

无线物理层安全通信的方法和通信装置

5 技术领域

本申请实施例涉及通信领域，并且，更具体地，涉及无线物理层安全通信的方法和通信装置。

背景技术

10 安全传输是通信的基础保障，传统的安全传输方案都是基于密钥的，密钥加密可以分为对称加密和非对称加密。对称加密双方共享密钥，非对称加密需要通信的一方将公钥传递给另一方，发端采用公钥加密，接收方采用私钥解密。无论哪种方法都需要密钥的维护和管理，密钥维护和管理需要复杂的协议支持，而协议的漏洞往往容易被攻击，使得密钥泄露，存在一定的风险。另外复杂的协议需要产生额外的通信开销和时延，无法适配未来
15 通信网络的高动态特性。

相较于传统的安全传输方案，物理层安全传输技术利用无线信道的物理特性，采取信号处理、编码调制技术等手段，能够在较小的通信开销下，实现无密钥的安全传输。

因此，提高物理层安全传输技术的安全性能对无线通信安全至关重要。

20 发明内容

本申请实施例提供一种无线物理层安全通信的方法和通信装置，能够在无密钥传输场景中，提升通信的安全性能。

第一方面，提供了一种无线物理层安全通信的方法。该方法可以由第一装置执行，第一装置可以是终端设备或网络设备，也可以是终端设备或网络设备中的芯片或电路，也可以
25 是能够实现全部或部分终端设备或网络设备功能的逻辑模块或软件，本申请对此不作限定。

该方法包括：第一装置基于第三装置的误码率对第一数据进行预处理，预处理用于使得第一装置和第二装置之间的通信达到安全等级；第一装置向第二装置发送第二数据，第二数据为对第一数据进行预处理之后得到的数据。

基于上述方案，发送端在发送数据之前，通过对待发送的数据进行预处理，该预处理
30 引入了第三装置的误码率，能够使得第一装置和第二装置之间的通信达到安全等级，从而能够提高通信安全。

另一方面，该方案能够定制安全等级，为不同的合法接收者提供差异化安全服务。比如物联网（internet of things, IoT）终端，算力有限，安全要求不高，可以利用本申请的方案定制较低的安全等级。因此，具有更强的灵活性。

35 结合第一方面，在第一方面的某些实现方式中，第一装置基于第三装置的误码率对第一数据进行预处理，包括：第一装置基于第三装置的误码率对第一数据进行分组；或，第一装置基于第三装置的误码率对第一数据进行分组并生成第一随机串。

基于上述方案，将第一数据进行分组处理，使得第一数据的各个分组都可以获得可证

明的安全强度，有助于提升通信安全。

结合第一方面，在第一方面的某些实现方式中，第一装置基于第三装置的误码率对第一数据进行分组，包括：第一装置根据误码率和安全等级确定第一数据的分组长度；第一装置以分组长度为单位对第一数据进行划分。

- 5 结合第一方面，在第一方面的某些实现方式中，该方法还包括：第一装置基于第一随机串对分组后的第一数据进行运算。

基于上述方案，在对第一数据进行预处理时，通过引入第一随机串，能够提升第一数据的传输安全。

- 10 结合第一方面，在第一方面的某些实现方式中，第一装置基于第一随机串对分组后的第一数据进行运算，包括：第一装置根据第一随机串和第二随机串获得第一比特串；第一装置基于第一比特串对分组后的第一数据进行运算。

基于上述方案，在对第一数据进行预处理和后处理时，可以以第一比特串作为等效密钥，使得第一数据的各个分组都可以获得可证明的安全强度，有助于提升通信安全。

- 15 结合第一方面，在第一方面的某些实现方式中，第一随机串的长度大于或等于分组长度，第二随机向量的长度等于第一随机串的长度。

基于上述方案，由于第一随机串的长度大于或等于分组长度，使得仅需要对第一随机串采用物理层安全传输技术，方案实现简单。

- 20 结合第一方面，在第一方面的某些实现方式中，第一随机串的长度小于分组长度，第二随机向量的长度等于分组长度。

基于上述方案，由于第一随机串的长度可以小于分组长度，使得传输速率损失小，码率较高。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：第一装置向第二装置发送第二随机串。

- 25 结合第一方面，在第一方面的某些实现方式中，分组长度为信道编码的分组大小。

基于上述方案，分组长度为信道编码的分组大小，能够减小信道编码的复杂度，便于实现。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：第一装置向第二装置发送第一信息；或，第一装置接收来自第二装置的第一信息；其中，第一信息用于指示安全等级。

- 30 基于上述方案，收发双端通过信令对齐安全等级，能够根据需求定制安全等级，灵活性更强。

结合第一方面，在第一方面的某些实现方式中，第一信息为指示信息。

结合第一方面，在第一方面的某些实现方式中，该指示信息用于指示终端设备的类型，终端设备的类型和通信安全等级之间具有对应关系。

- 35 基于上述方式，通过终端设备的类型指示安全等级，使得安全等级与终端设备的运算能力更匹配，能够减小终端的实现复杂度。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：第一装置接收来自第二装置的第二信息；或，第一装置向第二装置发送第二信息；其中，第二信息用于指示误码率。

基于上述方案，收发双端通过信令对齐误码率，便于预处理和后处理的实现。

结合第一方面，在第一方面的某些实现方式中，该第二信息为指示信息。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：第一装置确定误码率。

5 基于上述方案，第一装置能够确定误码率，使得确定的误码率更符合实际场景，当根据确定的误码率进行预处理时，能够提升当前环境中的通信安全。

结合第一方面，在第一方面的某些实现方式中，第一装置确定误码率，包括：第一装置确定受控区域，第二装置位于受控区域，第三装置位于受控区域之外；第一装置确定受控区域之外的最佳通信位置，第三装置在最佳通信位置具有最好的接收性能；第一装置根据最佳通信位置确定误码率。

10 基于上述方案，以受控区域外的最佳通信位置进行误码率估计，当根据确定的误码率进行预处理时，使得预处理的结果在第三装置的条件为最优时，仍然具有可靠的安全性能。

第二方面，提供了一种无线物理层安全通信的方法。该方法可以由第二装置执行，第二装置可以是终端设备或网络设备，也可以是终端设备或网络设备中的芯片或电路，也可以是能实现全部或部分终端设备或网络设备功能的逻辑模块或软件，本申请对此不作限定。

15 该方法包括：第二装置接收来自第一装置的第二数据；第二装置对第二数据进行后处理，得到第一数据，第二数据为基于第三装置的误码率对第一数据进行预处理之后得到的数据，预处理用于使得第一装置和第二装置之间的通信达到安全等级。

20 基于上述方案，发送端在发送数据之前，通过对待发送的数据进行预处理，该预处理引入了第三装置的误码率，能够使得第一装置和第二装置之间的通信达到安全等级，从而能够提高通信安全。

另一方面，该方案能够定制安全等级，为不同的合法接收者提供差异化安全服务。比如物联网（internet of things, IoT）终端，算力有限，安全要求不高，可以利用本申请的方案定制较低的安全等级。因此，具有更强的灵活性。

25 结合第二方面，在第二方面的某些实现方式中，第二装置对第二数据进行后处理，包括：第二装置对第二数据进行分组划分；第二装置根据第二随机串对分组划分后的第二数据进行处理。

结合第二方面，在第二方面的某些实现方式中，第二数据包括第一随机串，第二装置根据第二随机串对分组划分后的第二数据进行处理，包括：第二装置根据第一随机串和第二随机串获得第一比特串；第二装置基于第一比特串对分组划分后的第二数据进行运算。

30 基于上述方案，在对第一数据进行预处理和后处理时，可以以第一比特串作为等效密钥，使得第一数据的各个分组都可以获得可证明的安全强度，有助于提升通信安全。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：第二装置接收来自第一装置的第二随机串。

35 结合第二方面，在第二方面的某些实现方式中，该方法还包括：第二装置接收来自第一装置的第一信息；或，第二装置向第一装置发送第一信息；其中，第一信息用于指示安全等级。

基于上述方案，收发双端通过信令对齐安全等级，能够根据需求定制安全等级，灵活性更强。

结合第二方面，在第二方面的某些实现方式中，该第一信息为指示信息。

结合第二方面,在第二方面的某些实现方式中,该指示信息用于指示终端设备的类型,终端设备的类型和通信安全等级之间具有对应关系。

基于上述方式,通过终端设备的类型指示安全等级,使得安全等级与终端设备的运算能力更匹配,能够减小终端的实现复杂度。

- 5 结合第二方面,在第二方面的某些实现方式中,该方法还包括:第二装置接收来自第一装置的第二信息;或,第二装置向第一装置发送第二信息,其中,第二信息用于指示误码率。

基于上述方案,收发双端通过信令对齐误码率,便于预处理和后处理的实现。

结合第二方面,在第二方面的某些实现方式中,第二信息为指示信息。

- 10 结合第二方面,在第二方面的某些实现方式中,该方法还包括:第二装置确定误码率。

基于上述方案,第二装置也能够确定误码率,使得确定的误码率更符合实际场景,当根据确定的误码率进行预处理时,能够提升当前环境中的通信安全。

- 15 结合第二方面,在第二方面的某些实现方式中,第二装置确定误码率,包括:第二装置确定受控区域,第二装置位于受控区域,第三装置位于受控区域之外;第二装置确定受控区域之外的最佳通信位置,第三装置在最佳通信位置具有最好的接收性能;第二装置根据最佳通信位置确定误码率。

基于上述方案,以受控区域外的最佳通信位置进行误码率估计,当根据确定的误码率进行预处理时,使得预处理的结果在第三装置的条件为最优时,仍然具有可靠的安全性能。

- 20 第三方面,提供了一种通信装置。该通信装置是第一装置,第一装置可以是终端设备或网络设备,也可以是终端设备或网络设备中的芯片或电路,也可以是能实现全部或部分终端设备或网络设备功能的逻辑模块或软件,本申请对此不作限定。

- 25 第一装置可以包括收发单元和处理单元,该处理单元用于:基于第三装置的误码率对第一数据进行预处理,预处理用于使得第一装置和第二装置之间的通信达到安全等级;该收发单元用于向第二装置发送第二数据,第二数据为对第一数据进行预处理之后得到的数据。

结合第三方面,在第三方面的某些实现方式中,处理单元具体用于:基于第三装置的误码率对第一数据进行分组;或,基于第三装置的误码率对第一数据进行分组并生成第一随机串。

- 30 结合第三方面,在第三方面的某些实现方式中,处理单元具体用于:根据误码率和安全等级确定第一数据的分组长度;以分组长度为单位对第一数据进行划分。

结合第三方面,在第三方面的某些实现方式中,处理单元还用于:基于第一随机串对分组后的第一数据进行运算。

结合第三方面,在第三方面的某些实现方式中,处理单元具体用于:根据第一随机串和第二随机串获得第一比特串;基于第一比特串对分组后的第一数据进行运算。

- 35 结合第三方面,在第三方面的某些实现方式中,第一随机串的长度大于或等于分组长度,第二随机向量的长度等于第一随机串的长度。

结合第三方面,在第三方面的某些实现方式中,第一随机串的长度小于分组长度,第二随机向量的长度等于分组长度。

结合第三方面,在第三方面的某些实现方式中,收发单元还用于:向第二装置发送第

二随机串。

结合第三方面，在第三方面的某些实现方式中，分组长度为信道编码的分组大小。

结合第三方面，在第三方面的某些实现方式中，收发单元还用于：向第二装置发送第一信息；或，接收来自第二装置的第一信息；其中，第一信息用于指示安全等级。

5 结合第三方面，在第三方面的某些实现方式中，第一信息为指示信息。

结合第三方面，在第三方面的某些实现方式中，该指示信息用于指示终端设备的类型，终端设备的类型和通信安全等级之间具有对应关系。

结合第三方面，在第三方面的某些实现方式中，收发单元还用于：接收来自第二装置的第二信息；或，向第二装置发送第二信息；其中，第二信息用于指示误码率。

10 结合第三方面，在第三方面的某些实现方式中，该第二信息为指示信息。

结合第三方面，在第三方面的某些实现方式中，处理单元还用于：确定误码率。

结合第三方面，在第三方面的某些实现方式中，处理单元具体用于：确定受控区域，第二装置位于受控区域，第三装置位于受控区域之外；确定受控区域之外的最佳通信位置，第三装置在最佳通信位置具有最好的接收性能；根据最佳通信位置确定误码率。

15 第四方面，提供了一种通信装置。该通信装置是第二装置，第二装置可以是终端设备或网络设备，也可以是终端设备或网络设备中的芯片或电路，也可以是能实现全部或部分终端设备或网络设备功能的逻辑模块或软件，本申请对此不作限定。

第二装置可以包括收发单元和处理单元：该收发单元用于：接收来自第一装置的第二数据；该处理单元用于：对第二数据进行后处理，得到第一数据，第二数据为基于第三装置的误码率对第一数据进行预处理之后得到的数据，预处理用于使得第一装置和第二装置之间的通信达到安全等级。

结合第四方面，在第四方面的某些实现方式中，处理单元具体用于：对第二数据进行分组划分；根据第二随机串对分组划分后的第二数据进行处理。

25 结合第四方面，在第四方面的某些实现方式中，第二数据包括第一随机串，处理单元还用于：根据第一随机串和第二随机串获得第一比特串；基于第一比特串对分组划分后的第二数据进行运算。

结合第四方面，在第四方面的某些实现方式中，收发单元还用于：接收来自第一装置的第二随机串。

30 结合第四方面，在第四方面的某些实现方式中，收发单元还用于：接收来自第一装置的第一信息；或，向第一装置发送第一信息；其中，第一信息用于指示安全等级。

结合第四方面，在第四方面的某些实现方式中，该第一信息为指示信息。

结合第四方面，在第四方面的某些实现方式中，该指示信息用于指示终端设备的类型，终端设备的类型和通信安全等级之间具有对应关系。

35 结合第四方面，在第四方面的某些实现方式中，收发单元还用于：接收来自第一装置的第二信息；或，向第一装置发送第二信息，其中，第二信息用于指示误码率。

结合第四方面，在第四方面的某些实现方式中，第二信息为指示信息。

结合第四方面，在第四方面的某些实现方式中，处理单元还用于：确定误码率。

结合第四方面，在第四方面的某些实现方式中，处理单元具体用于：确定受控区域，第二装置位于受控区域，第三装置位于受控区域之外；确定受控区域之外的最佳通信位置，

第三装置在最佳通信位置具有最好的接收性能；根据最佳通信位置确定误码率。

第五方面，提供一种通信装置，该装置包括处理器，该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述以执行上述第一方面至第二方面中的任一方面，以及第一方面至第二方面中任一种可能实现方式中的方法。可选地，该装置还包括存储器，该存储器与处理器可能是分离部署的，也可能是集中部署的。可选地，该装置还包括通信接口，处理器与通信接口耦合。在一种实现方式中，该通信接口可以是收发器，或，输入/输出接口。

当该装置为芯片时，该通信接口可以是该芯片或芯片系统上的输入/输出接口、接口电路、输出电路、输入电路、管脚或相关电路等。该处理器也可以体现为处理电路或逻辑电路。

可选地，该收发器可以为收发电路。可选地，所述输入/输出接口可以为输入/输出电路。

在具体实现过程中，上述处理器可以为一个或多个芯片，输入电路可以为输入管脚，输出电路可以为输出管脚，处理电路可以为晶体管、门电路、触发器和各种逻辑电路等。输入电路所接收的输入的信号可以是但不限于接收器接收并输入的，输出电路所输出的信号可以是但不限于输出给发射器并由发射器发射的，且输入电路和输出电路可以是同一电路，该电路在不同的时刻分别用作输入电路和输出电路。本申请实施例对处理器及各种电路的具体实现方式不做限定。

第六方面，提供一种通信装置，该装置包括逻辑电路和输入/输出接口，该逻辑电路用于与输入/输出接口耦合，通过该输入/输出接口传输数据，以执行上述第一方面至第二方面中的任一方面，以及第一方面至第二方面中任一种可能实现方式中的方法。

第七方面，提供一种通信系统，该系统包括上述第三方面或第三方面中的任一种可能的实现方式中的第一装置，以及第四方面或第四方面中的任一种可能的实现方式中的第二装置。

第八方面，提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序（也可以称为代码，或指令）当其在计算机上运行时，使得计算机执行上述第一方面至第二方面中的任一方面，以及第一方面至第二方面中任一种可能实现方式中的方法。

第九方面，提供了一种计算机程序产品，该计算机程序产品包括：计算机程序（也可以称为代码，或指令），当该计算机程序被运行时，使得计算机执行上述第一方面至第二方面中的任一方面，以及第一方面至第二方面中任一种可能实现方式中的方法。

上述第三方面至第九方面带来的有益效果可以参考第一方面至第二方面中有益效果的描述，此处不再赘述。

附图说明

图 1 是适用于本申请实施例的通信方法的通信系统 100 的示意图。

图 2 是本申请实施例提供的装置的结构示意图。

图 3 是利用人工噪声实现物理层安全传输的示意图。

图 4 是通过人工噪声造成 UE#2 和 UE#3 的误码率的一种示意图。

图 5 是本申请实施例提供的一种无线物理层安全通信的方法 200 的流程交互图

图 6 是本申请实施例提供的预处理的过程的示意图。

图 7 是本申请实施例提供的后处理的过程的示意图。

图 8 是本申请的数据传输的流程示意图。

图 9 示出了受控区域的一种示意图。

5 图 10 示出了本申请提供的一种无线物理层安全通信的方法 300。

图 11 示出了本申请提供的一种无线物理层安全通信的方法 400。

图 12 是本申请实施例提供的通信装置的示意性框图。

图 13 示出了本申请实施例提供的一种通信装置 600。

图 14 示出了本申请实施例提供的一种通信装置 700。

10

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

本申请实施例的技术方案可以应用于各种通信系统，例如：全球移动通讯（Global System of Mobile communication, GSM）系统、码分多址（Code Division Multiple Access, CDMA）系统、宽带码分多址（Wideband Code Division Multiple Access, WCDMA）系统、通用分组无线业务（General Packet Radio Service, GPRS）、长期演进（Long Term Evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、第五代（5th Generation, 5G）移动通信系统或新空口（new radio, NR）、无线局域网（wireless local area network, WLAN）系统、无线保真（wireless fidelity, WiFi）系统。其中，5G 移动通信系统可以是非独立组网（non-standalone, NSA）或独立组网（standalone, SA）。

本申请提供的技术方案还可以应用于机器类通信（machine type communication, MTC）、机器间通信长期演进技术（long term evolution-machine, LTE-M）、设备到设备（device-to-device, D2D）网络、机器到机器（machine to machine, M2M）网络、物联网（internet of things, IoT）网络或者其他网络。其中，IoT 网络例如可以包括车联网。其中，车联网系统中的通信方式统称为车到其他设备（vehicle to X, V2X, X 可以代表任何事物），例如，该 V2X 可以包括：车辆到车辆（vehicle to vehicle, V2V）通信，车辆与基础设施（vehicle to infrastructure, V2I）通信、车辆与行人之间的通信（vehicle to pedestrian, V2P）或车辆与网络（vehicle to network, V2N）通信等。

本申请提供的技术方案还可以应用于未来的通信系统，如第六代（6th Generation, 6G）移动通信系统等。本申请对此不作限定。

在本申请实施例中，终端设备也可以称为用户设备（user equipment, UE）、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。

终端设备可以是一种向用户提供语音/数据连通性的设备，例如，具有无线连接功能的手持式设备、车载设备等。目前，一些终端的举例可以为：手机（mobile phone）、平板电脑（pad）、带无线收发功能的电脑（如笔记本电脑、掌上电脑等）、移动互联网设备（mobile

internet device, MID)、虚拟现实(virtual reality, VR)设备、增强现实(augmented reality, AR)设备、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程医疗(remote medical)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无线终端(例如,电视机等家电、智慧盒子、游戏机)、蜂窝电话、无绳电话、会话启动协议(session initiation protocol, SIP)电话、无线本地环路(wireless local loop, WLL)站、个人数字助理(personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备, 5G 网络中的终端设备或者未来演进的公用陆地移动通信网络(public land mobile network, PLMN)中的终端设备等。终端设备还可以是无线保真(wireless fidelity, WiFi)系统中的非接入点的站点(station, STA)。

其中,可穿戴设备也可以称为穿戴式智能设备,是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称,如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上,或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备,更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能,例如:智能手表或智能眼镜等,以及只专注于某一类应用功能,需要和其它设备如智能手机配合使用,如各类进行体征监测的智能手环、智能首饰等。

此外,终端设备还可以是物联网(Internet of things, IoT)系统中的终端设备。IoT 是未来信息技术发展的重要组成部分,其主要技术特点是将物品通过通信技术与网络连接,从而实现人机互连,物物互连的智能化网络。IoT 技术可以通过例如窄带(narrow band, NB)技术,做到海量连接,深度覆盖,终端省电。

在本申请实施例中,该终端设备还可以是车辆或整车,通过车联网可以实现通信,也可以是位于车辆内(例如放置在车辆内或安装在车辆内)的部件,即车载终端设备、车载模块或者车载单元(on-board unit, OBU)。

此外,终端设备还可以包括智能打印机、火车探测器、加油站等传感器,主要功能包括收集数据(部分终端设备)、接收网络设备的控制信息与下行数据,并发送电磁波,向网络设备传输上行数据。

本申请实施例中,网络设备可以是任意一种具有无线收发功能的设备。该设备包括但不限于:演进型节点 B(evolved Node B, eNB)、无线网络控制器(radio network controller, RNC)、节点 B(Node B, NB)、基站控制器(base station controller, BSC)、基站收发台(base transceiver station, BTS)、家庭基站(例如, home evolved NodeB, 或 home Node B, HNB)、基带单元(baseband unit, BBU),无线保真(wireless fidelity, WiFi)系统中的接入点(access point, AP)、无线中继节点、无线回传节点、传输点(transmission point, TP)或者发送接收点(transmission and reception point, TRP)等,还可以为 5G,如, NR, 系统中的 gNB,或,传输点(TRP 或 TP), 5G 系统中的基站的一个或一组(包括多个天线面板)天线面板,或者,还可以为构成 gNB 或传输点的网络节点,如基带单元(BBU),或,分布式单元(distributed unit, DU),或者下一代通信 6G 系统中的基站等。

在一些部署中, gNB 可以包括集中式单元(centralized unit, CU)和 DU。gNB 还可

以包括有源天线单元 (active antenna unit, AAU)。CU 实现 gNB 的部分功能, DU 实现 gNB 的部分功能。比如, CU 负责处理非实时协议和服务, 实现无线资源控制 (radio resource control, RRC), 分组数据汇聚层协议 (packet data convergence protocol, PDCP) 层的功能。DU 负责处理物理层协议和实时服务, 实现无线链路控制 (radio link control, RLC) 层、媒体接入控制 (medium access control, MAC) 层和物理 (physical, PHY) 层的功能。AAU 实现部分物理层处理功能、射频处理及有源天线的相关功能。由于 RRC 层的信息最终会变成 PHY 层的信息, 或者, 由 PHY 层的信息转变而来, 因而, 在这种架构下, 高层信令, 如 RRC 层信令, 也可以认为是由 DU 发送的, 或者, 由 DU 和 CU 发送的。可以理解的是, 网络设备可以为包括 CU 节点、DU 节点、AAU 节点中一项或多项的设备。此外, 10 可以将 CU 划分为接入网 (radio access network, RAN) 中的网络设备, 也可以将 CU 划分为核心网 (core network, CN) 中的网络设备, 本申请对此不做限定。

网络设备为小区提供服务, 终端设备通过网络设备分配的传输资源 (例如, 频域资源, 或者说, 频谱资源) 与小区进行通信, 该小区可以属于宏基站 (例如, 宏 eNB 或宏 gNB 等), 也可以属于小小区 (small cell) 对应的基站, 这里的小小区可以包括: 城市小区 (metro cell)、15 微小区 (micro cell)、微微小区 (pico cell)、毫微微小区 (femto cell) 等, 这些小小区具有覆盖范围小、发射功率低的特点, 适用于提供高速率的数据传输服务。

图 1 是适用于本申请实施例的通信方法的通信系统 100 的示意图。如图 1 所示, 该通信系统 100 可以包括至少一个网络设备, 例如图 1 所示的网络设备 110; 该通信系统 100 还可以包括至少一个终端设备, 例如图 1 所示的终端设备 120。网络设备 110 与终端设备 20 120 可通过无线链路通信。各通信设备, 如网络设备 110 或终端设备 120, 均可以配置多个天线。对于该通信系统中的每一个通信设备而言, 所配置的多个天线可以包括至少一个用于发送信号的发送天线和至少一个用于接收信号的接收天线。因此, 该通信系统中的各通信设备之间, 网络设备 110 与终端设备 120 之间, 可通过多天线技术通信。

应理解, 图 1 仅为便于理解而示例的简化示意图, 该通信系统中还可以包括其他网络设备或者还可以包括其他终端设备, 图 1 中未予以画出。

还应理解, 图 1 所示的通信系统 100 仅为本申请实施例的应用场景的一种示例, 本申请还可以适用于任意两个设备之间的通信, 例如, 适用于终端设备与终端设备的通信, 也可以适用于网络设备与网络设备之间的通信。

图 2 是本申请实施例提供的装置的结构示意图。其中, 该装置可以是终端设备, 也可以是网络设备, 该装置的内部功能模块包括预处理/后处理模块、物理层 (physical layer, PHY) 处理模块、天线等。其中, 预处理/后处理模块可以位于物理层之上的任一层中, 例如, 可以位于媒体接入控制 (media access control, MAC) 层。对于发送端, 在信道编码之前, 预处理/后处理模块可以对待发送数据进行预处理, 对于接收端, 在信道译码之后, 预处理/后处理模块可以对接收到的数据进行后处理。可以理解, 图 2 提供的装置的示意图 30 35 为一种示例, 不构成对本申请装置的限定。关于预处理和后处理的具体过程详见方法 200。

安全传输是通信的基础保障, 传统的安全传输方案都是基于密钥的, 分为对称加密和非对称加密。对称加密双方共享密钥, 非对称加密需要通信的一方将公钥传递给另一方, 发端采用公钥加密, 接收方采用私钥解密。无论哪种方法都需要密钥的维护和管理, 密钥维护和管理需要复杂的协议支持, 而协议的漏洞往往容易被攻击, 使得密钥泄露, 存在一

定的安全风险。另外复杂的协议需要产生额外的通信开销和时延，无法适配未来通信网络的高动态特性。

在当前无线通信协议中，物理层和 MAC 层的控制信令是没有基于密钥加密的，例如，有些信令是在密钥协商之前，因此无法采用基于密钥的安全通信手段。相较于传统的安全传输方案，物理层安全传输技术利用无线信道的物理特性，采取信号处理、编码、调制等手段，能够在较小的通信开销下，实现无密钥的安全传输。

具体来说，物理层安全传输是一种无密钥的安全传输方案。物理层安全传输是在物理层通过信号处理方式获得信道优势，使得合法信道的质量优于非法信道，进而实现合法双方在不用共享密钥的情况下秘密通信。物理层安全传输技术，例如，可以是指信道编码、人工噪声、预编码和波形调制等，物理层安全传输技术可以概括为使得非法接收端产生误码平台的技术。

图 3 是利用人工噪声实现物理层安全传输的一种示意图。如图 3 所示，gNB（第一装置的一例）需要实现与 UE#1（第二装置的一例）之间的安全通信，使得 UE#2（第三装置的一例）和 UE#3（第三装置的又一例）均无法获得 gNB 与 UE#1 之间传输的信息，因此，gNB 与 UE#1 之间的信道为合法信道，gNB 与 UE#2 之间的信道和 gNB 与 UE#3 之间的信道均为非法信道。一种实现的方式是，通过人工噪声对 UE#2 和 UE#3 进行干扰。人工噪声是通过多天预编码的方法，在合法信道的零空间注入噪声信号，导致非法信道的接收者（简称为非法接收者，例如，图 3 中的 UE#2 和 UE#3）产生误码平台，且不会对合法信道的接收者（简称为合法接收者，例如，图 3 中的 UE#1）产生干扰。具体见图 4。

图 4 是 UE#2 和 UE#3 的误码率的一种示意图。如图 4 所示，z 轴表示误码率（bit error rate, BER） P_e ，X 轴和 Y 轴表示水平面上两个互相垂直的方向，例如，X 轴表示南北方向，Y 轴表示东西方向，通过（X，Y）可以确定水平面上的一个位置，坐标原点（0，0）为合法接收者 UE#1 的位置，非法接收者 UE#2 和 UE#3 可以位于除了坐标原点以外的任意位置。由图 4 可以看出，在坐标原点以外的巨大多数位置，UE#2 和 UE#3 的误码率均达到 0.2，即产生了误码平台（floor），这能够增大破译难度。

然而，仅基于上述物理层安全传输技术，非法接收者的误码平台的提升空间有限，使得通信的安全性无法保证。因此，提高物理层安全传输技术的安全性能对无线通信安全至关重要。

有鉴于此，本申请提供一种无线物理层安全通信的方法和通信装置，该方案通过建立误码率和安全等级的关联，能够提高通信的安全性能。

图 5 是本申请实施例提供的一种无线物理层安全通信的方法的流程交互图。图 5 所示的方法 200 可以适用于图 1 至图 3 所示的系统或装置，该方法 200 包括以下步骤。

S210，第一装置对第一数据进行预处理。

其中，第一数据为待发送的数据，例如，第一数据可以是 MAC 层数据。第一数据也可以称为待发送消息，其可以是控制信令。

其中，该预处理基于第三装置的误码率，且该预处理用于使得第一装置和第二装置之间的通信达到安全等级。或者说，误码率和安全等级之间存在对应关系，第一装置能够基于该对应关系进行预处理，该误码率为第三装置的误码率，该安全等级为第一装置和第二装置之间的通信所需要的达到的安全等级。或者说，预处理通过随机提取器实现。应理解，

物理层安全传输技术通过在非法信道上引入随机熵,使得非法接收端产生误码率平台。随机提取器可以提取并扩散物理层安全传输技术在非法信道上引入的随机熵,得到近似均匀分布的等效密钥,该等效密钥可以使得第一数据的各个比特都获得可证明的安全强度。

具体地,第三装置的误码率可以理解为第三装置对物理层数据的解析产生的误码率。
5 具体地,第一装置和第二装置之间的通信达的安全等级,可以理解为第三装置暴力破解获得第一数据所产生的计算复杂度。例如,第一装置和第二装置之间的通信的安全等级为128,表示第三装置暴力破解需要的次数是 2^{128} 。

第一装置为第一数据的发送端,第二装置为第一数据的接收端,第一装置和第二装置之间的信道为合法信道,第二装置也可以称为第一数据的合法接收端或目标接收端。第一
10 装置和第三装置之间的信道为非法信道,换言之,第三装置为第一数据的非法接收端或非目标接收端。应理解,第三装置可以是真实存在的设备,也可以是假设的设备。

可选地,在一种实施场景中,第一装置为网络设备#1,第二装置为终端设备#1,第三装置可以为终端设备#2或网络设备#2。在又一种实施场景中,第一装置为终端设备#1,第二装置为网络设备#1,第三装置可以为网络设备#2或终端设备#2。在又一种实施场景中,
15 第一装置为终端设备#1,第二装置为终端设备#2,第三装置可以为终端设备#3。在又一种实施场景中,第一装置为网络设备#1,第二装置为网络设备#2,第三装置可以为网络设备#3。以上实施场景仅为示例,并不构成本申请的限定。

在安全通信领域,第一装置可以理解为 Alice,第二装置可以理解为 Bob,第三装置可以理解为 Eve。

20 S220,第一装置向第二装置发送第二数据,相应地,第二装置接收第二数据。

其中,第二数据为对第一数据进行预处理之后得到的数据,预处理可以理解为对第一数据进行加密。应理解,第二数据为物理层数据。

可选地,第一装置可以通过物理层安全传输技术发送第二数据的全部比特,也可以通过物理层安全传输技术发送第二数据的部分比特,并通过传统物理层传输技术发送第二数
25 据的剩余比特。其中,传统物理层传输技术,可以理解为不会使得非法接收端产生误码平台的技术。

基于上述方案,发送端在发送数据之前,通过对待发送的数据进行预处理,该预处理不仅引入了第三装置的误码率,还能够使得第一装置和第二装置之间的通信达到安全等级,从而能够提高通信安全。对比而言,在现有技术中,仅考虑误码率,无法说明通过物理层
30 安全传输技术可以保证安全性。

具体地,在现有的物理层安全传输技术中,考虑了误码率,使得第三装置的误码率可以达到一定水平,但是误码率并不等同于安全性,比如误码率为0.3,仅仅表示100个比特可能有30个是错误的,但是从安全性角度,这30个比特是有可能恢复出100个比特的。在本申请中,通过预处理,一方面可以提升误码率,比如,可以将误码率从0.3提高
35 为0.5。另一方面提升后的误码率可以被证明达到一定的安全等级,比如,安全等级是128,表示第三装置暴力破解需要的次数是 2^{128} ,从而能够提升通信安全。

另一方面,该方案能够定制安全等级,为不同的合法接收者提供差异化安全服务。比如IoT终端,算力有限,安全要求不高,可以利用本申请的方案定制较低的安全等级。因此,具有更强的灵活性。

可选地,该方法还包括: S230,第二装置对第二数据进行后处理,得到第一数据。

具体地,第二装置在进行调制解调、信道译码等物理层安全传输技术后,可以获得第二数据,第二装置可以进一步对第二数据进行后处理,得到第一数据。

其中,后处理可以理解为预处理的逆运算,即对第二数据进行解密,获得第一数据。

5 作为 S210 的一种实现方式,第一装置基于第三装置的误码率对第一数据进行预处理,包括:第一装置基于第三装置的误码率对第一数据进行分组并生成第一随机串。

其中,第一装置基于第三装置的误码率对第一数据进行分组,包括:第一装置根据误码率和安全等级确定第一数据的分组长度,并以分组长度为单位对第一数据进行划分。第一装置基于第三装置的误码率生成第一随机串,包括:第一装置根据误码率和安全等级确定随机串的长度 r ,并以长度 r 生成第一随机串。

具体地,误码率、安全等级、分组长度 b 和随机串的长度 r 之间具有对应关系,确定误码率和安全等级后,随机串的长度 r 和分组长度 b 的取值可以给定一个然后计算另一个。

15 可选地,分组长度为信道编码的分组大小。换言之,第一装置在对第一数据进行分组时,可以以信道编码的分组大小作为第一数据的分组长度。其中,信道编码也是将比特流进行分组处理,分组后每个分组的比特数就是信道编码的分组大小或者信道编码的分组长度。

20 可选地,确定误码率、安全等级和分组长度 b 之后,在满足误码率、安全等级、分组长度 b 和随机串的长度 r 之间的对应关系的前提下,随机串的长度 r 的取值可以为 b 的整数倍。

可选地,在该实现方式中,第一装置基于第三装置的误码率对第一数据进行预处理,还包括:第一装置基于第一随机串对分组后的第一数据进行运算。

具体地,第一装置可以根据第一随机串(r_i)和第二随机串(S)获得第一比特串(k_i),并基于第一比特串(k_i)对分组后的第一数据(m_i)进行运算,得到第三数据(c_i)。

25 其中,第二随机串(S)可以是公开的。第二随机串可以是收发双方采用某种同步机制产生的双方已知的随机数,同步机制也可以是公开的。例如,第二随机串可以由发送端确定,然后在消息中发送给接收端。也可以由接收端确定,然后在消息中发送给发送端。

具体地,第一装置根据第一随机串(r_i)和第二随机串(S)获得第一比特串(k_i)可以分为以下两种情况:

30 情况 1: 随机串的长度 r 大于或等于分组长度 b 。

在这种情况下,第二随机串(S)的长度可以与第一随机串(r_i)的长度相同,且在根据第一随机串(r_i)和第二随机串(S)获得第一比特串(k_i)时,可以对第一随机串(r_i)和第二随机串(S)的运算结果取前 b 个比特,即为第一比特串。换言之,第一比特串的长度等于分组长度 b 。

35 情况 2: 随机串的长度 r 小于分组长度 b 。

在这种情况下,第二随机串(S)的长度可以与分组长度 b 相同,且在根据第一随机串(r_i)和第二随机串(S)获得第一比特串(k_i)时,可以先补充第一随机串(r_i),使得补充后的第一随机串的长度与分组长度 b 相同,补充的方式可以是:对第一随机串级联 $(b-r)$ 个 0。补充后的第一随机串和第二随机串(S)的运算结果即为第一比特串。换

言之，第一比特串的长度等于分组长度 b 。

通过这种方式，由于第三数据是基于第一比特串 (k_i) 对分组后的第一数据 (m_i) 进行运算得到的，而第一比特串根据第一随机串和第二随机串获得，如此，第一比特串可以理解为等效密钥，通过第一比特串能够扩散随机熵，提升第三装置的误码率。

- 5 应理解，所谓提升第三装置的误码率，指的是，在预处理时使用的第三装置的误码率为 a ，非法接收端解码预处理后的第二数据时，产生的误码率将大于 a 。

可选地，在该实现方式中，第二数据包括第一随机串 (r_i) 和第三数据。

- 具体地，可以对第一随机串 (r_i) 和第三数据进行级联操作，所谓级联操作，可以理解为将第一随机串和第三数据按照任意顺序串联起来。例如，第一随机串为 $r=010$ ，第三数据为 $c=110$ ，级联操作得到的比特串可以是 010110 ，也可以是 110010 ，级联的顺序双方保持一致即可，可以采用预配置的形式。
- 10 作为 S230 的一种实现方式，第二装置对第二数据进行后处理，包括：第一装置对第二数据进行分组划分，获得第一随机串和第三数据。

- 具体地，对第二数据进行分组划分可以理解为级联操作的逆操作，第二装置已知级联的顺序，因此通过分组划分能够拆分第二数据，获得第一随机串和第三数据。
- 15 可选地，在该实现方式中，第二装置对第二数据进行后处理，还包括：第二装置根据第二随机串对分组划分后的第二数据进行处理。

- 具体地，由于第二数据包括第一随机串，且第二装置已知第二随机串，因此，第二装置也可以根据第一随机串和第二随机串 (S) 获得第一比特串 (k_i)。进一步，第二装置可以基于第一比特串 (k_i) 对第三数据进行运算，得到分组后的第一数据。在进一步，第二装置对分组后的第一数据进行级联，可得到第一数据。
- 20 其中，根据随机串的长度 r 与分组长度 b 的大小关系，第二装置确定第一比特串也分为两种情况，即随机串的长度 r 大于或等于分组长度 b 的情况，以及随机串的长度 r 小于分组长度 b 的情况，具体过程可参考上述情况 1 和情况 2，在此不赘述。

- 25 下面举例对预处理和后处理的过程进行详细说明。

作为该实现方式的第一示例，误码率和安全等级之间的对应关系为：

$$b \leq r \cdot \log \frac{1}{1-p_e} - 2\lambda + 2 \quad (1)$$

其中， b 表示分组长度， r 表示随机串的长度， p_e 表示第三装置的误码率， λ 表示安全等级，例如， λ 的取值可以为 128 或 256 等。

- 30 根据式 (1)，可以通过安全等级，第三装置的误码率定制化分组长度。由式 (1) 可以看出， $r > b$ ，比如 $r=1000$ ， $p_e=0.2$ ， b 的最大值为 67。

具体地，预处理的过程如下：

1. 输入待发送消息 $M \in \{0,1\}^l$ ，待发送消息 M 的长度为 l ，将其按照消息分组长度 b 划分，得到 $q = \lceil l/b \rceil$ 个消息分组，记为 m_i ， i 为整数， i 的取值为 $1, 2, \dots, q$ 。
- 35 2. 生成 q 个随机比特串，记为 r_i ， $r_i \in \{0,1\}^r$ ，长度为 r ，生成方法可以是任意随机数发生器。
3. 提取操作 H: $k_i = (S \odot r_i)|_b$ ，其中， $\odot$ 表示在有限域 $GF(2^r)$ 上的乘法， $|_b$ 表示取比特串的前 b 个比特。 $S \in \{0,1\}^r$ ，即 S 为长度为 r 的随机比特串。

4. 计算 $c_i = m_i \oplus k_i$, 其中, $\oplus$ 表示异或运算。
5. 级联操作: $r_1 || c_1 || \dots || r_q || c_q$, “||”表示级联操作, 顺序不做要求, 收发双方规定好即可。预处理输出级联的比特串。

相应地, 后处理的过程具体如下:

- 5 1. 经过纠错码, 分组划分得到 r_i 和 c_i , 并已知 S 。
2. 提取器操作: $k_i = (S \odot r_i)|_b$ 。
3. 计算 $m_i = c_i \oplus k_i$, 其中, $\oplus$ 表示异或运算。
4. 得到消息 $M = m_1 || m_2 || \dots || m_q$ 。

10 在该示例中, 待发送消息 M 为第一数据的一例, c_i 为第三数据的一例, r_i 为第一随机串的一例, S 为第二随机串的一例, k_i 为第一比特串的一例, r_i 和 c_i 级联后的数据为第二数据的一例。在发送级第二数据时, 由于随机串的长度 r 大于分组长度 b , 因此实现简单, 可以采用物理层安全传输技术发送随机串 r_i , 对第三数据 c_i 可以仍采用传统物理层传输技术。

作为该实现方式的第二示例, 误码率和安全等级之间的对应关系为:

$$15 \quad b \leq \frac{r \cdot \log \frac{1}{1-p_e} - 2\lambda + 2}{1 - \log \frac{1}{1-p_e}} \quad (2)$$

其中, b 、 r 、 p_e 、 λ 的含义与式 (1) 相同。根据式 (2) 可以通过安全等级、第三装置的误码率定制化分组长度。由式 (2) 可以看出, 存在两种情况, $r \geq b$ 的情况和 $r < b$ 的情况。

20 其中, 对于 $r \geq b$ 的情况, 第二示例和第一示例的预处理、后处理过程基本类似, 第二示例的预处理、后处理过程等都可以参考第一示例, 在此不赘述。

下面对第二示例中, $r < b$ 的情况作出说明。

具体地, 预处理的过程如下:

1. 输入待发送消息 $M \in \{0,1\}^l$, 待发送消息 M 的长度为 l , 将其按照消息分组长度 b 划分, 得到 $q = \lfloor l/b \rfloor$ 个消息分组, 记为 m_i , i 为整数, i 的取值为 $1, 2, \dots, q$ 。
- 25 2. 生成 q 个随机比特串, 记为 $r_i \in \{0,1\}^r$, 长度为 r , 生成方法可以是任意随机数发生器。
3. 提取操作 H: $k_i = S \odot (r_i || 0^{b-r})$, 其中 $\odot$ 表示在有限域 $GF(2^r)$ 上的乘法。 $S \in \{0,1\}^b$, 即 S 为 b 长的随机比特串, $||0^{b-r}$ 表示串联 $(b-r)$ 个 0。
4. 计算 $c_i = m_i \oplus k_i$, 其中, $\oplus$ 表示异或运算。
- 30 5. 级联操作: $r_1 || c_1 || \dots || r_q || c_q$, “||”表示级联操作, 顺序不做要求, 双方规定好即可。预处理输出级联的比特串。

相应地, 后处理的过程具体如下:

1. 经过纠错码, 分组划分得到 r_i 和 c_i , 并已知 S 。
2. 提取器操作: $k_i = S \odot (r_i || 0^{b-r})$ 。
- 35 3. 计算 $m_i = c_i \oplus k_i$, 其中, $\oplus$ 表示异或运算。
4. 得到消息 $M = m_1 || m_2 || \dots || m_q$ 。

在该示例中，待发送消息 M 为第一数据的一例， c_i 为第三数据的一例， r_i 和 c_i 级联后的数据为第二数据的一例。此外，在 $r < b$ 的情况中，在发送级第二数据时，由于随机串的长度 r 小于分组长度 b ，使得速率损失较小，码率更高，可以采用物理层安全传输技术发送随机串 r_i 和第三数据 c_i 。

- 5 作为 S210 的一种实现方式，第一装置基于第三装置的误码率对第一数据进行预处理，包括：第一装置基于第三装置的误码率对第一数据进行分组。

作为该实现方式的一个示例，误码率和安全等级之间的对应关系为：

$$b \leq \frac{\lambda}{\log \frac{1}{1-p_e}} \quad (3)$$

- 10 其中， b 、 p_e 、 λ 的含义与式 (1) 相同。根据式 (3)，可以通过安全等级、第三装置的误码率定制化分组长度。具体的预处理和后处理方式可以参考上文公式 (1) 和公式 (2) 对应的预处理和后处理方式，不同之处在于，使用公式 (3) 进行预处理时，可以不生成第一随机串，预处理之后，也可以只发送第三数据 c_i ，即不需要发送第一随机串 r_i ，且第三数据 c_i 可以仍采用传统物理层传输技术。

下面结合图 6 至图 7 对预处理和后处理的过程进行说明。

- 15 图 6 是本申请实施例提供的预处理的过程的示意图。如图 6 所示，第一装置分组后的第一数据记为 m_i ，生成的随机串 r_i (第一随机串的一例) 通过提取操作 (图 6 中的 H 操作) 可以得到比特串 k_i (第一比特串的一例)，通过 k_i 对 m_i 进行运算，得到的数据记为 c_i ，即物理层数据，可以将 c_i 和 r_i 进行物理层处理，包括但不限于信道编码等，然后发送至接收端。

- 20 图 7 是本申请实施例提供的后处理的过程的示意图。如图 7 所示，接收端接收的数据经过物理层处理得到随机串 r_i 和 c_i ，其中，物理层处理包括但不限于信道译码，此外，随机串 r_i 通过提取操作 (图 7 中的 H 操作) 可以得到比特串 k_i ，通过 k_i 对 c_i 进行运算，可以得到分组后的第一数据 m_i 。

- 25 应理解，图 6 和图 7 中的 k_i 可以理解为等效密钥，通过随机串 r_i ，可以提取并扩散物理层安全传输技术在非法信道上引入的随机熵，得到近似均匀分布的等效密钥 k_i ，通过该等效密钥 k_i 对分组后的第一数据进行预处理，可以使得第一数据的各个比特都获得可证明的安全强度。

- 30 图 8 是本申请的数据传输的流程示意图。如图 8 所示，待发送的第一数据经过预处理后依次进入信道编码流程、波形调制流程、多输入多输出 (multiple input multiple output, MIMO) 流程后，经过无线信道发送至接收端，接收端接收到的数据依次经过 MIMO 流程、波形调制流程、信道编码流程后，经过后处理，可以得到待发送的第一数据。其中，在预处理的过程中，考虑了第三装置的误码率。

可选地，在上述任一种实现方式中，该方法 200 还包括：第一装置向第二装置发送第一信息，或，第一装置接收来自第二装置的第一信息，其中，第一信息用于指示安全等级。

- 35 具体地，第一信息可以为指示信息。作为一个示例，指示信息为安全等级的索引，第一信息和安全等级之间具有对应关系。作为又一例示例，指示信息为终端设备的类型的索引，或者说，该指示信息可以用于指示终端设备的类型，终端设备的类型和通信安全等级

之间具有对应关系。其中，终端设备的类型，可以是手机、可穿戴设备、或 IoT 终端等。发送端发送第一信息后，通过第一信息，接收端可以获知安全等级，发送端可以是第一装置，也可以是第二装置。

5 可选地，在上述任一种实现方式中，该方法 200 还包括：第一装置接收来自第二装置的第二信息，或，第一装置向第二装置发送的第二信息，其中，第二信息用于指示误码率。

具体地，第一信息可以为指示信息。作为一个示例，指示信息为安全等级的索引，第一信息和安全等级之间具有对应关系，发送端发送第一信息后，通过第一信息，接收端可以获知安全等级，发送端可以是第一装置，也可以是第二装置。

10 可选地，在上述任一种实现方式中，该方法 200 还包括：第一装置确定误码率。

其中，第三装置的误码率和物理层安全传输技术相关，二者之间可以存在耦合的关系，并且都受到第三装置的接收机模型的影响。一种方法是给定物理层安全传输技术，假定第三装置的接收机模型，估算该物理层安全传输技术能够在第三装置端引入的误码率。另一种方法是给定希望达到的第三装置的误码率，假定第三装置的接收机模型，确定物理层安全传输技术。

15 作为示例，第一装置确定误码率，包括：第一装置确定受控区域，第二装置位于受控区域，第三装置位于受控区域之外，第一装置确定受控区域之外的最佳通信位置，第三装置在最佳通信位置具有最好的接收性能，第一装置根据最佳通信位置确定误码率。

具体地，第一装置为网络设备，第二装置为终端设备，第三装置为假设的侦听者为例，受控区域（confined region）是指对于特定合法终端没有侦听者的区域。例如，图 9 示出了受控区域的一种示意图，如图 9 所示，合法终端#1 在某个房间内，一般房间内没有侦听者，因此，这个房间可认定为受控区域。又如，受控区域也可以是汽车、工厂等，这些区域封闭管控，因此可以认为没有侦听者。又如，终端携带在用户身上，可以认为在某些范围内没有侦听者，比如 1m 以内，受控区域可以是指以终端为中心的范围。受控区域确定之后，需要确定侦听者的最优点，在这个点侦听者的性能就会是最好的。确定方法可以根据物理层安全传输技术、网络拓扑和网络设备的参数等确定。比如，物理层安全传输技术采用的是人工噪声方案，在网规阶段，可以粗略的估计采用人工噪声方案之后，在受控区域之外噪声能量最低的点，也就是接收信干噪比最高的点，这个点就是侦听者的最佳侦听点。最佳侦听点确定后，就可以估计侦听者的误码率。误码率的估计需要结合侦听者的接收机模型。在安全领域，往往假定侦听者的接收能力超过合法终端，因此在估算过程中一般假定侦听者采用最优的接收机算法并具有足够的计算能力。

应理解，上文以第一装置确定第三装置的误码率为例，本申请并不限于此，第三装置的误码率也可以由接收端设备（即第二装置）确定，并发送给发送端设备（即第一装置），第二装置的确定方式可以参考第一装置的确定方式，在此不赘述。

35 还应理解，在实际应用中，获得第三装置的真实误码率难度极大，因此，确定第三装置的误码率，也可以理解为第一装置或第二装置对第三装置的误码率进行估计。

下面结合图 10 和图 11 对本申请提供的无线物理层安全通信的方法 200 进行具体说明。

图 10 示出了本申请提供的一种无线物理层安全通信的方法 300，该方法 300 为方法 200 的一种具体实现。在方法 300 中，以第一装置为网络设备#A，第二装置为终端设备#A

为例。如图 10 所示，该方法 300 包括以下步骤。

S301，终端设备#A 向网络设备#A 发送无线帧#1。

其中，无线帧#1 携带第一参数，第一参数可以理解为预处理和后处理模块的参数，第一参数可包括安全等级要求、第三装置的误码率。根据第一参数，网络设备#A 可以对待发送的、具有安全要求的数据#1（第一数据的一例）进行预处理。可选地，数据#1 也是物理层数据。

可选地，若网络设备#A 不能满足终端设备#A 的安全等级要求，网络设备#A 可以向终端设备#A 发送安全等级，该安全等级可以低于终端设备#A 的安全等级要求。网络设备#A 可以根据发送的安全等级进行预处理，终端设备#A 可以根据接收的安全等级进行后处理。

终端设备#A 接收并解调无线帧#1，可以获得第一参数。

S302，网络设备#A 发送无线帧#2，无线帧#2 携带随机向量（第二随机串的一例）。

S302 和 S301 可以同时执行，即随机向量和第一参数可以携带于同一无线帧。

可选地，S302 不执行，随机向量在协议中定义，收发双端无需通过信令交互同步。

S303，网络设备#A 根据第一参数预处理数据#1，得到数据#2（第二数据的一例）。

S304，网络设备#A 向终端设备#A 发送无线帧#3。

无线帧#3 是对预处理过的数据#1 进行调制的信号，即无线帧#3 包括数据#2。

S305，终端设备#A 解调无线帧#3，可以获得数据#2。终端设备#A 对数据#2 进行后处理，得到数据#1，后处理根据第一参数执行。

图 11 示出了本申请提供的一种无线物理层安全通信的方法 400，该方法 400 为方法 200 的一种具体实现，在方法 400 中，以第一装置为网络设备#B，第二装置为终端设备#B 为例。如图 11 所示，该方法 400 包括以下步骤。

S401，网络设备#B 向终端设备#B 发送无线帧#1。

其中，无线帧#1 携带第一参数，第一参数可以理解为预处理和后处理模块的参数，第一参数可包括安全等级、第三装置的误码率。应理解，与方法 300 不同的是，网络设备#B 可以对待发送的、具有安全要求的数据进行统一配置，从而网络设备#B 可以向终端设备#B 指示预处理的安全等级。

终端设备#B 接收并解调无线帧#1，可以获得第一参数。

S402，网络设备#B 发送无线帧#2，无线帧#2 携带随机向量（第二随机串的一例）。

S402 和 S401 可以同时执行，即随机向量和第一参数可以携带于同一无线帧。

可选地，S402 不执行，随机向量在协议中定义，收发双端无需通过信令交互同步。

S403，网络设备#B 根据第一参数预处理数据#3（第一数据的一例），得到数据#4（第二数据的一例）。

S404，网络设备#B 向终端设备#B 发送无线帧#3。

无线帧#3 是对预处理过的数据#3 进行调制的信号，即无线帧#2 包括数据#4。

S405，终端设备#B 解调无线帧#3，可以获得数据#4。终端设备#B 对数据#4 进行后处理，得到数据#3，后处理根据第一参数执行。

上述流程图中虚线步骤为可选地步骤，且各步骤的先后顺序依照方法的内在逻辑确定，上述流程图所示的序号仅为示例，不对本申请步骤的先后顺序造成限制。

应理解，本申请实施例提供的方法可以单独使用，也可以结合使用，本申请对此不做限制。本申请实施例提供的各种实施方式可以单独使用，也可以结合使用，本申请对此不做限制。本申请实施例提供的各种示例可以单独使用，也可以结合使用，本申请对此不做限制。

5 还应理解，本申请中术语“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，其中 A，B 可以是单数或者复数。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系，但也可能表示的是一种“和/或”的关系，具体可参考前后文进行理解。

10 本申请实施例中，若无特殊说明，多个指两个或两个以上。

本申请实施例中，“至少一项（个）”是指一项（个）或者多项（个），“至少两项（个）”以及“多项（个）”是指两项（个）或两项（个）以上。“以下至少一项（个）”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a,b,或 c 中的至少一项（个），可以表示：a, b, c, a-b, a-c, b-c,或 a-b-c，其中 a,b,c 可以

15 是单个，也可以是多个。
需注意的是，图 5、图 10、图 11 中示意的执行主体仅为示例，该执行主体也可以是支持该执行主体实现图 5、图 10、图 11 所示方法的芯片、芯片系统、或处理器，本申请对此不作限制。

上文结合附图描述了本申请实施例的方法实施例，下面描述本申请实施例的装置实施例。可以理解，方法实施例的描述与装置实施例的描述可以相互对应，因此，未描述的部分可以参见前面方法实施例。

可以理解的是，上述各个方法实施例中，由第一装置实现的方法和操作，也可以由第一装置中的部件（例如芯片或者电路）实现，由第二装置实现的方法和操作，也可以由第二装置中的部件（例如芯片或者电路）实现。

25 上述主要从各个装置之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是，各个装置，例如发射端设备或者接收端设备，为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

30 本申请实施例可以根据上述方法示例对发射端设备或者接收端设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。下面以采用对应各个功能划分各个功能模块为例进行说明。

图 12 是本申请实施例提供的通信装置的示意性框图。图 12 所示的通信装置 500 包括收发单元 510 和处理单元 520。收发单元 510 可以与外部进行通信，处理单元 520 用于进

行数据处理。收发单元 510 还可以称为通信接口或通信单元。

可选的，收发单元 510 可以包括发送单元和接收单元。发送单元用于执行上述方法实施例中的发送操作。接收单元用于执行上述方法实施例中的接收操作。

- 5 需要说明的是，通信装置 500 可以包括发送单元，而不包括接收单元。或者，通信装置 500 可以包括接收单元，而不包括发送单元。具体可以视通信装置 500 执行的上述方案中是否包括发送动作和接收动作。

可选地，该通信装置 500 还可以包括存储单元，该存储单元可以用于存储指令或者和/或数据，处理单元 520 可以读取存储单元中的指令或者和/或数据。

- 10 在一种设计中，通信装置 500 可以用于执行上文方法实施例中第一装置所执行的动作。可选地，该通信装置 500 可以执行上文方法实施例中第一装置所执行的动作。第一装置可以是终端设备或网络设备，也可以是终端设备或网络设备中的芯片或电路，也可以是能实现全部或部分终端设备或网络设备功能的逻辑模块或软件，本申请对此不作限定。

- 15 可选地，该通信装置 500 可以为第一装置，收发单元 510 用于执行上文方法实施例中第一装置的接收或发送的操作，处理单元 520 用于执行上文方法实施例中第一装置内部处理的操作。

可选地，该通信装置 500 可以为包括第一装置的设备。或者，该通信装置 500 可以为配置在第一装置中的部件，例如，第一装置中的芯片。这种情况下，收发单元 510 可以为接口电路、管脚等。具体地，接口电路可以包括输入电路和输出电路，处理单元 520 可以包括处理电路。

- 20 一种可能的实现方式中，该处理单元 520 用于：基于第三装置的误码率对第一数据进行预处理，预处理用于使得第一装置和第二装置之间的通信达到安全等级；该收发单元 510 用于向第二装置发送第二数据，第二数据为对第一数据进行预处理之后得到的数据。

一种可能的实现方式中，处理单元 520 具体用于：基于第三装置的误码率对第一数据进行分组；或，基于第三装置的误码率对第一数据进行分组并生成第一随机串。

- 25 一种可能的实现方式中，处理单元 520 具体用于：根据误码率和安全等级确定第一数据的分组长度；以分组长度为单位对第一数据进行划分。

一种可能的实现方式中，处理单元 520 还用于：基于第一随机串对分组后的第一数据进行运算。

- 30 一种可能的实现方式中，处理单元 520 具体用于：根据第一随机串和第二随机串获得第一比特串；基于第一比特串对分组后的第一数据进行运算。

一种可能的实现方式中，第一随机串的长度大于或等于分组长度，第二随机向量的长度等于第一随机串的长度。

一种可能的实现方式中，第一随机串的长度小于分组长度，第二随机向量的长度等于分组长度。

- 35 一种可能的实现方式中，收发单元 510 还用于：向第二装置发送第二随机串。

一种可能的实现方式中，分组长度为信道编码的分组大小。

一种可能的实现方式中，收发单元 510 还用于：向第二装置发送第一信息；或，接收来自第二装置的第一信息；其中，第一信息用于指示安全等级。

一种可能的实现方式中，第一信息为指示信息。

一种可能的实现方式中，该指示信息用于指示终端设备的类型，终端设备的类型和通信安全等级之间具有对应关系。

一种可能的实现方式中，收发单元 510 还用于：接收来自第二装置的第二信息；或，向第二装置发送第二信息；其中，第二信息用于指示误码率。

5 一种可能的实现方式中，该第二信息为指示信息。

一种可能的实现方式中，处理单元 520 还用于：确定误码率。

一种可能的实现方式中，处理单元 520 具体用于：确定受控区域，第二装置位于受控区域，第三装置位于受控区域之外；确定受控区域之外的最佳通信位置，第三装置在最佳通信位置具有最好的接收性能；根据最佳通信位置确定误码率。

10 在一种设计中，通信装置 500 可以用于执行上文方法实施例第二装置所执行的动作。

可选地，该通信装置 500 可以执行上文方法实施例第二装置所执行的动作。第二装置可以是终端设备或网络设备，也可以是终端设备或网络设备中的芯片或电路，也可以是能实现全部或部分终端设备或网络设备功能的逻辑模块或软件，本申请对此不作限定。

15 可选地，该通信装置 500 可以为第二装置，收发单元 510 用于执行上文方法实施例第二装置的接收或发送的操作，处理单元 520 用于执行上文方法实施例第二装置内部处理的操作。

20 可选地，该通信装置 500 可以为包括第二装置的设备。或者，该通信装置 500 可以为配置在第二装置中的部件，例如，第二装置中的芯片。这种情况下，收发单元 510 可以为接口电路、管脚等。具体地，接口电路可以包括输入电路和输出电路，处理单元 520 可以包括处理电路。

一种可能的实现方式中，该收发单元 510 用于：接收来自第一装置的第二数据；该处理单元 520 用于：对第二数据进行后处理，得到第一数据，第二数据为基于第三装置的误码率对第一数据进行预处理之后得到的数据，预处理用于使得第一装置和第二装置之间的通信达到安全等级。

25 一种可能的实现方式中，处理单元 520 具体用于：对第二数据进行分组划分；根据第二随机串对分组划分后的第二数据进行处理。

一种可能的实现方式中，第二数据包括第一随机串，处理单元 520 还用于：根据第一随机串和第二随机串获得第一比特串；基于第一比特串对分组划分后的第二数据进行运算。

一种可能的实现方式中，收发单元 510 还用于：接收来自第一装置的第二随机串。

30 一种可能的实现方式中，收发单元 510 还用于：接收来自第一装置的第一信息；或，向第一装置发送第一信息；其中，第一信息用于指示安全等级。

一种可能的实现方式中，该第一信息为指示信息。

一种可能的实现方式中，该指示信息用于指示终端设备的类型，终端设备的类型和通信安全等级之间具有对应关系。

35 一种可能的实现方式中，收发单元 510 还用于：接收来自第一装置的第二信息；或，向第一装置发送第二信息，其中，第二信息用于指示误码率。

一种可能的实现方式中，第二信息为指示信息。

一种可能的实现方式中，处理单元 520 还用于：确定误码率。

一种可能的实现方式中，处理单元 520 具体用于：确定受控区域，第二装置位于受控

区域,第三装置位于受控区域之外;确定受控区域之外的最佳通信位置,第三装置在最佳通信位置具有最好的接收性能;根据最佳通信位置确定误码率。

如图 13 所示,本申请实施例还提供一种通信装置 600。该通信装置 600 包括处理器 610,处理器 610 与存储器 620 耦合,存储器 620 用于存储计算机程序或指令或者和/或数据,处理器 610 用于执行存储器 620 存储的计算机程序或指令和/或者数据,使得上文方法实施例中的方法被执行。

可选地,该通信装置 600 包括的处理器 610 为一个或多个。

可选地,如图 13 所示,该通信装置 600 还可以包括存储器 620。

可选地,该通信装置 600 包括的存储器 620 可以为一个或多个。

10 可选地,该存储器 620 可以与该处理器 610 集成在一起,或者分离设置。

可选地,如图 13 所示,该通信装置 600 还可以包括收发器 630 和/或通信接口,收发器 630 和/或通信接口用于信号的接收和/或发送。例如,处理器 610 用于控制收发器 630 和/或通信接口进行信号的接收和/或发送。

15 可选地,可以将收发器 630 中用于实现接收功能的器件视为接收模块,将收发器 630 中用于实现发送功能的器件视为发送模块,即收发器 630 包括接收器和发送器。收发器有时也可以称为收发机、收发模块、或收发电路等。接收器有时也可以称为接收机、接收模块、或接收电路等。发送器有时也可以称为发射机、发射器、发射模块或者发射电路等。

20 作为一种方案,该通信装置 600 用于实现上文方法实施例中由第一装置执行的操作。例如,处理器 610 用于实现上文方法实施例中由第一装置内部执行的操作(例如 S210 的操作),收发器 630 用于实现上文方法实施例中由第一装置执行的接收或发送的操作(例如 S220 的操作)。

25 作为另一种方案,该通信装置 600 用于实现上文方法实施例中由第二装置执行的操作。例如,处理器 610 用于实现上文方法实施例中由第二装置内部执行的操作(例如 S230 的操作),收发器 630 用于实现上文方法实施例中由第二装置执行的接收或发送的操作(例如 S220 的操作)。

如图 14,本申请实施例还提供了一种通信装置 700。该通信装置 700 包括逻辑电路 710 以及输入/输出接口(input/output interface)720。

30 其中,逻辑电路 710 可以为通信装置 700 中的处理电路。逻辑电路 710 可以耦合连接存储单元,调用存储单元中的指令,使得通信装置 700 可以实现本申请各实施例的方法和功能。输入/输出接口 720,可以为通信装置 700 中的输入输出电路,将通信装置 700 处理好的信息输出,或将待处理的数据或信令信息输入通信装置 700 进行处理。

作为一种方案,该通信装置 700 用于实现上文各个方法实施例中由数据处理装置执行的操作。

35 例如,逻辑电路 710 用于实现上文方法实施例中由第一装置执行的处理相关的操作,如, S210。输入/输出接口 720 用于实现上文方法实施例中由第一装置执行的发送和/或接收相关的操作,如 S220。逻辑电路 710 执行的操作具体可以参见上文对处理单元 520 的说明,输入/输出接口 720 执行的操作可以参见上文对收发单元 510 的说明,这里不再赘述。

作为另一种方案，该通信装置 700 用于实现上文各个方法实施例中由数据编排装置执行的操作。

例如，逻辑电路 710 用于实现上文方法实施例中由第二装置执行的处理相关的操作，如，方法实施例中的第二装置执行的处理相关的操作，如 S230，输入/输出接口 720 用于实现上文方法实施例中由第二装置执行的发送和/或接收相关的操作，如 S220。逻辑电路 710 执行的操作具体可以参见上文对处理单元 720 的说明。逻辑电路 710 执行的操作具体可以参见上文对处理单元 520 的说明，输入/输出接口 720 执行的操作可以参见上文对收发单元 510 的说明，这里不再赘述。

应理解，上述通信装置可以是一个或多个芯片。例如，该通信装置可以是现场可编程门阵列（field programmable gate array, FPGA），可以是专用集成芯片（application specific integrated circuit, ASIC），还可以是系统芯片（system on chip, SoC），还可以是中央处理器（central processor unit, CPU），还可以是网络处理器（network processor, NP），还可以是数字信号处理电路（digital signal processor, DSP），还可以是微控制器（micro controller unit, MCU），还可以是可编程控制器（programmable logic device, PLD）或其他集成芯片。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中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），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如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 (synchlink DRAM, SLD RAM) 和直接内存总线随机存取存储器 (direct rambus RAM, DR RAM)。应注意, 5 本文描述的系统和方法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。

根据本申请实施例提供的方法, 本申请还提供一种计算机可读介质, 该计算机可读介质存储有程序代码, 当该程序代码在计算机上运行时, 使得该计算机执行方法实施例所示的方法。例如, 该计算机程序被计算机执行时, 使得该计算机可以实现上述方法实施例中由第一装置执行的方法, 或由第二装置执行的方法。

10 本申请实施例还提供一种包含指令的计算机程序产品, 该指令被计算机执行时使得该计算机实现上述方法实施例中由第一装置执行的方法, 或由第二装置执行的方法。

本申请实施例还提供一种通信系统, 包括第一装置和第二装置。

上述提供的任一种通信装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例, 此处不再赘述。

15 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。所述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所述计算机指令时, 全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中, 20 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线 (例如同轴电缆、光纤、数字用户线 (digital subscriber line, DSL)) 或无线 (例如红外、无线、微波等) 方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数 25 据存储设备。所述可用介质可以是磁性介质 (例如, 软盘、硬盘、磁带)、光介质 (例如, 高密度数字视频光盘 (digital video disc, DVD))、或者半导体介质 (例如, 固态硬盘 (solid state drive, SSD)) 等。

上述各个装置实施例中的数据编排装置, 数据处理装置与方法实施例中的数据编排装置, 数据处理装置对应, 由相应的模块或单元执行相应的步骤, 例如通信单元 (收发器) 30 执行方法实施例中接收或发送的步骤, 除发送、接收外的其它步骤可以由处理单元 (处理器) 执行。具体单元的功能可以参考相应的方法实施例。其中, 处理器可以为一个或多个。

在本说明书中使用的术语“部件”、“模块”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如, 部件可以是但不限于, 在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。 35 通过图示, 在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中, 部件可位于一个计算机上和/或分布在两个或更多个计算机之间。此外, 这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组 (例如来自与本地系统、分布式系统和/或网络间的另一部件交互的二个部件的数据, 例如通过信号与其它系统交互的互联网) 的信号通过本地和/或远

程进程来通信。

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

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

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

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

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

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

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所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种无线物理层安全通信的方法，其特征在于，包括：
- 5 第一装置基于第三装置的误码率对第一数据进行预处理，所述预处理用于使得所述第一装置和第二装置之间的通信达到安全等级；
- 所述第一装置向第二装置发送第二数据，所述第二数据为对所述第一数据进行所述预处理之后得到的数据。
2. 根据权利要求 1 所述的方法，其特征在于，所述第一装置基于第三装置的误码率对第一数据进行预处理，包括：
- 10 所述第一装置基于第三装置的误码率对所述第一数据进行分组；或，
- 所述第一装置基于第三装置的误码率对所述第一数据进行分组并生成第一随机串。
3. 根据权利要求 2 所述的方法，其特征在于，所述第一装置基于第三装置的误码率对所述第一数据进行分组，包括：
- 所述第一装置根据所述误码率和所述安全等级确定所述第一数据的分组长度；
- 15 所述第一装置以所述分组长度为单位对所述第一数据进行划分。
4. 根据权利要求 3 所述的方法，其特征在于，所述方法还包括：
- 所述第一装置基于所述第一随机串对分组后的所述第一数据进行运算。
5. 根据权利要求 4 所述的方法，其特征在于，所述第一装置基于所述第一随机串对分组后的所述第一数据进行运算，包括：
- 20 所述第一装置根据所述第一随机串和第二随机串获得第一比特串；
- 所述第一装置基于第一比特串对分组后的所述第一数据进行运算。
6. 根据权利要求 5 所述的方法，其特征在于，所述第一随机串的长度大于或等于所述分组长度，所述第二随机向量的长度等于所述第一随机串的长度。
7. 根据权利要求 5 所述的方法，其特征在于，所述第一随机串的长度小于所述分组长度，所述第二随机向量的长度等于所述分组长度。
- 25 8. 根据权利要求 5 至 7 中任一项所述的方法，其特征在于，所述方法还包括：
- 所述第一装置向所述第二装置发送所述第二随机串。
9. 根据权利要求 3 至 8 中任一项所述的方法，其特征在于，所述分组长度为信道编码的分组大小。
- 30 10. 根据权利要求 1 至 9 中任一项所述的方法，其特征在于，所述方法还包括：
- 所述第一装置向所述第二装置发送第一信息；或，
- 所述第一装置接收来自所述第二装置的第一信息；
- 其中，所述第一信息用于指示所述安全等级。
11. 根据权利要求 10 所述的方法，其特征在于，所述第一信息为指示信息，所述指示信息用于指示终端设备的类型，所述终端设备的类型和所述通信安全等级之间具有对应关系。
- 35 12. 根据权利要求 1 至 11 中任一项所述的方法，其特征在于，所述方法还包括：
- 所述第一装置接收来自所述第二装置的第二信息；或，

所述第一装置向所述第二装置发送第二信息；

其中，所述第二信息用于指示所述误码率。

13. 根据权利要求 1 至 12 中任一项所述的方法，其特征在于，所述方法还包括：
所述第一装置确定所述误码率。

5 14. 根据权利要求 13 所述的方法，其特征在于，所述第一装置确定所述误码率，包括：

所述第一装置确定受控区域，所述第二装置位于所述受控区域，所述第三装置位于所述受控区域之外；

10 所述第一装置确定所述受控区域之外的最佳通信位置，所述第三装置在所述最佳通信位置具有最好的接收性能；

所述第一装置根据所述最佳通信位置确定所述误码率。

15. 一种无线物理层安全通信的方法，其特征在于，包括：

第二装置接收来自第一装置的第二数据；

15 所述第二装置对所述第二数据进行后处理，得到第一数据，所述第二数据为基于第三装置的误码率对所述第一数据进行预处理之后得到的数据，所述预处理用于使得所述第一装置和第二装置之间的通信达到安全等级。

16. 根据权利要求 15 所述的方法，其特征在于，所述第二装置对所述第二数据进行后处理，包括：

所述第二装置对所述第二数据进行分组划分；

20 所述第二装置根据第二随机串对分组划分后的所述第二数据进行处理。

17. 根据权利要求 16 所述的方法，其特征在于，所述第二数据包括第一随机串，所述第一随机串根据第二随机串对分组划分后的所述第二数据进行处理，包括：

所述第二装置根据所述第一随机串和所述第二随机串获得第一比特串；

所述第二装置基于第一比特串对分组划分后的所述第二数据进行运算。

25 18. 根据权利要求 16 或 17 所述的方法，其特征在于，所述方法还包括：

所述第二装置接收来自所述第一装置的所述第二随机串。

19. 根据权利要求 15 至 18 中任一项所述的方法，其特征在于，所述方法还包括：

所述第二装置接收来自所述第一装置的第一信息；或，

所述第二装置向所述第一装置发送第一信息；

30 其中，所述第一信息用于指示所述安全等级。

20. 根据权利要求 19 所述的方法，其特征在于，所述第一信息为指示信息，所述指示信息用于指示终端设备的类型，所述终端设备的类型和所述通信安全等级之间具有对应关系。

21. 根据权利要求 15 至 20 中任一项所述的方法，其特征在于，所述方法还包括：

35 所述第二装置接收来自所述第一装置的第二信息；或，

所述第二装置向所述第一装置发送第二信息；

其中，所述第二信息用于指示所述误码率。

22. 根据权利要求 15 至 21 中任一项所述的方法，其特征在于，所述方法还包括：
所述第二装置确定所述误码率。

23. 根据权利要求 22 所述的方法, 其特征在于, 所述第二装置确定所述误码率, 包括:

所述第二装置确定受控区域, 所述第二装置位于所述受控区域, 所述第三装置位于所述受控区域之外;

5 所述第二装置确定所述受控区域之外的最佳通信位置, 所述第三装置在所述最佳通信位置具有最好的接收性能;

所述第二装置根据所述最佳通信位置确定所述误码率。

24. 一种通信装置, 其特征在于, 所述装置包括用于执行如权利要求 1 至 14 中任一项所述方法的步骤的单元, 或所述装置包括用于执行如权利要求 15 至 23 中任一项所述方法的步骤的单元。
10

25. 一种通信装置, 其特征在于, 所述装置包括处理器, 所述处理器与存储器耦合, 所述存储器存储有指令, 所述指令被所述处理器运行时, 使得所述处理器执行如权利要求 1 至 14 中任一项所述的方法, 或执行如权利要求 15 至 23 中任一项所述的方法。

26. 一种通信装置, 其特征在于, 所述装置包括逻辑电路, 所述逻辑电路用于与输入/输出接口耦合, 通过所述输入/输出接口传输数据, 以执行如权利要求 1 至 14 中任一项所述的方法, 或执行如权利要求 15 至 23 中任一项所述的方法。
15

27. 一种通信系统, 其特征在于, 所述系统包括第一装置和第三装置, 所述第一装置用于执行如权利要求 1 至 14 中任一项所述的方法, 所述第三装置用于执行如权利要求 15 至 23 中任一项所述的方法。

28. 一种计算机可读存储介质, 其特征在于, 所述计算机可读存储介质用于存储计算机程序, 当所述计算机程序在计算机上运行时, 使得所述计算机执行如权利要求 1 至 14 中任一项所述的方法, 或执行如权利要求 15 至 23 中任一项所述的方法。
20

29. 一种计算机程序产品, 其特征在于, 所述计算机程序产品包括: 计算机程序代码, 当所述计算机程序代码被运行时, 实现如权利要求 1 至 14 中任一项所述的方法, 或执行如权利要求 15 至 23 中任一项所述的方法。
25