组密钥的方式,在所述实施例中已经详述,这里不做重复说明。

本实施方式中,第一设备在得到自身的组密钥即第一组密钥之后,还可以发起校验处理,以确定各个第二设备生成的第二组密钥与自身的第一组密钥是否相同。

在一些实施例中,所述第一设备基于所述第一组密钥,计算组密钥校验信息,可以为:所述第一设备将所述第一组密钥通过第一预设函数进行映射得到第一数值,将该第一数值作为组密钥校验信息。该第一预设函数可以是哈希(hash)函数,该哈希函数所采用的具体算法,可以根据实际情况设置,本实施例不对其进行限定,另外,该第一预设函数也可以是其他类型的函数,只要通过该函数可以得到对应的映射数值,就在本实施例保护范围内。

在一些实施例中,所述第一设备基于所述第一组密钥,计算组密钥校验信息,可以为:所述第一设备计算所述第一组密钥的循环冗余校验(CRC, Cyclic Redundancy Check)码,将CRC(码)作为组密钥校验信息。该CRC计算所采用的具体算法,可以根据实际情况设置,本实施例不对其进行限定。

所述第一设备向所述每个第二设备发送第一消息的方式,可以是组播、广播或单播,均在本实施例保护范围内。在一种优选的示例中,第一设备可以是向全部第二设备广播该第一消息。

在一些实施例中,所述目标第二设备基于所述第二组密钥计算验证信息,可以为:所述目标第二设备将所述第二组密钥通过第一预设函数进行映射得到第二数值,将该第二数值作为验证信息。该第一预设函数与前述实施例相同,不做赘述。

在一些实施例中,所述目标第二设备基于所述第二组密钥计算验证信息,可以为:所述目标第二设备计算所述第二组密钥的循环冗余校验(CRC, Cyclic Redundancy Check)码,将第二组密钥的CRC(码)作为验证信息。

需要指出的是,目标第二设备(也就是任意一个第二设备)计算验证信息的具体处理方式,应与第一设备基于组密钥校验信息的方式为相同的。

在一些实施例中,所述方法还包括以下至少之一:所述目标第二设备在所述第二组密钥与所述第一组密钥一致的情况下,所述目标第二设备向所述第一设备发送第二消息,其中,所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功;所述目标第二设备在所述第二组密钥与所述第一组密钥不一致的情况下,所述目标第二设备向所述第一设备发送第三消息,其中,所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

相应的,第一设备的处理中,所述方法还包括以下之一:所述第一设备接收来自目标第二设备的第二消息,其中,所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功,所述目标第二设备为所述多个第二设备中之一;所述第一设备接收来自所述目标第二设备的第三消息,其中,所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

若第一设备接收到目标第二设备发来第二消息,则第一设备可以记录该目标第二设备为成功生成组密钥的第二设备,然后使用第一组密钥与该目标第二设备进行通信;这里,通信可以指的是基于第一组密钥对接收到的数据进行解密和/或基于第一组密钥对发送的数据进行加密。也就是说,第一设备接收到任意一个第二设备发来的第二消息的情况下,就可以确定该第二设备生成组密钥成功,记录该第二设备并与该第二设备进行通信。

同样的,若目标第二设备发送第二消息,则该目标第二设备可以使用第二组密钥与第一设备进行通信;这里,通信可以指的是基于第二组密钥对接收到的数据进行解密和/或基于第二组密钥对发送的数据进行加密。

若第一设备接收到目标第二设备发来的第三消息,则第一设备可以下一次继续向该目标第二设备执行前述处理,以使得目标第二设备生成与第一组密钥相同的第二组密钥。同样的,若目标第二设备发送第三消息,则该目标第二设备可以等待下一次生成组密钥。

在一些可能的实施方式中,所述多个信号用于所述每个第二设备生成第二组密钥,所述方法还包括:所述第一设备基于所述第一组密钥,计算组密钥纠错信息,其中,所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥;所述第一设备向所述每个第二设备发送第四消息,其中,所述第四消息携带所述组密钥纠错信息。

以设备组中的任意一个第二设备为目标第二设备为例,该目标第二设备的处理中,所述方法还包括:所述目标第二设备接收来自所述第一设备的第四消息,其中,所述第四消息携带组密钥纠错信息,所述组密钥纠错信息为所述第一设备基于第一组密钥计算的,所述第一组密钥为所述第一设备基于所述多个信息生成的;所述目标第二设备基于所述组密钥纠错信息对所述第二组密钥进行纠错,得到与所述第一组密钥一致的组密钥。

所述第一设备基于所述第一组密钥,计算组密钥纠错信息,可以是第一设备基于第二预设计算方式对所述第一组密钥,计算得到校验码,将该校验码作为组密钥纠错信息。所述目标第二设备基于所述组密钥纠错信息对所述第二组密钥进行纠错,得到与所述第一组密钥一致的组密钥,可以为:所述目标第二设备基于第二预设方式所对应的纠错方式,采用组密钥纠错信息对所述第二组密钥进行译码纠错,得到与所述第一组密钥一致的组密钥。

其中,第二预设计算方式所采用的计算函数(或计算方式)可以根据实际情况设置,比如,可以采用 LDPC (Low Density Parity-check Codes, 低密度奇偶校验码)、Turbo 译码等等任意一种或多种函数,这里不对全部可能的方式进行穷举,只要能够对序列进行编码以得到校验码,从而使得对端进行译码纠错,就在本实施例保护范围内。

在一些可能的实施方式中,所述第一设备可以触发更新组密钥。

在一些实施例中,第一设备可以周期性触发更新组密钥。该周期性的周期时长可以根据实际情况设置,比如可以是 7 天、1 天、或更长或更短,这里不对其进行穷举。

在一些实施例中,第一设备可以是在设备组中增加或减少第二设备的情况下触发更新组密钥。该第一设备确定设备组中增加或减少第二设备的方式,可以是该第一设备可以接收网络设备发来的指示信息,该指示信息用于指示设备组中新增第二设备或移除第二设备,该网络设备可以是接入网设备、或核心网设备、或应用功能(AF)等等,这里不对其进行穷举。

该第一设备更新组密钥的处理方式,可以是再次执行前述实施例所提供的方式,以使得自身以及设备组中的当前各个第二设备均更新组密钥。

结合以下多个示例,均以第一设备为 reader (读写器),设备组中总共有 N 个 tag (标签)为例,对本申请所提供的密钥生成方法进行示例性说明。该 reader 和 N 个 tag 组成的系统如图 4 所示:以 reader 为圆心, d_1 为半径的区域内,存在 N 个 tag 与 reader 进行通信。组密钥方案的目的是在 reader 与 N 个 tag 之间生成一个共知的组密钥 Gk 。同时,存在窃听者试图通过窃听组密钥生成过程中的某些信息,也获得 k 。为更接近实际场景,假设窃听者不会存在于以 reader 为圆心, d_2 为半径的区域内,称为安全区域。

结合图 5 进行一种示例说明,在图 5 涉及的方案中, N 个 tag 均为单天线设备, reader 配置有 M 根天线,具体步骤如下:

步骤 501: reader 广播发射一个组密钥生成信令,比如该组密钥生成信令可以表示为 *message1*。

步骤 502: N 个 tag 中所有 tag 收到此组密钥生成信令后,按照时隙防碰撞机制依次向 reader 反射导频信号 s 。

步骤 503: reader 依次接收每个 tag 在步骤 502 所发送的反射导频信号,估计与每个 tag 间的信道特征。

以 N 个 tag 中的 tag_1 为例,具体如下:连续载波(幅度记为 1)由 reader 的第一根天线发射出去,则 reader 接收到的 tag_1 反射导频信号为: $[y_1^1 \ \dots \ y_M^1] = ref * s[h_1^1 h_1^1 \ h_1^1 h_2^1 \ \dots \ h_1^1 h_M^1]$ 。通过接收导频信号, reader 可解出 tag_1 与 reader 之间的信道 $[h_1^1 \ h_2^1 \ \dots \ h_M^1]$ 。最终, reader 获得所有 tag

$$H = \begin{bmatrix} h_1^1 & \dots & h_M^1 \\ \vdots & \vdots & \vdots \\ h_1^N & \dots & h_M^N \end{bmatrix}$$

与 reader 之间的信道:关于本步骤中各个公式内包含的内容的含义,均与前述实施例相同,不做重复说明。

步骤 504: reader 计算天线权系数。该天线权系数即前述实施例中的射频系数。

本步骤的具体过程如下: reader 将 H 按行分为 K 组, $K = \text{ceil}(N/M)$, $\text{ceil}(\cdot)$ 表示向上取整; 得到

$$H_k = \begin{bmatrix} H((k-1)M+1) \\ \vdots \\ H((k-1)M+M) \end{bmatrix}$$

第 k 组信道矩阵为 $(1 \leq k \leq K)$: H_k ; 求第 k 组信道矩阵的右逆矩阵: $H_k^{\text{inv}} = H_k^H (H_k H_k^H)^{-1}$; 计算第 k 组 (即第 k 组 tag) 对应的天线权系数: $w_k = \text{sum_column}(H_k^{\text{inv}})$ 。本步骤中各个公式包含的内容的含义, 均与前述实施例相同, 不做赘述。

步骤 505: reader 发射信号 r , 使 N 个 tag 接收到的信号都为 r 。

具体的, reader 发 K 次信号 r , 也就是 reader 向 N 个 tag 所划分的 K 组 tag 中, 每组 tag 分别发送该信号 r , 在前述实施例中已经说明, 向每组 tag 可以发送多个信号, 本步骤中的信号 r 可以是向每组 tag 发送的多个信号中的任意之一。

以 reader 发 K 次信号的处理中的发送第 k 次信号为例, 也就是 reader 向第 k 组 tag 发送的第 i 个信号, 可以将其表示为 r_i , 第 k 次的天线权系数为 w_k , 则第 k 组 tag 中涉及的第 n 个 tag 收到的信号为: $r_i H_k w_k = r_i I_{n \times 1}$, 该公式中各个内容的含义与前述实施例相同, 不做赘述。

reader 经过 K 次发射后, 网络中所有的 tag 都将会接收到信号 r_i , reader 也知道 r_i , 所以 r_i 中的信息或特征 (即信号的相关信息, 也就是第 i 个信号的相关信息) 可以作为密钥源进行量化。

若相干时间很长, 即信道环境处于静态环境, 则 reader 无需重复执行步骤 501 到步骤 504, reader 只需要多次重复执行步骤 505, 可以每次都改变信号 r (也就是改变信号的相关信息) 并再次发射信号 r , 也就是可以改变步骤 505 中的 r , 即可使密钥源时变并再次发射信号。应理解的是, 不同次发送信号的时候, reader 可以根据实际需求来确定是否改变信号的相关信息, 也有一些可能的示例中, 可能存在任意两次发送相同的信号, 本实施例不对其全部可能的情况进行穷举。

若信道环境时变, 则在不同的相干时间内执行步骤 501 到步骤 505 即可, 只是每次执行步骤 505 时, 可以改变 r , 使得密钥源时变。

步骤 506: 经过多次执行步骤 505 后, reader 和所有 tag 都积累了多个不同 r 的信息或特征, 进而可以确定各自的组密钥。至此, reader 得到前述实施例中的第一组密钥, 每个 tag 得到了前述实施例中的各自的第二组密钥。

步骤 507: reader 和 N 个 tag 确定一致的组密钥。

本步骤可以基于 tag 计算能力, 给出不同的最终组密钥确定方法。

方法 1: reader 将初始密钥序列 (即 reader 的第一组密钥) 通过某个 hash 函数映射为某个值, 或者计算该序列的循环冗余校验码 (CRC), 将哈希映射值或循环冗余校验码广播发射出去, N 个 tag 接收到后, 分别根据自己的初始密钥序列 (即 tag 自身的第二组密钥) 计算自己的哈希映射值或循环冗余校验码, 与接收到 reader 的数据进行比较, 若一致, 则返回 success 指令。不一致, 则返回 fail 指令, 等待下一次组密钥生成。reader 记录成功生成组密钥的 tag, 可利用此次组密钥与这些 tag 进行通信。

方法 2: 若 N 个 tag 具备某些译码纠错能力 (如 LDPC、Turbo 译码), 则 reader 将初始密钥序列 (即 reader 的第一组密钥) 通过某编码方法生成校验码, 将校验码发送给 N 个 tag, 所有 tag 利用校验码进行译码纠错 (即每个 tag 对自身的第二组密钥进行译码纠错), 从而使得 reader 和各个 tag 获得一致的密钥。

上述两个方法中, 方法 1 针对计算能力较弱的 tag, 无法纠错, 如果密钥出现不一致, 则需等待下一次组密钥生成。方法 2 是常用的密钥纠错方法, 但对于 tag, 需要支持具有一定复杂程度的译码算法。

进一步结合上述图 5 所提供的示例的仿真实验进行说明: reader 与 tag 之间的的信道建模如下:

$G_{rt} = \sqrt{L_0 d_{rt}^{-\alpha_{rt}}} \left[\sqrt{\frac{\beta_{rt}}{1+\beta_{rt}}} G_{rt}^{\text{LOS}} + \sqrt{\frac{1}{1+\beta_{rt}}} G_{rt}^{\text{NLOS}} \right]$, 其中, $L_0 = \left(\frac{\lambda_c}{4\pi}\right)^2$ 表示路径损耗常数, λ_c 表示载波波长, 载波频率取 900Mhz。 G_{rt}^{NLOS} 满足瑞利分布, d_{rt} 是指 reader 与 tag 的距离。 α_{rt} 指路径损耗指数, 取 2。 β_{rt} 为莱斯因子, 取 3。 $G_{rt}^{\text{LOS}} = (d^*)c$, 其中, $d = [d_1 \cdots d_{N_{tag}}]^T$, $c = [c_1 \cdots c_M]$, $c_m = \exp\left(j2\pi \frac{d_r}{\lambda_c} (m-1) \sin \theta_r\right)$, $1 \leq m \leq M$, $d_{n_{tag}} = \exp\left(j2\pi \frac{d_t}{\lambda_c} (n_{tag}-1) \sin \theta_t\right)$, $1 \leq n_{tag} \leq N_{tag}$, 其中, d_r 和 d_t 表示 reader 和 tag 中天线之间的距离, $\frac{d_r}{\lambda_c}$ 取 0.5, $\frac{d_t}{\lambda_c}$ 取 0, $N_{tag} = 1$ 。 $M = 8$, $\theta_r = \tan^{-1} \frac{y_r - y_t}{x_r - x_t}$, $\theta_t = \pi - \theta_r$, (x_r, y_r) 是 reader 的坐标, 这里取为原点。 (x_t, y_t) 是 tag 的坐标, N 个 tag 随

机均匀分布, $N = 32$ 。通信范围半径 $d_1 = 50m$, $d_2 = 5m$ 。量化阶数 Q 取 8, 信号 r 的最小功率 $P_{min} = -20dBm$, 信号 r 的最大功率 $P_{max} = 20dBm$, $ref = 0.9$ 。

基于上述建模, 仿真 N 个 tag 与 reader 之间的密钥不一致率、eve 与 reader 之间的密钥不一致率, 结果如图 6 所示, 图 6 中的“tag”所表示的 tag 与 reader 之间的密钥不一致率具体指的是 N 个 tag (的第二组密钥) 与 reader (的第一组密钥) 的密钥不一致率的平均值, 通过图 6 可以看出, 随着信噪比的增加, tag 与 reader 之间的密钥不一致率越来越小, 比如信噪比在 10dB 时, tag 与 reader 之间的密钥不一致率在 0.3 左右, 信噪比在 30dB 时, tag 与 reader 之间的密钥不一致率接近 0.05, 而窃听者与 reader 之间的密钥不一致率平稳 0.45~0.5 附近, 说明上述示例可以使得 Reader 和 tag 安全生成各自的组密钥。

结合图 7 进行另一种示例说明, 在图 7 涉及的方案中, 信号 r 的强度作为密钥源, 也就是前述实施例中信号的相关信息具体为信号的强度, 本示例选择信号 r 的强度作为密钥源, 即不关心信号 r 的具体内容, 只利用其信号强度。具体步骤如下:

步骤 701~步骤 704 的具体说明, 与前述示例的步骤 501~步骤 504 相同, 因此不做重复说明。

步骤 705: reader 发射信号 r , 使 N 个 tag 接收到的信号强度一样。

具体过程如下: reader 发射信号 r 的强度记为 P , 发 K 次。以第 k 次为例: 第 k 次的天线权系数为 w_k , 则第 k 组中涉及的 tag 收到的信号幅度为: $\sqrt{P}H_k w_k = \sqrt{P}I_{k,N \times 1}$, 公式中处理 P 表示信号强度 (或幅度) 之外, 其余内容与前述实施例相同, 不做赘述。经过 K 次发射后, 所有的 tag 都将会记录得到信号强度 P , reader 也知道 P , 所以 P 将会作为密钥源进行量化。

若相干时间很长, 即信道环境处于静态环境, 则 reader 无需重复执行步骤 701 到步骤 704, 只需要改变步骤 705 中的 P 值, 即可使密钥源时变。若信道环境时变, 则在不同的相干时间内执行步骤 701 到步骤 705 即可。

步骤 706: 经过多次执行步骤 705 的积累后, 假设所有 tag 获得了 L 个强度值, reader 也已知这 L 个强度值, 则双方开始量化, reader 和 N 个 tag 获得初始密钥序列, 也就是 reader 得到了第一组密钥, 每个 tag 得到了各自的第二组密钥。具体过程如下: 设 reader 取 P 的范围为: $P_{min} \leq P \leq P_{max}$ 。量化阶数为 Q 时, 将 P 的范围均匀分为 Q 个, 每个范围对应长度为 $\log_2 Q$ 的格雷码, 此时每个强度值对应 $\log_2 Q$ bit。为了减少量化边界左右微小误差导致的量化结果的不同, reader 和 tag 可对所有获取的强度值执行就近取整, 然后进行量化, 至此 reader 和 N 个 tag 获得初始密钥序列。量化方法包括但不限于此处所述的方法。

步骤 707: reader 和 N 个 tag 确定一致的组密钥。具体的, 利用给出的方法 1 或方法 2, reader 和 N 个 tag 确定最终的一致密钥。

结合图 8 进行一种示例说明, 在图 8 涉及的方案中, 信号 r 的数据信息作为密钥源, 本示例设计将信号 r 中携带的数据信息, 将其作为密钥源, 以此抵抗 Eve 贴近 tag 或合法信道与非法信道差异性较小的恶劣窃听场景。具体实施包括以下步骤:

步骤 801~步骤 804 与前述示例中的步骤 501~步骤 504 相同, 不做重复说明。

步骤 805: reader 发射信号 r , 使 N 个 tag 接收到相同组密钥。

具体过程如下: reader 发 K 次信号 r 。当第 k 次发射 r_{jk} 时, r_{jk} 的帧结构设计为:

$[ID_1^k \oplus k_j, ID_2^k \oplus k_j, \dots, ID_n^k \oplus k_j]$ 。当第 k 组中任意一个 tag 收到 r_{jk} 后, 取出自身对应的数据段 (即目标数据段), 然后用自己的 ID 异或该数据段, 获得 k_j 。如此, 经过 K 次发射后, 所有的 tag 都将会得到相同的 k_j 。关于本步骤中公式的内容含义与前述实施例相同, 不做赘述。

在同一相干时间内, 只需要改变步骤 805 中的 k , 即可使密钥源时变。在不同的相干时间内执行步骤 801 到步骤 805 即可。

步骤 806: 将多次积累的不同 k (即密钥序列) 串联作为组密钥序列。至此, reader 得到了第一组密钥 (也就是 reader 得到的组密钥序列), 每个 tag 得到了各自的第二组密钥 (也就是每个 tag 得到的组密钥序列)。

步骤 807: reader 和 N 个 tag 确定一致的组密钥。也就是利用给出的方法 1 或方法 2, reader 和 N 个 tag 确定最终的一致密钥。

以上多种示例针对以 reader 为中心节点, 多个 tag 为子节点的零功耗通信网络, 设计了一种物理层组密钥生成方案。该方案通过给读写器多天线配置权系数, 使多个 tag 可同时收到相同的密钥源, 从而获得组密钥。从而, 有效降低了组密钥生成的时间开销。同时, 由于权系数是利用合法信道值计算得到, 对于窃听者, 合法信道与窃听信道具有差异性, 使其无法收到与 tag 一样的密钥源, 从而保

证了组密钥的安全性。进一步通过设计密钥源，可以抵抗不同窃听程度的非法窃听，以此适应不同的应用场景。

本实施例提供的方案中，由第一设备向每个第二设备发送多个信号，该多个信号的射频系数为基于第二设备与第一设备间的信道特征计算得到的，进而第一设备自身也会基于各个信号的相关信息生成用于与各个第二设备通信的组密钥。如此，通过对发送至不同第二设备的信号配置对应于不同第二设备的射频系数，从而能够准确的抵消该第二设备与第一设备之间的信道特征，即抵消该第二设备与第一设备的信道的损耗或干扰，从而在保证降低生成组密钥的时间开销的同时，还保证了组密钥的安全性。

最后，结合相关技术对本实施例的有益效果进一步进行说明。

对于组密钥生成技术的研究，主要分为两类，一类是基于密码学的组密钥生成；一类是基于物理层特征的组密钥生成。其中，基于密码学的组密钥生成，以一个 AP (AccessPoint, 接入点) 和多个 STA (Station, 站点) 生成组密钥的处理为例来说：AP 首先与每个 STA 进行四次握手，生成对应的对密钥，不同 STA 的对密钥不同；当需要生成组密钥时，AP 生成组密钥 GTK，然后用对密钥对 GTK 加密，将加密数据发给 STA，STA 利用对密钥解密得到 GTK，也就是如果有 N 个 STA，就需要发 N 次 GTK。基于物理层特征的组密钥的处理方式可以包括：第一种方式中，中心节点和子节点在一个相干时间内相互交互导频，各自记录信号强度，然后中心节点计算多个强度差，分别发送给子节点，子节点利用自己记录的信号强度和收到的强度差恢复出组密钥；第二种方式中，需要所有子节点配置多天线，子节点将多天线中收到信号的天线记为 1，未收到信号的天线记为 0，最终获得一个多天线接收信号状态的序列；第三种方式中，通过指定方法，可以保证多个子节点的状态序列相同，因此可将这一状态序列作为组密钥。

然而上述相关技术的组密钥生成方案存在以下问题：

第一，对于子节点设备能力要求高。基于密码学的组密钥生成，需要设备支持密钥生成器以及复杂的加解密算法。基于物理层特征的组密钥部分方案中也需要子节点设备具有一定的硬件能力或算法能力。这些对于子节点有特别要求的方案，在零功耗网络中不具备普适性，大部分场景下的零功耗设备都是极简的电路设计、低计算力、低存储力，无法支撑这些方案所需。

第二，生成组密钥的时间开销大。这里假设节点到节点的一次单向通信时间为 T ，一共有 N 个子节点。以一个 AP (AccessPoint, 接入点) 和多个 STA (Station, 站点) 生成组密钥的处理为例来说，每个子节点生成对密钥就需要四次握手，最后的组密钥还需要依次发送给每个 STA，所以生成组密钥的时间大于 $2NT$ 。对于基于物理层特征的组密钥，以第一种方式为例来说，生成一次组密钥的时间为 $2NT$ ，且一个相干时间内，信道不变时，只能进行一次组密钥生成，在相干时间较长的场景下，组密钥不会变化。

而采用本申请实施例所提供的密钥生成方法，首先可以降低组密钥生成的时间开销。具体来说，本申请提供的密钥生成方法所有 tag (即每个第二设备) 获取一次组密钥的量化结果或密钥序列 (也就是获取一次信号的相关信息，或基于一个信号的相关信息得到量化结果或密钥序列) 的时间为

$\left(1 + N + \text{ceil}\left(\frac{N}{M}\right)\right)T$ ，小于 $2NT$ ，即低于已有标准 (802.11i) 中组密钥生成方案的时间开销。再次，

本申请提供的密钥生成方法不需要 tag (也就是第二设备) 增加任何额外的开销，对于零功耗设备 tag，不增加任何多余过程，tag 只需要执行简单的反射和接收信号就可以实现组密钥的生成，不需要改变零功耗设备支持的技术和简易的电路设计。最后，即使在相干时间较长的环境中，仍可以使组密钥更新，避免单一密钥使用时间过长的问题。同时，不仅可利用内生信道保护密钥源，也可以通过对信号 r 进行设计，加强密钥源的保护，抵抗不同窃听程度的窃听者。

图 9 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 901，用于向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的；

第一处理单元 902，用于基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

所述第一通信单元，用于向所述每个第二设备发送组密钥生成信令；接收来自所述每个第二设备的导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号；

所述第一处理单元，用于基于所述每个第二设备的导频信号，计算所述每个第二设备与所述第一设备间的信道特征。

所述第一处理单元，用于基于所述每个第二设备与所述第一设备间的信道特征，计算一个或多个射频系数，其中，所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

所述第一通信单元,用于基于所述一个或多个射频系数中的第k个射频系数,向第k组第二设备中的每个第二设备发送所述多个信号,其中,所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备,所述第k组第二设备为所述多个第二设备的一个或多个分组中之一,k为正整数。

5 所述第一处理单元,用于基于所述多个信号的相关信息,得到多个第一量化结果;基于所述多个第一量化结果,生成所述第一组密钥。

10 所述第一处理单元,用于基于所述多个信号中第i个信号的相关信息,确定所述第i个信号对应的第一量化范围,将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第i个第一量化结果,其中,所述第一量化范围为多个第一候选量化范围中之一,所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值,i为正整数。

所述多个信号的相关信息,包括以下至少之一:所述多个信号中每个信号的强度、所述每个信号的相位。

所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列;所述第一处理单元,用于基于所述多个信号中每个信号携带的密钥序列,生成所述第一组密钥。

15 所述多个信号中第j个信号携带一个或多个数据段,所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第j个密钥序列计算的,j为正整数。

所述多个信号用于所述每个第二设备生成第二组密钥;所述第一处理单元,用于基于所述第一组密钥,计算组密钥校验信息,其中,所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性;

20 所述第一通信单元,用于向所述每个第二设备发送第一消息,其中,所述第一消息携带所述组密钥校验信息。

25 所述第一通信单元,用于执行以下之一:接收来自目标第二设备的第二消息,其中,所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功,所述目标第二设备为所述多个第二设备中之一;接收来自所述目标第二设备的第三消息,其中,所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

所述多个信号用于所述每个第二设备生成第二组密钥;所述第一处理单元,用于基于所述第一组密钥,计算组密钥纠错信息,其中,所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥;

30 所述第一通信单元,用于向所述每个第二设备发送第四消息,其中,所述第四消息携带所述组密钥纠错信息。

所述第一设备为以下之一:终端设备、网络设备;所述第二设备为零功耗设备。

图10是根据本申请一实施例的目标第二设备的组成结构示意图,包括:

第二通信单元1001,用于接收来自第一设备的多个信号,其中,所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的;

35 第二处理单元1002,用于基于所述多个信号的相关信息,生成第二组密钥,其中,所述第二组密钥用于所述目标第二设备与所述第一设备的通信,所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

40 所述第二通信单元,用于接收来自所述第一设备的组密钥生成信令;向所述第一设备发送导频信号,其中,所述导频信号为所述组密钥生成信令所对应的反射信号,所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。

所述第二处理单元,用于基于所述多个信号的相关信息,得到多个第二量化结果;基于所述多个第二量化结果,生成所述第二组密钥。

45 所述第二处理单元,用于基于所述多个信号中第i个信号的相关信息,确定所述第i个信号对应的第二量化范围,将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第i个第二量化结果,其中,所述第二量化范围为多个第二候选量化范围中之一,所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值,i为正整数。

所述多个信号的相关信息,包括以下之一:所述多个信号中每个信号的强度、所述每个信号的相位。

50 所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列;所述第二处理单元,用于基于所述多个信号中每个信号携带的密钥序列,生成所述第二组密钥。

所述多个信号中第j个信号携带一个或多个数据段,所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第j个密钥序列计算的;所述第二处理单元,用于从所述第j个信号中,

提取所述目标第二设备对应的目标数据段, j 为正整数; 基于所述目标第二设备的标识和所述目标数据段, 计算所述第 j 个信号携带的第 j 个密钥序列。

所述第二通信单元, 用于接收来自所述第一设备的第一消息, 其中, 所述第一消息携带组密钥校验信息, 所述组密钥校验信息为所述第一设备基于第一组密钥计算的, 所述第一组密钥为所述第一设备基于所述多个信息生成的;

所述第二处理单元, 用于基于所述第二组密钥计算验证信息; 基于所述组密钥校验信息和所述验证信息, 校验所述第二组密钥与所述第一组密钥的一致性。

所述第二通信单元, 用于执行以下至少之一: 在所述第二组密钥与所述第一组密钥一致的情况下, 向所述第一设备发送第二消息, 其中, 所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功; 在所述第二组密钥与所述第一组密钥不一致的情况下, 向所述第一设备发送第三消息, 其中, 所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

所述第二通信单元, 用于接收来自所述第一设备的第四消息, 其中, 所述第四消息携带组密钥纠错信息, 所述组密钥纠错信息为所述第一设备基于第一组密钥计算的, 所述第一组密钥为所述第一设备基于所述多个信息生成的;

所述第二处理单元, 用于基于所述组密钥纠错信息对所述第二组密钥进行纠错, 得到与所述第一组密钥一致的组密钥。

所述第一设备为以下之一: 终端设备、网络设备; 所述目标第二设备为零功耗设备。

本申请实施例的设备能够实现前述的密钥生成方法实施例中的各个设备的对应功能。该第一设备、或目标第二设备中的各个模块(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一设备、或目标第二设备中的各个模块(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 11 是根据本申请实施例的通信设备 1100 示意性结构图。该通信设备 1100 包括处理器 1110, 处理器 1110 可以从存储器中调用并运行计算机程序, 以使通信设备 1100 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 1100 还可以包括存储器 1120。其中, 处理器 1110 可以从存储器 1120 中调用并运行计算机程序, 以使通信设备 1100 实现本申请实施例中的方法。

其中, 存储器 1120 可以是独立于处理器 1110 的一个单独的器件, 也可以集成在处理器 1110 中。

在一种可能的实现方式中, 通信设备 1100 还可以包括收发器 1130, 处理器 1110 可以控制该收发器 1130 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 1130 可以包括发射机和接收机。收发器 1130 还可以进一步包括天线, 天线的数量可以是一个或多个。

在一种可能的实现方式中, 该通信设备 1100 可为本申请实施例的第一设备、或目标第二设备, 并且该通信设备 1100 可以实现本申请实施例的各个方法中由第一设备、或目标第二设备实现的相应流程, 为了简洁, 在此不再赘述。

在本申请的实施例中提供一种第一设备, 包括: 处理器, 与所述处理器通信的存储器, 所述存储器用于存储指令, 当所述指令被所述处理器执行时, 所述指令使所述第一设备执行: 向多个第二设备中的每个第二设备发送多个信号, 其中, 所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的; 基于所述多个信号的相关信息, 生成第一组密钥, 所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

所述指令还使所述第一设备执行: 向所述每个第二设备发送组密钥生成信令; 接收来自所述每个第二设备的导频信号, 其中, 所述导频信号为所述组密钥生成信令所对应的反射信号; 基于所述每个第二设备的导频信号, 计算所述每个第二设备与所述第一设备间的信道特征。

所述指令还使所述第一设备执行: 基于所述每个第二设备与所述第一设备间的信道特征, 计算一个或多个射频系数, 其中, 所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

所述指令还使所述第一设备执行: 基于所述一个或多个射频系数中的第 k 个射频系数, 向第 k 组第二设备中的每个第二设备发送所述多个信号, 其中, 所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备, 所述第 k 组第二设备为所述多个第二设备的一个或多个分组中之一, k 为正整数。

所述指令还使所述第一设备执行: 基于所述多个信号的相关信息, 得到多个第一量化结果; 基于所述多个第一量化结果, 生成所述第一组密钥。

所述指令还使所述第一设备执行：基于所述多个信号中第*i*个信号的相关信息，确定所述第*i*个信号对应的第一量化范围，将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第*i*个第一量化结果，其中，所述第一量化范围为多个第一候选量化范围中之一，所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值，*i*为正整数。

5 所述多个信号的相关信息，包括以下至少之一：所述多个信号中每个信号的强度、所述每个信号的相位。

所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述指令还使所述第一设备执行：基于所述多个信号中每个信号携带的密钥序列，生成所述第一组密钥。

10 所述多个信号中第*j*个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第*j*个密钥序列计算的，*j*为正整数。

所述多个信号用于所述每个第二设备生成第二组密钥；所述指令还使所述第一设备执行：基于所述第一组密钥，计算组密钥校验信息，其中，所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性；向所述每个第二设备发送第一消息，其中，所述第一消息携带所述组密钥校验信息。

15 所述指令还使所述第一设备执行以下之一：接收来自目标第二设备的第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功，所述目标第二设备为所述多个第二设备中之一；接收来自所述目标第二设备的第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

20 所述多个信号用于所述每个第二设备生成第二组密钥；所述指令还使所述第一设备执行：基于所述第一组密钥，计算组密钥纠错信息，其中，所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥；向所述每个第二设备发送第四消息，其中，所述第四消息携带所述组密钥纠错信息。

所述第一设备为以下之一：终端设备、网络设备；所述第二设备为零功耗设备。

25 在本申请的实施例中提供一种目标第二设备，包括：处理器，与所述处理器通信的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，所述指令使所述目标第二设备执行：接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

30 所述指令还使所述目标第二设备执行：接收来自所述第一设备的组密钥生成信令；向所述第一设备发送导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号，所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。

所述指令还使所述目标第二设备执行：基于所述多个信号的相关信息，得到多个第二量化结果；基于所述多个第二量化结果，生成所述第二组密钥。

35 所述指令还使所述目标第二设备执行：基于所述多个信号中第*i*个信号的相关信息，确定所述第*i*个信号对应的第二量化范围，将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第*i*个第二量化结果，其中，所述第二量化范围为多个第二候选量化范围中之一，所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值，*i*为正整数。

40 所述多个信号的相关信息，包括以下之一：所述多个信号中每个信号的强度、所述每个信号的相位。

所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述指令还使所述目标第二设备执行：基于所述多个信号中每个信号携带的密钥序列，生成所述第二组密钥。

45 所述多个信号中第*j*个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第*j*个密钥序列计算的；所述指令还使所述目标第二设备执行：从所述第*j*个信号中，提取所述目标第二设备对应的目标数据段，*j*为正整数；基于所述目标第二设备的标识和所述目标数据段，计算所述第*j*个信号携带的第*j*个密钥序列。

50 所述指令还使所述目标第二设备执行：接收来自所述第一设备的第一消息，其中，所述第一消息携带组密钥校验信息，所述组密钥校验信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；基于所述第二组密钥计算验证信息；基于所述组密钥校验信息和所述验证信息，校验所述第二组密钥与所述第一组密钥的一致性。

所述指令还使所述目标第二设备执行以下至少之一：在所述第二组密钥与所述第一组密钥一致的情况下，向所述第一设备发送第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二

组密钥与所述第一组密钥的一致性校验成功；在所述第二组密钥与所述第一组密钥不一致的情况下，向所述第一设备发送第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

所述指令还使所述目标第二设备执行：接收来自所述第一设备的第四消息，其中，所述第四消息携带组密钥纠错信息，所述组密钥纠错信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；基于所述组密钥纠错信息对所述第二组密钥进行纠错，得到与所述第一组密钥一致的组密钥。

所述第一设备为以下之一：终端设备、网络设备；所述目标第二设备为零功耗设备。

图 12 是根据本申请实施例的芯片 1200 的示意性结构图。该芯片 1200 包括处理器 1210，处理器 1210 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 1200 还可以包括存储器 1220。其中，处理器 1210 可以从存储器 1220 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 1220 可以是独立于处理器 1210 的一个单独的器件，也可以集成在处理器 1210 中。

在一种可能的实现方式中，该芯片 1200 还可以包括输入接口 1230。其中，处理器 1210 可以控制该输入接口 1230 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 1200 还可以包括输出接口 1240。其中，处理器 1210 可以控制该输出接口 1240 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、或目标第二设备，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、或目标第二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。

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。

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 13 是根据本申请实施例的通信系统 1300 的示意性框图。该通信系统 1300 包括第一设备 1310、目标第二设备 1320。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。

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

1.一种密钥生成方法,包括:

第一设备向多个第二设备中的每个第二设备发送多个信号,其中,所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的;

所述第一设备基于所述多个信号的相关信息,生成第一组密钥,所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

2.根据权利要求1所述的方法,其中,所述方法还包括:

所述第一设备向所述每个第二设备发送组密钥生成信令;

所述第一设备接收来自所述每个第二设备的导频信号,其中,所述导频信号为所述组密钥生成信令所对应的反射信号;

所述第一设备基于所述每个第二设备的导频信号,计算所述每个第二设备与所述第一设备间的信道特征。

3.根据权利要求2所述的方法,其中,所述方法还包括:

所述第一设备基于所述每个第二设备与所述第一设备间的信道特征,计算一个或多个射频系数,其中,所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

4.根据权利要求3所述的方法,其中,所述第一设备向多个第二设备中的每个第二设备发送多个信号,包括:

所述第一设备基于所述一个或多个射频系数中的第k个射频系数,向第k组第二设备中的每个第二设备发送所述多个信号,其中,所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备,所述第k组第二设备为所述多个第二设备的一个或多个分组中之一,k为正整数。

5.根据权利要求1-4任一项所述的方法,其中,所述第一设备基于所述多个信号的相关信息,生成第一组密钥,包括:

所述第一设备基于所述多个信号的相关信息,得到多个第一量化结果;

所述第一设备基于所述多个第一量化结果,生成所述第一组密钥。

6.根据权利要求5所述的方法,其中,所述第一设备基于所述多个信号的相关信息,得到多个第一量化结果,包括:

所述第一设备基于所述多个信号中第i个信号的相关信息,确定所述第i个信号对应的第一量化范围,将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第i个第一量化结果,其中,所述第一量化范围为多个第一候选量化范围中之一,所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值,i为正整数。

7.根据权利要求5或6所述的方法,其中,所述多个信号的相关信息,包括以下至少之一:所述多个信号中每个信号的强度、所述每个信号的相位。

8.根据权利要求1-4任一项所述的方法,其中,所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列;所述第一设备基于所述多个信号的相关信息,生成第一组密钥,包括:

所述第一设备基于所述多个信号中每个信号携带的密钥序列,生成所述第一组密钥。

9.根据权利要求8所述的方法,其中,所述多个信号中第j个信号携带一个或多个数据段,所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第j个密钥序列计算的,j为正整数。

10.根据权利要求1-9任一项所述的方法,其中,所述多个信号用于所述每个第二设备生成第二组密钥,所述方法还包括:

所述第一设备基于所述第一组密钥,计算组密钥校验信息,其中,所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性;

所述第一设备向所述每个第二设备发送第一消息,其中,所述第一消息携带所述组密钥校验信息。

11.根据权利要求10所述的方法,其中,所述方法还包括以下之一:

所述第一设备接收来自目标第二设备的第二消息,其中,所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功,所述目标第二设备为所述多个第二设备中之一;

所述第一设备接收来自所述目标第二设备的第三消息,其中,所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

12.根据权利要求1-9任一项所述的方法,其中,所述多个信号用于所述每个第二设备生成第二组密钥,所述方法还包括:

所述第一设备基于所述第一组密钥，计算组密钥纠错信息，其中，所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥；

所述第一设备向所述每个第二设备发送第四消息，其中，所述第四消息携带所述组密钥纠错信息。

5 13.根据权利要求 1-12 任一项所述的方法，其中，所述第一设备为以下之一：终端设备、网络设备；所述第二设备为零功耗设备。

14.一种密钥生成方法，包括：

目标第二设备接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；

10 所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

15.根据权利要求 14 所述的方法，其中，所述方法还包括：

所述目标第二设备接收来自所述第一设备的组密钥生成信令；

15 所述目标第二设备向所述第一设备发送导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号，所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。

16.根据权利要求 14 或 15 所述的方法，其中，所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，包括：

20 所述目标第二设备基于所述多个信号的相关信息，得到多个第二量化结果；

所述目标第二设备基于所述多个第二量化结果，生成所述第二组密钥。

17.根据权利要求 16 所述的方法，其中，所述目标第二设备基于所述多个信号的相关信息，得到多个第二量化结果，包括：

25 所述目标第二设备基于所述多个信号中第 i 个信号的相关信息，确定所述第 i 个信号对应的第二量化范围，将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第 i 个第二量化结果，其中，所述第二量化范围为多个第二候选量化范围中之一，所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值， i 为正整数。

18.根据权利要求 16 或 17 所述的方法，其中，所述多个信号的相关信息，包括以下之一：所述多个信号中每个信号的强度、所述每个信号的相位。

30 19.根据权利要求 14 或 15 所述的方法，其中，所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述目标第二设备基于所述多个信号的相关信息，生成第二组密钥，包括：

所述目标第二设备基于所述多个信号中每个信号携带的密钥序列，生成所述第二组密钥。

20.根据权利要求 19 所述的方法，其中，所述多个信号中第 j 个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的；所述方法还包括：

35 所述目标第二设备从所述第 j 个信号中，提取所述目标第二设备对应的目标数据段， j 为正整数；

所述目标第二设备基于所述目标第二设备的标识和所述目标数据段，计算所述第 j 个信号携带的第 j 个密钥序列。

21.根据权利要求 14-20 任一项所述的方法，其中，所述方法还包括：

40 所述目标第二设备接收来自所述第一设备的第一消息，其中，所述第一消息携带组密钥校验信息，所述组密钥校验信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；

所述目标第二设备基于所述第二组密钥计算验证信息；

45 所述目标第二设备基于所述组密钥校验信息和所述验证信息，校验所述第二组密钥与所述第一组密钥的一致性。

22.根据权利要求 21 所述的方法，其中，所述方法还包括以下至少之一：

所述目标第二设备在所述第二组密钥与所述第一组密钥一致的情况下，所述目标第二设备向所述第一设备发送第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功；

50 所述目标第二设备在所述第二组密钥与所述第一组密钥不一致的情况下，所述目标第二设备向所述第一设备发送第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

23.根据权利要求 14-20 任一项所述的方法,其中,所述方法还包括:

所述目标第二设备接收来自所述第一设备的第四消息,其中,所述第四消息携带组密钥纠错信息,所述组密钥纠错信息为所述第一设备基于第一组密钥计算的,所述第一组密钥为所述第一设备基于所述多个信息生成的;

5 所述目标第二设备基于所述组密钥纠错信息对所述第二组密钥进行纠错,得到与所述第一组密钥一致的组密钥。

24.根据权利要求 14-23 任一项所述的方法,其中,所述第一设备为以下之一:终端设备、网络设备;所述目标第二设备为零功耗设备。

25.一种第一设备,包括:

10 第一通信单元,用于向多个第二设备中的每个第二设备发送多个信号,其中,所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计算得到的;

第一处理单元,用于基于所述多个信号的相关信息,生成第一组密钥,所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

26.根据权利要求 25 所述的第一设备,其中,所述第一通信单元,用于向所述每个第二设备发送组密钥生成信令;接收来自所述每个第二设备的导频信号,其中,所述导频信号为所述组密钥生成信令所对应的反射信号;

15 所述第一处理单元,用于基于所述每个第二设备的导频信号,计算所述每个第二设备与所述第一设备间的信道特征。

27.根据权利要求 26 所述的第一设备,其中,所述第一处理单元,用于基于所述每个第二设备与所述第一设备间的信道特征,计算一个或多个射频系数,其中,所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

28.根据权利要求 27 所述的第一设备,其中,所述第一通信单元,用于基于所述一个或多个射频系数中的第 k 个射频系数,向第 k 组第二设备中的每个第二设备发送所述多个信号,其中,所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备,所述第 k 组第二设备为所述多个第二设备的一个或多个分组中之一, k 为正整数。

29.根据权利要求 25-28 任一项所述的第一设备,所述第一处理单元,用于基于所述多个信号的相关信息,得到多个第一量化结果;基于所述多个第一量化结果,生成所述第一组密钥。

30.根据权利要求 29 所述的第一设备,其中,所述第一处理单元,用于基于所述多个信号中第 i 个信号的相关信息,确定所述第 i 个信号对应的第一量化范围,将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第 i 个第一量化结果,其中,所述第一量化范围为多个第一候选量化范围中之一,所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值, i 为正整数。

31.根据权利要求 29 或 30 所述的第一设备,其中,所述多个信号的相关信息,包括以下至少之一:所述多个信号中每个信号的强度、所述每个信号的相位。

32.根据权利要求 25-28 任一项所述的第一设备,其中,所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列;所述第一处理单元,用于基于所述多个信号中每个信号携带的密钥序列,生成所述第一组密钥。

33.根据权利要求 32 所述的第一设备,其中,所述多个信号中第 j 个信号携带一个或多个数据段,所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的, j 为正整数。

34.根据权利要求 25-33 任一项所述的第一设备,其中,所述多个信号用于所述每个第二设备生成第二组密钥;所述第一处理单元,用于基于所述第一组密钥,计算组密钥校验信息,其中,所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性;

40 所述第一通信单元,用于向所述每个第二设备发送第一消息,其中,所述第一消息携带所述组密钥校验信息。

35.根据权利要求 34 所述的第一设备,其中,所述第一通信单元,用于执行以下之一:接收来自目标第二设备的第二消息,其中,所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功,所述目标第二设备为所述多个第二设备中之一;接收来自所述目标第二设备的第三消息,其中,所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

36.根据权利要求 25-33 任一项所述的第一设备,其中,所述多个信号用于所述每个第二设备生成

第二组密钥；所述第一处理单元，用于基于所述第一组密钥，计算组密钥纠错信息，其中，所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥；

所述第一通信单元，用于向所述每个第二设备发送第四消息，其中，所述第四消息携带所述组密钥纠错信息。

5 37.根据权利要求 25-36 任一项所述的第一设备，其中，所述第一设备为以下之一：终端设备、网络设备；所述第二设备为零功耗设备。

38.一种目标第二设备，包括：

第二通信单元，用于接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；

10 第二处理单元，用于基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

15 39.根据权利要求 38 所述的目标第二设备，其中，所述第二通信单元，用于接收来自所述第一设备的组密钥生成信令；向所述第一设备发送导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号，所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。

40.根据权利要求 38 或 39 所述的目标第二设备，其中，所述第二处理单元，用于基于所述多个信号的相关信息，得到多个第二量化结果；基于所述多个第二量化结果，生成所述第二组密钥。

20 41.根据权利要求 40 所述的目标第二设备，其中，所述第二处理单元，用于基于所述多个信号中第 i 个信号的相关信息，确定所述第 i 个信号对应的第二量化范围，将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第 i 个第二量化结果，其中，所述第二量化范围为多个第二候选量化范围中之一，所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值， i 为正整数。

25 42.根据权利要求 40 或 41 所述的目标第二设备，其中，所述多个信号的相关信息，包括以下之一：所述多个信号中每个信号的强度、所述每个信号的相位。

43.根据权利要求 38 或 39 所述的目标第二设备，其中，所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述第二处理单元，用于基于所述多个信号中每个信号携带的密钥序列，生成所述第二组密钥。

30 44.根据权利要求 43 所述的目标第二设备，其中，所述多个信号中第 j 个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的；所述第二处理单元，用于从所述第 j 个信号中，提取所述目标第二设备对应的目标数据段， j 为正整数；基于所述目标第二设备的标识和所述目标数据段，计算所述第 j 个信号携带的第 j 个密钥序列。

35 45.根据权利要求 38-44 任一项所述的目标第二设备，其中，所述第二通信单元，用于接收来自所述第一设备的第一消息，其中，所述第一消息携带组密钥校验信息，所述组密钥校验信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；

所述第二处理单元，用于基于所述第二组密钥计算验证信息；基于所述组密钥校验信息和所述验证信息，校验所述第二组密钥与所述第一组密钥的一致性。

40 46.根据权利要求 45 所述的目标第二设备，其中，所述第二通信单元，用于执行以下至少之一：在所述第二组密钥与所述第一组密钥一致的情况下，向所述第一设备发送第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功；在所述第二组密钥与所述第一组密钥不一致的情况下，向所述第一设备发送第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

45 47.根据权利要求 38-44 任一项所述的目标第二设备，其中，所述第二通信单元，用于接收来自所述第一设备的第四消息，其中，所述第四消息携带组密钥纠错信息，所述组密钥纠错信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；

所述第二处理单元，用于基于所述组密钥纠错信息对所述第二组密钥进行纠错，得到与所述第一组密钥一致的组密钥。

48.根据权利要求 38-47 任一项所述的目标第二设备，其中，所述第一设备为以下之一：终端设备、网络设备；所述目标第二设备为零功耗设备。

50 49.一种第一设备，包括：处理器，与所述处理器通信的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，所述指令使所述第一设备执行：向多个第二设备中的每个第二设备发送多个信号，其中，所述多个信号的射频系数为基于所述每个第二设备与所述第一设备间的信道特征计

算得到的；基于所述多个信号的相关信息，生成第一组密钥，所述第一组密钥用于所述第一设备与所述多个第二设备的通信。

50.根据权利要求 49 所述的第一设备，其中，所述指令还使所述第一设备执行：向所述每个第二设备发送组密钥生成信令；接收来自所述每个第二设备的导频信号，其中，所述导频信号为所述组密钥生成信令所对应的反射信号；基于所述每个第二设备的导频信号，计算所述每个第二设备与所述第一设备间的信道特征。

51.根据权利要求 50 所述的第一设备，其中，所述指令还使所述第一设备执行：基于所述每个第二设备与所述第一设备间的信道特征，计算一个或多个射频系数，其中，所述一个或多个射频系数中不同的射频系数对应不同的第二设备。

52.根据权利要求 51 所述的第一设备，其中，所述指令还使所述第一设备执行：基于所述一个或多个射频系数中的第 k 个射频系数，向第 k 组第二设备中的每个第二设备发送所述多个信号，其中，所述一个或多个射频系数中不同的射频系数对应所述多个第二设备的不同分组、且所述多个第二设备的不同分组中包括不同的第二设备，所述第 k 组第二设备为所述多个第二设备的一个或多个分组之一， k 为正整数。

53.根据权利要求 49-52 任一项所述的第一设备，所述指令还使所述第一设备执行：基于所述多个信号的相关信息，得到多个第一量化结果；基于所述多个第一量化结果，生成所述第一组密钥。

54.根据权利要求 53 所述的第一设备，其中，所述指令还使所述第一设备执行：基于所述多个信号中第 i 个信号的相关信息，确定所述第 i 个信号对应的第一量化范围，将所述第一量化范围对应的第一量化值作为所述多个第一量化结果中的第 i 个第一量化结果，其中，所述第一量化范围为多个第一候选量化范围中之一，所述多个第一候选量化范围中每个第一候选量化范围具备对应的第一候选量化值， i 为正整数。

55.根据权利要求 53 或 54 所述的第一设备，其中，所述多个信号的相关信息，包括以下至少之一：所述多个信号中每个信号的强度、所述每个信号的相位。

56.根据权利要求 49-52 任一项所述的第一设备，其中，所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述指令还使所述第一设备执行：基于所述多个信号中每个信号携带的密钥序列，生成所述第一组密钥。

57.根据权利要求 56 所述的第一设备，其中，所述多个信号中第 j 个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的， j 为正整数。

58.根据权利要求 49-57 任一项所述的第一设备，其中，所述多个信号用于所述每个第二设备生成第二组密钥；所述指令还使所述第一设备执行：基于所述第一组密钥，计算组密钥校验信息，其中，所述组密钥校验信息用于所述每个第二设备校验所述第二组密钥与所述第一组密钥的一致性；向所述每个第二设备发送第一消息，其中，所述第一消息携带所述组密钥校验信息。

59.根据权利要求 58 所述的第一设备，其中，所述指令还使所述第一设备执行以下之一：接收来自目标第二设备的第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功，所述目标第二设备为所述多个第二设备中之一；接收来自所述目标第二设备的第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

60.根据权利要求 49-57 任一项所述的第一设备，其中，所述多个信号用于所述每个第二设备生成第二组密钥；所述指令还使所述第一设备执行：基于所述第一组密钥，计算组密钥纠错信息，其中，所述组密钥纠错信息用于所述每个第二设备对所述第二组密钥纠错得到与所述第一组密钥一致的组密钥；向所述每个第二设备发送第四消息，其中，所述第四消息携带所述组密钥纠错信息。

61.根据权利要求 49-60 任一项所述的第一设备，其中，所述第一设备为以下之一：终端设备、网络设备；所述第二设备为零功耗设备。

62.一种目标第二设备，包括：处理器，与所述处理器通信的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，所述指令使所述目标第二设备执行：接收来自第一设备的多个信号，其中，所述多个信号的射频系数为基于所述目标第二设备与所述第一设备间的信道特征计算得到的；基于所述多个信号的相关信息，生成第二组密钥，其中，所述第二组密钥用于所述目标第二设备与所述第一设备的通信，所述第二组密钥为多个第二设备相同的密钥、且所述目标第二设备为所述多个第二设备中之一。

63.根据权利要求 62 所述的目标第二设备，其中，所述指令还使所述目标第二设备执行：接收来自所述第一设备的组密钥生成信令；向所述第一设备发送导频信号，其中，所述导频信号为所述组密

钥生成信令所对应的反射信号，所述导频信号用于所述第一设备计算所述目标第二设备与所述第一设备间的信道特征。

64.根据权利要求 62 或 63 所述的目标第二设备，其中，所述指令还使所述目标第二设备执行：基于所述多个信号的相关信息，得到多个第二量化结果；基于所述多个第二量化结果，生成所述第二组密钥。

65.根据权利要求 64 所述的目标第二设备，其中，所述指令还使所述目标第二设备执行：基于所述多个信号中第 i 个信号的相关信息，确定所述第 i 个信号对应的第二量化范围，将所述第二量化范围对应的第二量化值作为所述多个第二量化结果中的第 i 个第二量化结果，其中，所述第二量化范围为多个第二候选量化范围中之一，所述多个第二候选量化范围中每个第二候选量化范围具备对应的第二候选量化值， i 为正整数。

66.根据权利要求 64 或 65 所述的目标第二设备，其中，所述多个信号的相关信息，包括以下之一：所述多个信号中每个信号的强度、所述每个信号的相位。

67.根据权利要求 62 或 63 所述的目标第二设备，其中，所述多个信号的相关信息包括所述多个信号中每个信号携带的密钥序列；所述指令还使所述目标第二设备执行：基于所述多个信号中每个信号携带的密钥序列，生成所述第二组密钥。

68.根据权利要求 67 所述的目标第二设备，其中，所述多个信号中第 j 个信号携带一个或多个数据段，所述一个或多个数据段中不同的数据段为基于不同的第二设备的标识和第 j 个密钥序列计算的；所述指令还使所述目标第二设备执行：从所述第 j 个信号中，提取所述目标第二设备对应的目标数据段， j 为正整数；基于所述目标第二设备的标识和所述目标数据段，计算所述第 j 个信号携带的第 j 个密钥序列。

69.根据权利要求 62-68 任一项所述的目标第二设备，其中，所述指令还使所述目标第二设备执行：接收来自所述第一设备的第一消息，其中，所述第一消息携带组密钥校验信息，所述组密钥校验信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；基于所述第二组密钥计算验证信息；基于所述组密钥校验信息和所述验证信息，校验所述第二组密钥与所述第一组密钥的一致性。

70.根据权利要求 69 所述的目标第二设备，其中，所述指令还使所述目标第二设备执行以下至少之一：在所述第二组密钥与所述第一组密钥一致的情况下，向所述第一设备发送第二消息，其中，所述第二消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验成功；在所述第二组密钥与所述第一组密钥不一致的情况下，向所述第一设备发送第三消息，其中，所述第三消息用于指示所述目标第二设备对所述第二组密钥与所述第一组密钥的一致性校验失败。

71.根据权利要求 62-68 任一项所述的目标第二设备，其中，所述指令还使所述目标第二设备执行：接收来自所述第一设备的第四消息，其中，所述第四消息携带组密钥纠错信息，所述组密钥纠错信息为所述第一设备基于第一组密钥计算的，所述第一组密钥为所述第一设备基于所述多个信息生成的；基于所述组密钥纠错信息对所述第二组密钥进行纠错，得到与所述第一组密钥一致的组密钥。

72.根据权利要求 62-71 任一项所述的目标第二设备，其中，所述第一设备为以下之一：终端设备、网络设备；所述目标第二设备为零功耗设备。

73.一种芯片，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 13、或权利要求 14 至 24 中任一项所述的方法。

74.一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 13、或权利要求 14 至 24 中任一项所述的方法。

75.一种计算机程序产品，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 13、或权利要求 14 至 24 中任一项所述的方法。

76.一种计算机程序，所述计算机程序使得计算机执行如权利要求 1 至 13、或权利要求 14 至 24 中任一项所述的方法。

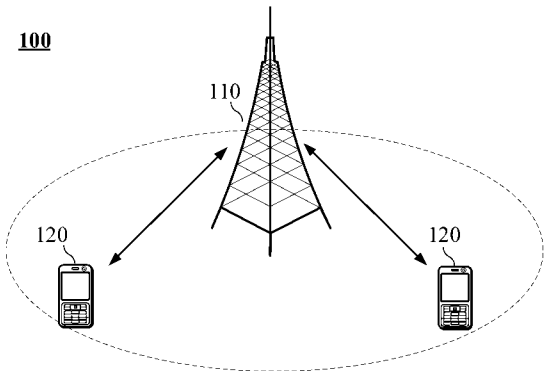


图 1

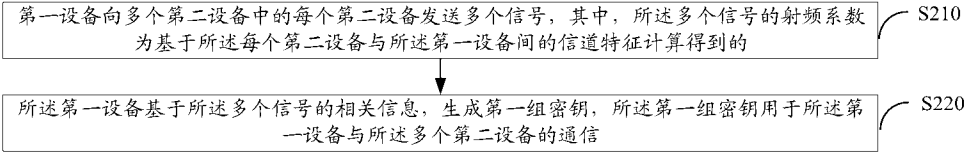


图 2

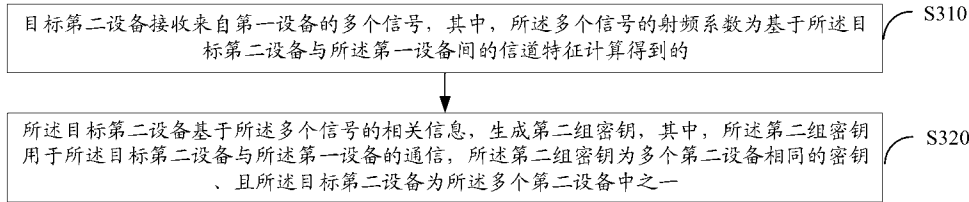


图 3

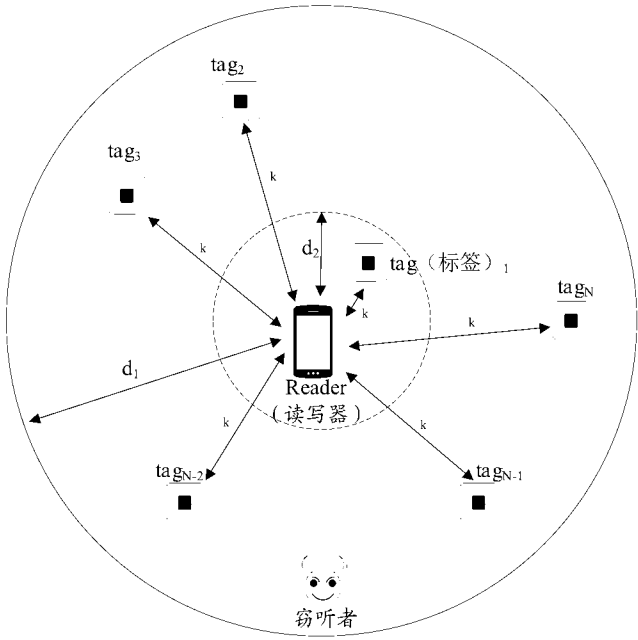


图 4

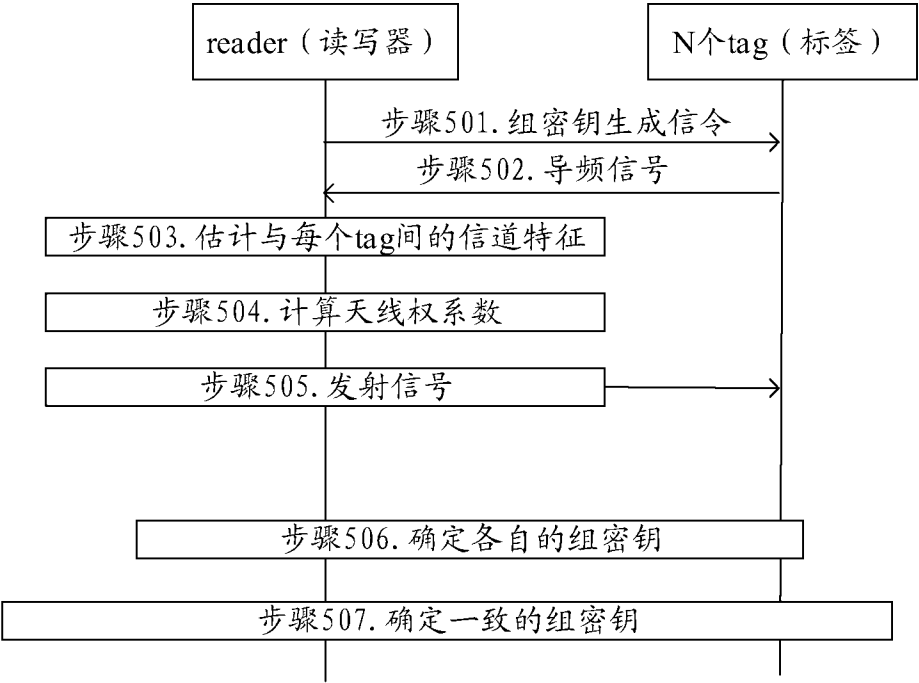


图 5

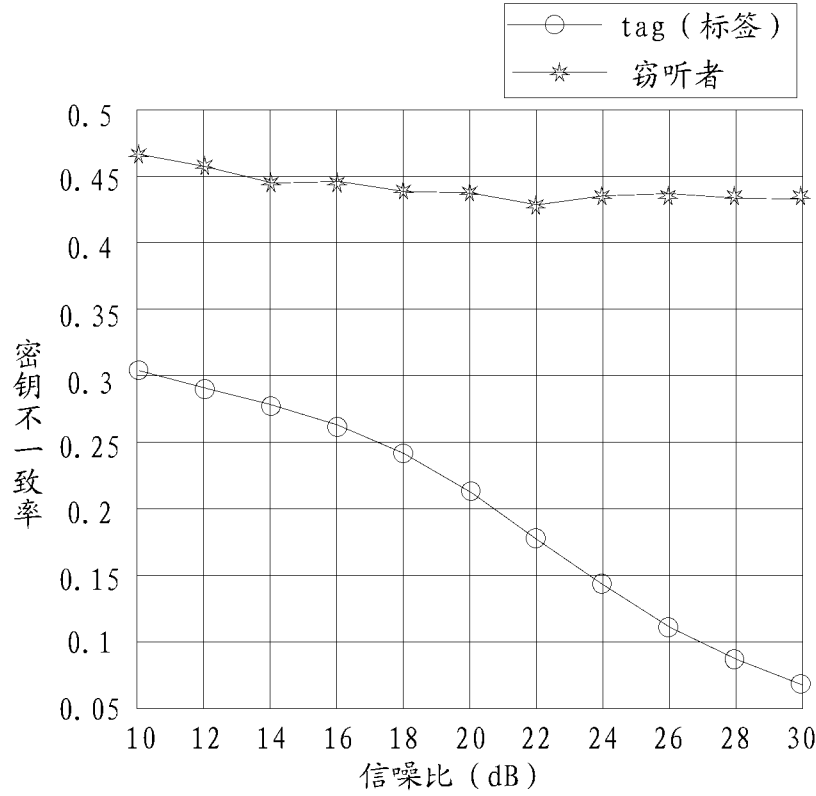


图 6

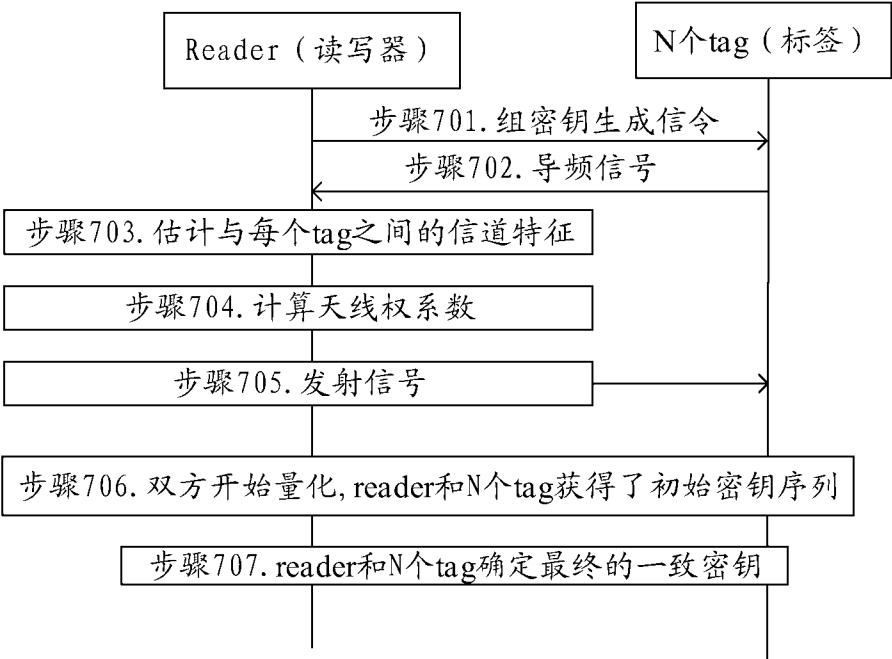


图 7

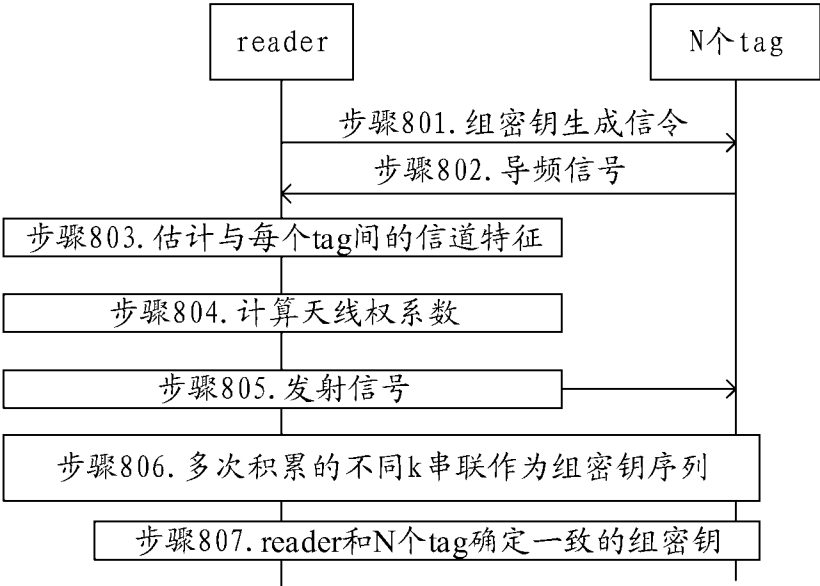


图 8

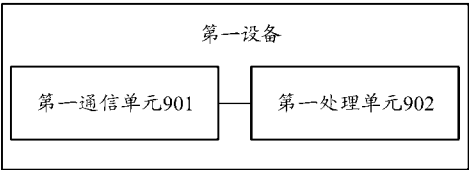


图 9

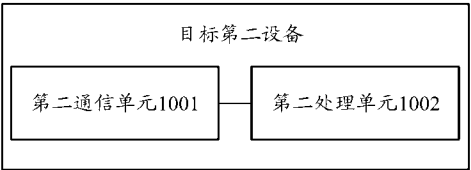


图 10

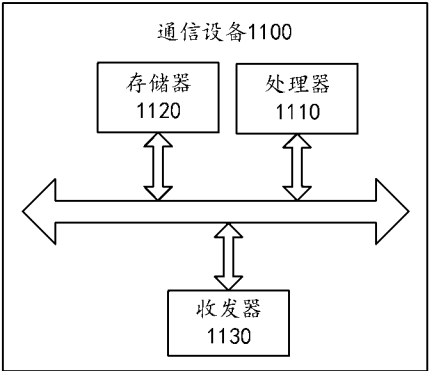


图 11

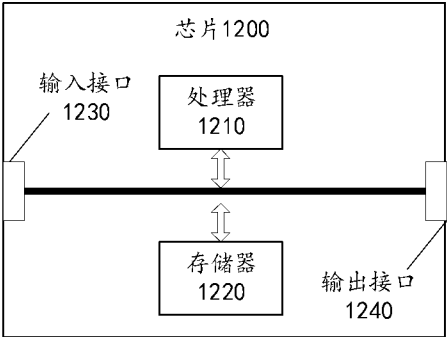


图 12

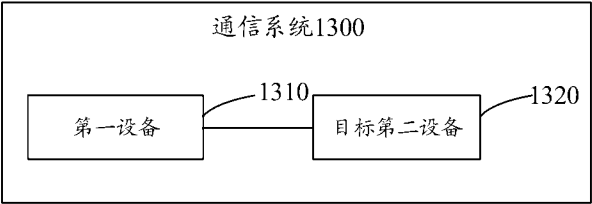


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/096686

A. CLASSIFICATION OF SUBJECT MATTER		
H04L 9/08(2006.01)i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC: H04L H04W		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
CNTXT, CNKI, ENTXT, ENTXTC, VEN, IEEE, 3GPP: 阅读器, 读写器, 读取器, 标签, 组密钥, 共享密钥, 信道特征, 信道分析, 信道估计, 损耗, 衰减, 噪声, 射频, 天线, 天线权, 发射, 传送, 传输, 增益, 权重, 系数, 因数, 因子, 强度, 相位, 量化, reader, tag?, group key, shared key, channel characteristics, channel analysis, channel estimation, loss, attenuation, noise, radio frequency, RF, antenna, antenna weight, transmission, gain, weight, coefficient, factor, strength, phase, quantiz+		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106603228 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 26 April 2017 (2017-04-26) description, paragraphs 0002-0067	1-76
A	CN 103067042 A (INFORMATION ENGINEERING UNIVERSITY OF PLA) 24 April 2013 (2013-04-24) entire document	1-76
A	CN 105721142 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 29 June 2016 (2016-06-29) entire document	1-76
A	CN 116095677 A (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE et al.) 09 May 2023 (2023-05-09) entire document	1-76
☒ 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
17 December 2023		21 December 2023
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/CN2023/096686

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014307871 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 October 2014 (2014-10-16) entire document	1-76

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/096686

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106603228	A	26 April 2017	None			
CN	103067042	A	24 April 2013	None			
CN	105721142	A	29 June 2016	None			
CN	116095677	A	09 May 2023	WO	2023078400	A1	11 May 2023
US	2014307871	A1	16 October 2014	KR	20140123723	A	23 October 2014

A. 主题的分类 H04L 9/08(2006.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) IPC: H04L H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNTXT, CNKI, ENTXT, ENTXTC, VEN, IEEE, 3GPP: 阅读器, 读写器, 读取器, 标签, 组密钥, 共享密钥, 信道特征, 信道分析, 信道估计, 损耗, 衰减, 噪声, 射频, 天线, 天线权, 发射, 传送, 传输, 增益, 权重, 系数, 因数, 因子, 强度, 相位, 量化, reader, tag2, group key, shared key, channel characteristics, channel analysis, channel estimation, loss, attenuation, noise, radio frequency, RF, antenna, antenna weight, transmission, gain, weight, coefficient, factor, strength, phase, quantiz+		
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
A	CN 106603228 A (广东工业大学) 2017年4月26日 (2017 - 04 - 26) 说明书第0002-0067段	1-76
A	CN 103067042 A (中国人民解放军信息工程大学) 2013年4月24日 (2013 - 04 - 24) 全文	1-76
A	CN 105721142 A (广东工业大学) 2016年6月29日 (2016 - 06 - 29) 全文	1-76
A	CN 116095677 A (中国移动通信有限公司研究院 等) 2023年5月9日 (2023 - 05 - 09) 全文	1-76
A	US 2014307871 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2014年10月16日 (2014 - 10 - 16) 全文	1-76
☐ 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 2023年12月17日		国际检索报告邮寄日期 2023年12月21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		授权官员 李文 电话号码 (+86) 010-53961682

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/096686

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	106603228	A	2017年4月26日	无			
CN	103067042	A	2013年4月24日	无			
CN	105721142	A	2016年6月29日	无			
CN	116095677	A	2023年5月9日	WO	2023078400	A1	2023年5月11日
US	2014307871	A1	2014年10月16日	KR	20140123723	A	2014年10月23日