

数据传输方法、装置、系统、计算机设备和存储介质

本申请要求于 2020 年 11 月 20 日提交中国专利局，申请号为 202011308606.3，申请名称为“数据传输方法、装置、系统、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及无线通信技术领域，特别是涉及一种数据传输方法、装置、计算机设备和存储介质。

背景技术

在一些特定的应用场景中，存在两种不同的设备进行数据传输，这两种不同的设备可以通过无线方式进行数据传输，在采用无线方式传输数据的过程中，为了确保数据安全传输通常会对通信链路进行加密。然而，在数据传输过程中，采用通信链接加密的方式可能无法有效地保证数据安全，而若在两种不同设备上分别进行数据加密和解密的过程，则需要对两种不同设备上的进行软件适配，如采用蓝牙方式传输数据时需要进行蓝牙软件适配，导致软件的通用性差，从而无法在确保数据安全传输的同时也保证设备之间的交互效果。

发明内容

根据本申请的各种实施例，提供了一种数据传输方法、装置、系统、计算机设备和存储介质。

一种数据传输方法，执行于通信适配器，所述方法包括：

与第一交互设备进行双向认证；

当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；以及

通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

一种数据传输装置，所述装置包括：

认证模块，用于与第一交互设备进行双向认证；

接收模块，用于当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的

认证密钥进行映射得到的；

解密模块，用于根据在通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；以及

发送模块，用于通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

一种数据传输系统，所述系统包括：第一交互设备、第二交互设备以及与所述第一交互设备无线连接、且与所述第二交互设备电连接的通信适配器；

所述通信适配器，用于对所述第一交互设备进行认证；

所述第一交互设备，用于当所述通信适配器完成认证时，对所述通信适配器进行认证，并在认证完成后，基于对双向认证时所采用的认证密钥进行映射得到的工作密钥加密交互数据，得到加密交互数据；

所述通信适配器，还用于接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；

所述通信适配器，还用于根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；

所述第二交互设备，用于识别所述通信适配器所模拟的设备节点；以及

所述通信适配器，还用于通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤：

与第一交互设备进行双向认证；

当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；以及

通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

一种计算机可读存储介质，其上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现以下步骤：

与第一交互设备进行双向认证；

当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数

据进行解密；以及

通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

一种计算机可读指令产品，该计算机可读指令产品包括计算机可读指令，该计算机可读指令存储在计算机可读存储介质中；计算机设备的处理器从计算机可读存储介质读取该计算机可读指令，处理器执行该计算机可读指令，使得该计算机设备执行上述数据传输方法的步骤。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征、目的和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为一个实施例中数据传输方法的应用环境图；

图 2 为一个实施例中数据传输方法的流程示意图；

图 3 为一个实施例中双向认证步骤的流程示意图；

图 4 为另一个实施例中数据传输方法的流程示意图；

图 5 为一个实施例中数据从第二交互设备向第一交互设备传输步骤的流程示意图；

图 6 为一个实施例中数据传输系统的结构框图；

图 7 为一个实施例中人脸支付场景下的数据传输系统的结构框图；

图 8a 为一个实施例中密钥生成步骤的流程示意图；

图 8b 为一个实施例中密钥生成和双向认证步骤的流程示意图；

图 9 为一个实施例中数据传输装置的结构框图；

图 10 为另一个实施例中数据传输装置的结构框图；

图 11 为一个实施例中计算机设备的内部结构图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本申请提供的数据传输方法，可以应用于如图 1 所示的应用环境中。在该应用环境中，包括通信适配器 102、第一交互设备 104 和第二交互设备 106。通信适配器 102 与第一交互设备 104 之间进行无线连接，通信适配器 102 与第二交互设备 106 之间进行电连接，如有线连接。通信适配器 102 与第一交互设备 104 进行双向认证；在完成双向认证之后，通信适配器

102 接收第一交互设备 104 所发送的基于工作密钥加密交互数据得到的加密交互数据；该工作密钥是由第一交互设备对认证密钥进行映射得到的；通信适配器 102 根据在自身上对认证密钥进行映射得到的工作密钥，对加密交互数据进行解密；通过所模拟的由第二交互设备 106 能够识别的设备节点，基于第二交互设备 106 的原生适配设备节点的通信协议，向第二交互设备 106 传输解密所得的交互数据。

其中，通信适配器 102 可以作为第一交互设备 104 与第二交互设备 106 之间的桥梁，作为中间桥梁实现第一交互设备 104 与第二交互设备 106 之间的数据交互。具体地，该通信适配器 102 可以是蓝牙适配器（Bluetooth dongle）、紫蜂（ZigBee）适配器、近场通信适配器以及其它无线适配器等。需要指出的是，该通信适配器 102 可以是独立的器件，也可以是集成于第二交互设备 106 中的器件。

第一交互设备 104 可以是扫描设备，如用于扫描人脸的设备，用于扫描图形码的设备等。其中，该图形码可以是条形码或二维码，也可以是携带信息的其它类型图形码。

第二交互设备 106 可以是资源转移设备，用于在与第一交互设备 102 进行交互过程中，根据交互数据进行交互操作，该交互操作包括资源转移操作。此外，也可以根据双方发送的控制数据执行控制操作。

在一个实施例中，如图 2 所示，提供了一种数据传输方法，以该方法应用于图 1 中的通信适配器 102 为例进行说明，该通信适配器 102 与第一交互设备 104 无线连接、且与第二交互设备 106 电连接，该方法包括以下步骤：

S202，与第一交互设备进行双向认证。

其中，双向认证可以是第一交互设备也会对通信适配器进行认证，然后通信适配器对第一交互设备进行认证，以确保通信适配器和第一交互设备均为可靠设备。

在一个实施例中，通信适配器可以采用认证密钥与第一交互设备进行双向认证，也可以结合认证密钥和随机数与第一交互设备进行双向认证。因此，对比 S202，可以分为以下两种认证方式进行阐述：

方式 1，结合认证密钥和随机数与第一交互设备进行双向认证。

在一个实施例中，通信适配器接收第一交互设备发送的第一挑战码；基于认证密钥对第一挑战码进行解密，得到第一随机数；第一随机数是由第一交互设备生成的随机数；对第一随机数进行哈希运算，得到第一哈希值；生成第二随机数，并基于认证密钥加密第一哈希值和第二随机数，得到第二挑战码；向第一交互设备发送第二挑战码，以使第一交互设备基于认证密钥解密第二挑战码得到第一哈希值，将第一哈希值与第一交互设备基于认证密钥对第一随机数加密所得的第二哈希值进行对比，若第一哈希值和第二哈希值相同，则对解密第二挑战码所得的第二随机数进行哈希运算，将哈希运算所得的第二哈希值进行返回；接收第一交互设备返回的第二哈希值，并将第二哈希值与在通信适配器本地基于认证密钥对第二随机数进行哈希运算所得的第三哈希值进行对比，若第二哈希值与第三哈希值相同，则完成通信适配器与第一交互设备间的双向认证。

其中，方式 1 中的认证密钥可以根据通信适配器的设备序列号生成的密钥，可结合随机数与第一交互设备进行双向认证。

第一挑战码可以是第一交互设备根据认证密钥对自身生成的第一随机数进行加密所得的挑战码。第一随机数可以由第一交互设备生成的真随机数或假随机数。

第二随机数可以由通信适配器生成的真随机数或假随机数。其中，第一随机数和第二随机数是不同的两个随机数。第二挑战码是通信适配器利用认证密钥对第一哈希值和第二随机数的组合进行加密所得的挑战码，或者是利用认证密钥分别对第一哈希值和第二随机数进行加密，然后将加密的结果进行组合得到的挑战码。

在本方法的方案中，第一交互设备不直接发送第一随机数，而是发送利用认证密钥加密第一随机数所得的第一挑战码；而且，通信适配器不直接发送第二随机数，而是发送利用认证密钥加密第一哈希值和第二随机数所得的第二挑战码，可以避免信息泄露的同时，还可以提高认证过程中的准确性。

需要指出的是，通信适配器在对第二随机数进行加密时，所采用的认证密钥是通信适配器根据自身的设备序列号生成的。而第一交互设备在对第一随机数进行加密时，所采用的认证密钥是第一交互设备根据通信适配器的设备序列号生成的。而第一交互设备生成的认证密钥和通信适配器生成的认证密钥相同。其中，该通信适配器和第一交互设备在生成认证密钥时，根据序号加密密钥对通信适配器的设备序列号进行加密，从而得到认证密钥。

对于认证密钥的获得方法，其步骤可以包括：通信适配器接收所述第一交互设备发送的序列号获取请求；获取所述序列号获取请求指定的设备序列号；向所述第一交互设备反馈获取的设备序列号，以使所述第一交互设备基于反馈的所述设备序列号生成所述第一交互设备上的认证密钥；依据获取的所述设备序列号生成所述通信适配器上的认证密钥；所述第一交互设备上的认证密钥与所述通信适配器上的认证密钥相同。

其中，上述第一交互设备上的认证密钥，是基于第一交互设备存储的序列号加密密钥对反馈的设备序列号进行加密所得的。

在一个实施例中，上述依据获取的设备序列号生成通信适配器上的认证密钥的步骤，具体可以包括：通信适配器获取在通信适配器存储的序列号加密密钥；基于序列号加密密钥对获取的设备序列号进行加密，得到通信适配器上的认证密钥。

为了更加清楚且直观的了解上述双向认证的过程，可以结合图 3 对双向认证的过程进行描述，如图 3 所示，该双向认证的步骤包括：

S302a，第一交互设备生成随机数 A；

S302b，第一交互设备利用认证密钥对随机数 A 进行加密，得到挑战码 A；

S304a，通信适配器生成随机数 B；

S304b，通信适配器对随机数 B 进行哈希运算，得到哈希值 B；

S306，第一交互设备发送挑战码 A；

S308，通信适配器在接收到挑战码 A 之后，利用认证密钥对挑战码 A 进行解密，得到随机数 A；

其中，S308 中所使用的认证密钥可以是通信适配器利用通信适配器自身的设备序号生成的。

S310，通信适配器对随机数 A 进行哈希运算，得到哈希值 A'；

S312，通信适配器利用认证密钥对哈希值 A' 和随机数 B 进行加密，得到挑战码 B；

S314，通信适配器发送挑战码 B；

S316，第一交互设备在接收到挑战码 B 之后，利用认证密钥解密挑战码 B，得到哈希值 A' 和随机数 B；

其中，S316 中所使用的认证密钥可以是第一交互设备利用通信适配器的设备序号生成的。

S318，第一交互设备对随机数 A 进行哈希运算，并将所得的哈希值 A 与哈希值 A' 对比；

S320，第一交互设备若哈希值 A 与哈希值 A' 相同，则完成对通信适配器的认证；

S322，第一交互设备对随机数 B 进行哈希运算，得到哈希值 B'；

S324，第一交互设备发送哈希值 B'；

S326，通信适配器将哈希值 B' 与哈希值 B 进行对比；

S328，若哈希值 B' 与哈希值 B 相同，则完成通信适配器与第一交互设备的双向认证。

方式 2，采用认证密钥与第一交互设备进行双向认证。

在一个实施例中，该认证密钥包括通信适配器根据其自身的设备序列号生成的第一认证密钥，以及第一交互设备根据其自身的设备序列号生成的第二认证密钥。通信适配器向第一交互设备发送第一认证密钥，以使该第一交互设备将接收的第一认证密钥与在第一交互设备中存储的认证密钥进行对比，或与认证服务器中存储的认证密钥进行对比，若存储的认证密钥中存在与第一认证密钥相同的认证密钥时，则通信适配器通过认证，从而第一交互设备完成对通信适配器的认证，此时第一交互设备会向通信适配器发送第二认证密钥。通信适配器接收第一交互设备发送的第二认证密钥，然后将该第二认证密钥与通信适配器存储的认证密钥进行对比，或与认证服务器中存储的认证密钥进行对比，若对比一致，则第一交互设备通过认证，从而通信适配器完成对第一交互设备的认证，此时完成双向认证。

S204，接收第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据。

其中，交互数据用于第一交互设备与第二交互设备之间进行交互，该交互数据可以是人脸图像数据、支付码数据或控制数据。例如，当交互数据为人脸图像数据时，第一交互设备向第二交互设备发送加密的人脸图像数据，从而第二交互设备对该人脸图像数据进行识别，然后将识别的结果与人脸特征库中的人脸特征进行对比，查找到匹配的人脸特征，然后将与该匹配的人脸特征关联的支付信息返回给第一交互设备进行显示，以使用户进行支付确认。

工作密钥是由第一交互设备对认证密钥进行映射得到的，用于对传输的数据进行加密和解密。例如第一交互设备对认证密钥进行加密得到工作密钥，或对认证密钥进行哈希运算得到工作密钥。需要指出的是，第一交互设备所使用的认证密钥可以是第一交互设备根据通信适配器的设备序列号生成的密钥，如通过序号加密密钥对通信适配器的设备序列号进行加密所得到的密钥。此外，第一交互设备所使用的认证密钥也可以是认证服务器根据通信适配器的设备序列号生成并下发的密钥。

在一个实施例中，通信适配器和第一交互设备均可以存储有认证密钥，该认证密钥是根据通信适配器的设备序列号生成的；S204 具体可以包括：当第一交互设备基于自身存储的认证密钥映射得到工作密钥、并通过所得的工作密钥对交互数据进行加密得到加密交互数据后，通信适配器接收第一交互设备发送的进行加密得到的加密交互数据。其中，第一交互设备中存储的认证密钥可以是第一交互设备根据通信适配器的设备序列号生成的，此外第一交互设备中存储的认证密钥可以是认证服务器根据通信适配器的设备序列号生成并下发的，生成认证密钥的方式可以是利用序号加密密钥对通信适配器的设备序列号进行加密得到的认证密钥。

具体地，第一交互设备基于自身存储的认证密钥映射得到工作密钥，通过所得的工作密钥对交互数据进行加密，得到加密交互数据，然后将该加密交互数据发送给通信适配器，从而通信适配器可以接收到第一交互设备发送的对交互数据进行加密得到的加密交互数据。

S206，根据在通信适配器上对认证密钥进行映射得到的工作密钥，对加密交互数据进行解密。

在一个实施例中，通信适配器和第一交互设备均可以存储有认证密钥；S206 具体可以包括：通信适配器根据在通信适配器存储的认证密钥映射得到工作密钥，基于所得的工作密钥对加密交互数据进行解密。其中，通信适配器中存储的认证密钥可以是根据自身的设备序列号生成的，此外通信适配器中存储的认证密钥可以是认证服务器根据通信适配器的设备序列号生成并下发的。

S208，通过所模拟的由第二交互设备能够识别的设备节点，基于第二交互设备的原生适配设备节点的通信协议，向第二交互设备传输解密所得的交互数据。

其中，该设备节点是用于通信适配器与第二交互设备进行通信的虚拟节点。该设备节点是通信适配器在插入第二交互设备的硬件接口之后所模拟出来的虚拟节点，可以包括人机交互键盘节点和人机交互控制器节点。该人机交互键盘节点可以是 USB-HID (Universal Serial Bus-Human Interface Device, 通用串行总线人机接口装置) 键盘节点。该人机交互控制器节点可以是 USB-HID 控制器节点。

该通信协议可以是 USB-HID 协议，是用于通信适配器与第二交互设备进行连接和通信的协议。由于该通信协议是第二交互设备的操作系统原生适配的，也即是该操作系统所默认支持的协议，因此用户将通信适配器插入第二交互设备时，可以无需安装驱动即可直接使用该通信适配器，实现通信适配器的即插即用。

原生适配设备节点的通信协议可以指：通信适配器在插入第二交互设备的相应硬件接口时，可以利用该通信协议产生该设备节点，从而该通信协议原生适配该设备节点。

在一个实施例中，该通信适配器包括 HID 接口芯片。在通信适配器插入第二交互设备的情况下，通信适配器可以通过该 HID 接口芯片模拟出设备节点。

在一个实施例中，S208 具体可以包括：通信适配器将解密所得的交互数据，转换为与原生适配设备节点的通信协议匹配的目标交互数据；通过所模拟的由第二交互设备能够识别的设备节点，将经过格式转换后的目标交互数据传输至第二交互设备。

该解密所得的交互数据可以是以数据包形式存在。具体地，通信适配器对解密所得的交

互数据进行解析，得到包头部分和正文部分，然后基于该通信协议对正文部分进行封装，从而得到与该通信协议匹配的目标格式的目标交互数据；或者，基于该通信协议对交互数据添加一个相应的包头，从而得到与该通信协议匹配的目标格式的目标交互数据。然后通过所模拟的由第二交互设备能够识别的设备节点将目标交互数据传输至第二交互设备。

在一个实施例中，目标交互数据可以属于控制类型数据或交易类型数据，对应地，交互数据也属于控制类型数据或交易类型数据。S208 具体可以包括：当目标交互数据属于控制类型数据时，通信适配器将目标交互数据上报至人机交互控制器节点，以使第二交互设备通过人机交互控制器节点获取目标交互数据；当目标交互数据属于交易类型数据时，通信适配器将目标交互数据上报至人机交互键盘节点，以使第二交互设备通过人机交互键盘节点获取目标交互数据。

具体地，通信适配器读取目标交互数据的包头，当根据该包头中的接口标识确定属于控制类型数据时，根据该控制类型数据选择数据上报的人机交互控制器节点，然后将该目标交互数据上报至人机交互控制器节点；或者，根据包头中的接口标识选择数据上报的人机交互控制器节点，然后将该目标交互数据上报至人机交互控制器节点。当根据该包头中的接口标识确定属于交易类型数据时，根据该交易类型数据选择数据上报的人机交互键盘节点，然后将该目标交互数据上报至人机交互键盘节点；或者，根据包头中的接口标识选择数据上报的人机交互键盘节点，然后将该目标交互数据上报至人机交互键盘节点。

在一个实施例中，当加密交互数据或从第二交互设备接收的控制数据属于恶意攻击包，或者接收到的来源于网络侧终端的网络数据包属于恶意攻击包时，则触发安全事件；安全事件用于禁用通信适配器。

其中，该安全事件可以指用于改变通信适配器工作状态的事件。

具体地，通信适配器中还包含防拆点，当通信适配器中的防拆点检测到来自于第一交互设备、或第二交互设备、或网络侧终端的攻击时，表示传输的数据存在被窃取的风险，此时该防拆点触发安全事件，通过该安全事件来触发对通信适配器的禁用。

为了更加清楚且直观的理解上述数据传输方法，将该数据传输方法应用于人脸支付场景进行描述，在人脸支付场景中，上述第一交互设备可以是用于扫描人脸的人脸扫描设备，第二交互设备可以是 POS（Point of Sales，销售点）机，通信适配器可以是蓝牙适配器，该蓝牙适配器插入于第二交互设备，或者集成于第二交互设备；如图 4 所示，该数据传输方法具体可以包括：

S402，人脸扫描设备扫描用户的人脸，得到人脸图像数据；

S404，人脸扫描设备利用工作密钥对人脸图像数据进行加密，得到加密后人脸图像数据；

其中，人脸扫描设备中包含 SE（Secure Element，安全元件）芯片，SE 芯片利用工作密钥对人脸图像数据进行加密。

S406，人脸扫描设备通过蓝牙透传方式向蓝牙适配器发送加密后人脸图像数据；

S408，蓝牙适配器利用工作密钥对接收的加密后人脸图像数据进行解密，得到人脸图像数据；

其中，该蓝牙适配器中包含蓝牙透传芯片、SE 芯片、HID 接口芯片、RTC（Real-Time Clock，实时时钟）电池和至少两个防拆点。

蓝牙适配器的 SE 芯片，利用工作密钥对接收的加密后人脸图像数据进行解密，得到人脸图像数据。

S410，蓝牙适配器将人脸图像数据转换为符合 USB-HID 协议的人脸图像数据。

S412，蓝牙适配器将符合 USB-HID 协议的人脸图像数据通过 HID 键盘节点传输给 POS 机。

S414，POS 机对该人脸图像数据进行识别，得到与识别的结果匹配的支付信息，以使用户进行支付确认。

其中，该支付信息可以包括与用户关联的支付账号。该支付信息可以由 POS 机通过蓝牙适配器传输给人脸扫描设备，以使人脸扫描设备的显示器显示该支付信息，以使用户进行支付确认。

上述实施例中，在进行数据传输之前，先完成通信适配器与第一交互设备间的双向认证，从而可以确保数据传输的双方设备是可靠的，避免了数据传输至未认证的设备而出现信息安全的问题。在完成双向认证之后，通信适配器开始接收第一交互设备发送的经过加密的加密交互数据，且该加密交互数据是依据基于双向认证时所采用的认证密钥映射所得的工作密钥对交互数据进行加密所得，从而可以有效地确保交互数据在传输过程中的安全性。此外，通信适配器通过基于自身存储的认证密钥映射得到的工作密钥对加密交互数据进行解密，通过所模拟的由第二交互设备能够识别的设备节点，基于第二交互设备的原生适配设备节点的通信协议，向第二交互设备传输解密所得的交互数据，避免了在第一交互设备和第二交互设备双方上进行数据加密和解密的过程，从而无需对两种不同设备上的软件进行适配，有利于提高软件的通用性，有利于提高第一交互设备和第二交互设备之间的交互效果。而且，由于通信适配器模拟的设备节点能够被第二交互设备识别，而且所采用的通信协议是第二交互设备原生适配的，从而通信适配器在与第二交互设备电连接时，无需安装驱动即可实现通信适配器与第二交互设备之间兼容，实现了通信适配器即插即用的效果，避免了数据传输之前的准备工作，有利于提高数据传输的整体工作效率。

在一个实施例中，如图 5 所示，该方法还可以包括：

S502，通过人机交互控制器节点接收第二交互设备发送的控制数据。

其中，人机交互控制器节点是通信适配器插入第二交互设备之后模拟出来的设备节点，该人机交互控制器节点能够被第二交互设备识别，控制数据可以传输到该节点上，从而第二交互设备和通信适配器从该节点获得传输的控制数据。

S504，将控制数据转换为串口控制数据。

S506，根据在通信适配器上对认证密钥进行映射得到的工作密钥，对串口控制数据进行加密，得到加密控制数据。

其中，通信适配器上的 SE 芯片可以对认证密钥进行映射得到工作密钥，然后通过工作密钥对串口控制数据进行加密，然后将所得的加密控制数据传递给通信适配器上的无线单元。

该无线单元可以包括蓝牙透传芯片或其它无线芯片。

S508, 将加密控制数据传输给第一交互设备; 加密控制数据, 用于指示第一交互设备通过映射认证密钥得到的工作密钥, 对加密控制数据解密, 以根据解密所得的控制数据执行控制操作。

通信适配器可以通过无线单元将加密控制数据传输给第一交互设备, 例如通信适配器通过蓝牙透传芯片将加密控制数据以蓝牙透传方式传输给第一交互设备。

上述实施例中, 利用工作密钥对来自于第二交互设备的控制数据进行加密, 然后将加密所得的加密控制数据传输给第一交互设备, 而且第一交互设备利用映射认证密钥得到的工作密钥对加密控制数据解密, 而该工作密钥是对认证密钥映射所得的工作密钥, 从而可以有效地确保交互数据在传输过程中的安全性。

在一个实施例中, 如图 6 所示, 提供了一种数据传输系统, 该系统包括: 第一交互设备 602、第二交互设备 604 以及与第一交互设备无线连接、且与第二交互设备电连接的通信适配器 606;

通信适配器 606, 用于对第一交互设备 602 进行认证;

第一交互设备 602, 用于当通信适配器 606 完成认证时, 对通信适配器 606 进行认证, 并在认证完成后, 基于对双向认证时所采用的认证密钥进行映射得到的工作密钥加密交互数据, 得到加密交互数据;

通信适配器 606, 还用于接收第一交互设备 602 所发送的基于工作密钥加密交互数据得到的加密交互数据;

其中, 通信适配器 606 可以通过无线单元接收第一交互设备 602 发送的加密交互数据。

通信适配器 606, 还用于根据在通信适配器 606 上对认证密钥进行映射得到的工作密钥, 对加密交互数据进行解密;

其中, 通信适配器 606 可以通过 SE 芯片对加密交互数据进行解密, 具体地, 通信适配器 606 中的 SE 芯片对认证密钥进行映射得到的工作密钥之后, 利用工作密钥对加密交互数据进行解密。

第二交互设备 604, 用于识别通信适配器 606 所模拟的设备节点;

通信适配器 606, 还用于通过所模拟的由第二交互设备 604 能够识别的设备节点, 基于第二交互设备 604 的原生适配设备节点的通信协议, 向第二交互设备 604 传输解密所得的交互数据。

其中, 通信适配器 606 通过 HID 接口芯片模拟虚拟的设备节点。SE 芯片将解密所得的交互数据通过串口传输给 HID 接口芯片, 然后 HID 接口芯片将该交互数据转换为符合该通信协议的目标交互数据, 然后将该目标交互数据通过设备节点传输给第二交互设备 604。

在其中的一个实施例中, 通信适配器 606, 还用于接收第一交互设备 602 发送的第一挑战码; 基于认证密钥对第一挑战码进行解密, 得到第一随机数; 第一随机数是由第一交互设备 602 生成的随机数; 生成第二随机数, 并对第一随机数进行哈希运算, 得到第一哈希值;

基于认证密钥加密第一哈希值和第二随机数，得到第二挑战码；向第一交互设备 602 发送第二挑战码；

第一交互设备 602，还用于基于认证密钥解密接收的第二挑战码得到第一哈希值，将第一哈希值与第一交互设备 602 基于认证密钥对第一随机数加密所得的第二哈希值进行对比，若第一哈希值和第二哈希值相同，则对解密第二挑战码所得的第二随机数进行哈希运算，将哈希运算所得的第二哈希值进行返回；

通信适配器 606，还用于接收第一交互设备 602 返回的第二哈希值，并将第二哈希值与在通信适配器 606 本地基于认证密钥对第二随机数进行哈希运算所得的第三哈希值进行对比，若第二哈希值与第三哈希值相同，则完成通信适配器 606 与第一交互设备 602 间的双向认证。

其中，上述加密和解密的操作，以及后续的加密和解密的操作，均可以通过第一交互设备 106 的 SE 芯片或通信适配器 606 的 SE 芯片执行。例如，通信适配器 606 的 SE 芯片基于认证密钥对第一挑战码进行解密，得到第一随机数。

在其中的一个实施例中，通信适配器 606，还用于接收第一交互设备 602 发送的序列号获取请求；获取序列号获取请求指定的设备序列号；向第一交互设备 602 反馈获取的设备序列号；

第一交互设备 602，还用于基于反馈的设备序列号生成第一交互设备 602 上的认证密钥；

通信适配器 606，还用于依据获取的设备序列号生成通信适配器 606 上的认证密钥；第一交互设备 602 上的认证密钥与通信适配器 606 上的认证密钥相同。

在其中的一个实施例中，第一交互设备 602 上的认证密钥，是基于第一交互设备 602 存储的序列号加密密钥对反馈的设备序列号进行加密所得的；

通信适配器 606，还用于获取在通信适配器 606 存储的序列号加密密钥；基于序列号加密密钥对获取的设备序列号进行加密，得到通信适配器 606 上的认证密钥。

在其中的一个实施例中，通信适配器 606 和第一交互设备 602 均存储有认证密钥；认证密钥是根据通信适配器 606 的设备序列号生成的；

通信适配器 606，还用于当第一交互设备 602 基于自身存储的认证密钥映射得到工作密钥、并通过所得的工作密钥对交互数据进行加密得到加密交互数据后，接收第一交互设备 602 发送的对所示交互数据进行加密得到的加密交互数据；根据在通信适配器 606 存储的认证密钥映射得到工作密钥，基于所得的工作密钥对加密交互数据进行解密。

在其中的一个实施例中，通信适配器 606，还用于将解密所得的交互数据，转换为与原生适配设备节点的通信协议匹配的目标交互数据；通过所模拟的由第二交互设备 604 能够识别的设备节点，将经过格式转换后的目标交互数据传输至第二交互设备 604。

在其中的一个实施例中，设备节点包括人机交互键盘节点和人机交互控制器节点；通信适配器 606，还用于当目标交互数据属于控制类型数据时，将目标交互数据上报至人机交互控制器节点，以使第二交互设备 604 通过人机交互控制器节点获取目标交互数据；当目标交互数据属于交易类型数据时，将目标交互数据上报至人机交互键盘节点；

第二交互设备 604，用于通过人机交互键盘节点获取目标交互数据。

在其中的一个实施例中，通信适配器 606，还用于当加密交互数据或从第二交互设备 604 接收的控制数据属于恶意攻击包，或者接收到的来源于网络侧终端的网络数据包属于恶意攻击包时，则触发安全事件；安全事件用于禁用通信适配器 606。

其中，通信适配器 606 中的防拆点在确定受到恶意攻击时，触发安全事件以禁用通信适配器 606。

上述实施例中，在进行数据传输之前，通信适配器先完成通信适配器与第一交互设备间的双向认证，从而可以确保数据传输的双方设备是可靠的，避免了数据传输至未认证的设备而出现信息安全的问题。在完成双向认证之后，通信适配器开始接收第一交互设备发送的经过加密的加密交互数据，且该加密交互数据是依据基于双向认证时所采用的认证密钥映射所得的工作密钥对交互数据进行加密所得，从而可以有效地确保交互数据在传输过程中的安全性。此外，通信适配器通过基于自身存储的认证密钥映射得到的工作密钥对加密交互数据进行解密，通过所模拟的由第二交互设备能够识别的设备节点，基于第二交互设备的原生适配设备节点的通信协议，向第二交互设备传输解密所得的交互数据，避免了在第一交互设备和第二交互设备双方上进行数据加密和解密的过程，从而无需对两种不同设备上的软件进行适配，有利于提高软件的通用性，有利于提高第一交互设备和第二交互设备之间的交互效果。而且，由于通信适配器模拟的设备节点能够被第二交互设备识别，而且所采用的通信协议是第二交互设备原生适配的，从而通信适配器在与第二交互设备电连接时，无需安装驱动即可实现通信适配器与第二交互设备之间兼容，实现了通信适配器即插即用的效果，避免了数据传输之前的准备工作，有利于提高数据传输的整体工作效率。

在其中的一个实施例中，设备节点包括人机交互控制器节点；

通信适配器 606，还用于通过人机交互控制器节点接收第二交互设备 604 发送的控制数据；将控制数据转换为串口控制数据；根据在通信适配器 606 上对认证密钥进行映射得到的工作密钥，对串口控制数据进行加密，得到加密控制数据；将加密控制数据传输给第一交互设备 602；

第一交互设备 602，还用于通过映射认证密钥得到的工作密钥，对加密控制数据解密，以根据解密所得的控制数据执行控制操作。

上述实施例中，利用工作密钥对来自于第二交互设备的控制数据进行加密，然后将加密所得的加密控制数据传输给第一交互设备，而且第一交互设备利用映射认证密钥得到的工作密钥对加密控制数据解密，而该工作密钥是对认证密钥映射所得的工作密钥，从而可以有效地确保交互数据在传输过程中的安全性。

当数据传输系统应用于人脸支付场景时，如图 7 所示，该数据传输系统则包括人脸扫描设备、蓝牙适配器和 POS 机，其中：

A) 人脸扫描设备：包含 SE 芯片，该 SE 芯片可以用于对密钥进行管理和对蓝牙透传的数据进行加密和解密；此外，该人脸扫描设备还具备蓝牙功能，可支持蓝 4.0 及以上的版本；

B) 蓝牙适配器：包含蓝牙透传芯片、SE 芯片、HID 接口芯片和防拆点等；

其中，该 HID 接口芯片为串口转 USB HID 接口通讯芯片。

C) POS 机：商户侧的收银 POS 主机。

接下来，对蓝牙适配器所包含的器件进行具体阐述：

1) 蓝牙透传芯片

该蓝牙透传芯片可进行数据双向传输，具体如下所述：

a、将从 POS 机传输过来的、且经过 SE 芯片加密的串口数据通过蓝牙透传芯片传输给人脸扫描设备；

b、将从人脸扫描设备通过蓝牙透传芯片传输过来的、且进行了加密的数据经 SE 安全芯片解密，并将解密所得的数据传输给 POS 机。

2) HID 接口芯片

该 HID 接口芯片在插入 POS 机后，可以在 POS 机上模拟出两个 HID 设备节点，该设备节点包括 HID 键盘节点和 HID 控制器节点。该 HID 接口芯片可以将符合 HID 接口芯片传输格式的数据转换成符合 USB HID 协议标准的数据，然后通过模拟的设备节点将转换后的数据传输到 POS 机。

其中，window、android 和 linux 等系统默认都支持 USB HID 协议，实现了 POS 机侧免驱动更新，从而做到即插即用。

3) SE 芯片

该 SE 芯片的安全区存放有蓝牙适配器的密钥，如认证密钥和工作密钥；通过该 SE 芯片可以执行以下功能：

a、与人脸扫描设备进行双向认证；

b、对蓝牙透传的数据进行加密。

4) 防拆点

由于数据经过 SE 芯片解密后，解密所得的数据通过串口传输给 HID 接口芯片，若 PCB 直接暴露，数据存在被窃取的风险，因此在蓝牙适配器上配置防拆点，当有外界攻击时，防拆点可以触发安全事件，以禁用蓝牙适配器设备。

通过上述的系统，可以执行以下方法的步骤：生成认证密钥，蓝牙适配器与人脸扫描设备进行双向认证，以及数据加密和数据传输；其中：

(一) 生成认证密钥

其中，生成认证密钥的流程如图 8a 和图 8b 所示，其步骤具体可以包括：

1) 获取蓝牙适配器的设备序列号；

2) 用主密钥 KEY_Main 加密设备序列号，加密的结果结果作为认证密钥，其中，加密过程如下：

KEY_Auth=Encrypt (KEY_Main,SN)；

其中，该认证密钥再数据传输的过程中，可以基于该认证密钥生成静态或动态变化的工作密钥，利用该工作密钥对传输的数据进行加密和解密。

(二) 人脸扫描设备和蓝牙适配器进行双向认证

其中，双向认证的流程如图 8b 所示，其步骤具体可以包括：

- 1) 人脸扫描设备向蓝牙适配器请求获取设备序列号；
- 2) 人脸扫描设备根据蓝牙适配器的设备序列号生成认证密钥 KEY_Auth；
- 3) 人脸扫描设备在本地生成真随机数 TRNG_A，并对该 TRNG_A 做 Hash 运算，生成对应的哈希值 HASH_A=Hash(TRNG_A)；
- 4) 人脸扫描设备在本地用认证密钥加密真随机数 TRNG_A，生成挑战码 CODE_A；
其中，CODE_A=Encrypt(KEY_Auth,TRNG_A)；
- 5) 人脸扫描设备通过蓝牙透传的方式发送挑战码 CODE_A 给蓝牙适配器；
- 6) 蓝牙适配器采用认证密钥解密 CODE_A，并对解密所得的真随机数 TRNG_A 进行 hash 运算，得到 HASH_A1；
- 7) 蓝牙适配器在本地生成真随机数 TRNG_B；
- 8) 蓝牙适配器利用认证密钥加密 HASH_A1 和 TRNG_B，得到挑战码 CODE_B；
其中，CODE_B=Encrypt(KEY_Auth,HASH_A1,TRNG_B)；
- 9) 蓝牙适配器将挑战码 CODE_B 通过蓝牙透传的方式发送给人脸扫描设备；
- 10) 人脸扫描设备利用认证密钥解密 CODE_B，得到 HASH_A1 和 TRNG_B；
- 11) 人脸扫描设备将自身生成的 HASH_A 和由蓝牙适配器生成的 HASH_A1 进行对比，当对比的结果表示 HASH_A 和 HASH_A1 匹配时，则蓝牙适配器通过人脸扫描设备的认证；否则，则认证失败，流程终止；
- 12) 人脸扫描设备对蓝牙适配器的真随机数 TRNG_B 进行 Hash 运算，得到 HASH_B1；
- 13) 人脸扫描设备利用认证密钥对 HASH_B1 加密，并通过蓝牙透传的方式传输到蓝牙适配器；
- 14) 蓝牙适配器利用认证密钥对加密的 HASH_B1 进行解密，得到 HASH_B；
- 15) 蓝牙适配器将自身生成的 HASH_B 和由人脸扫描设备生成的 HASH_B1 进行对比，若对比的结果表示 HASH_B 与 HASH_B1 匹配，则人脸扫描设备通过蓝牙适配器的认证；否则，则认证失败，流程终止。

(三) 人脸扫描设备和蓝牙适配器在完成双向认证智慧，按照蓝牙标准协议完成配对，建立数据通信链路。

(四) 数据加密传输

- 1) 人脸扫描设备和蓝牙适配器的蓝牙传输通路建立之后，根据认证密钥生成工作密码；
- 2) 再进行双向传输数据时，SE 芯片可以利用工作密钥对数据进行加解密运算，实现对蓝牙透传的数据加解密；

不同类型或业务的数据，传输的过程相类似，但也存在一些差别，具体如下：

(1) 付款码数据的传输

- A) 人脸扫描设备产生付款码；
- B) 人脸扫描设备的 SE 芯片采用认证密钥对付款码数据加密；

- C) 通过蓝牙透传的方式, 将加密后的付款码数据传输到蓝牙适配器上的蓝牙透传芯片;
- D) 蓝牙适配器上的蓝牙透传芯片再收到加密的付款码数据后, 通过串口传输该加密的付款码数据至蓝牙适配器上的 SE 芯片;
- E) 该 SE 芯片采用认证密钥解密该付款码数据;
- F) 该 SE 芯片把解密后的付款码数据通过串口传输给 HID 接口芯片;
- G) HID 接口芯片接收到的付款码数据转换成符合 HID 协议的付款码数据, 然后上报到 HID 键盘节点;
- H) POS 机通过 HID 键盘节点获得付款码数据, 然后将该付款码数据给应用层调用。

(2) 控制数据的传输

其中, 控制数据可以在数据传输系统中进行双向通信。

人脸扫描设备传输控制数据的流程与传输付款码数据的流程类似; 主要区别在于 POS 机对应的设备节点不同, 控制数据传输到 HID 控制器节点, 而付款码数据传输到 HID 键盘节点。接下来重点介绍 POS 机传输控制数据到人脸扫描设备的流程:

- A) POS 机中的应用层 ERP (Enterprise Resource Planning, 企业资源计划) 系统将控制数据下发给 HID 控制器节点;
- B) 驱动层将控制器节点收到的控制数据通过 USB 传输给相对应的硬件设备 CH9329;
- C) CH9329 把 USB 接口收到的控制数据转换成串口类型的控制数据发送给 dongle 上的 SE 安全芯片;
- D) 安全芯片用认证过的密钥对控制数据加密, 并把加密后的控制数据通过串口发送给蓝牙透传芯片;
- E) 蓝牙透传芯片 CH9141 把收到的密文通过蓝牙透传给人脸扫描设备;
- F) 人脸扫描设备把从蓝牙收到的控制数据给到人脸扫描设备内部的 SE 芯片;
- G) SE 芯片用认证过的密钥解密控制数据;
- H) 解密后的控制数据给到应用层调用。

通过实施上述实施例的方案, 可以产生以下有益效果:

首先, 采用无线传输的方式, 具备低成本、免驱和双向通信等优点;

其次, 对蓝牙传输的数据本身进行加解密, 提高了数据传输的安全性。

应该理解的是, 虽然图 2-4 的流程图中的各个步骤按照箭头的指示依次显示, 但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明, 这些步骤的执行并没有严格的顺序限制, 这些步骤可以以其它的顺序执行。而且, 图 2-4 中的至少一部分步骤可以包括多个步骤或者多个阶段, 这些步骤或者阶段并不必然是在同一时刻执行完成, 而是可以在不同的时刻执行, 这些步骤或者阶段的执行顺序也不必然是依次进行, 而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

在一个实施例中, 如图 9 所示, 提供了一种数据传输装置, 该装置可以采用软件模块或

硬件模块，或者是二者的结合成为计算机设备的一部分，该装置具体包括：认证模块 902、接收模块 904、解密模块 906 和发送模块 908，其中：

认证模块 902，用于与第一交互设备进行双向认证；

接收模块 904，用于当完成双向认证后，接收第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；工作密钥是由第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

解密模块 906，用于根据在通信适配器上对认证密钥进行映射得到的工作密钥，对加密交互数据进行解密；

发送模块 908，用于通过所模拟的由第二交互设备能够识别的设备节点，基于第二交互设备的原生适配设备节点的通信协议，向第二交互设备传输解密所得的交互数据。

在一个实施例中，认证模块 902，还用于接收第一交互设备发送的第一挑战码；基于认证密钥对第一挑战码进行解密，得到第一随机数；第一随机数是由第一交互设备生成的随机数；生成第二随机数，并对第一随机数进行哈希运算，得到第一哈希值；基于认证密钥加密第一哈希值和第二随机数，得到第二挑战码；向第一交互设备发送第二挑战码，以使第一交互设备基于认证密钥解密第二挑战码得到第一哈希值，将第一哈希值与第一交互设备基于认证密钥对第一随机数加密所得的第二哈希值进行对比，若第一哈希值和第二哈希值相同，则对解密第二挑战码所得的第二随机数进行哈希运算，将哈希运算所得的第二哈希值进行返回；接收第一交互设备返回的第二哈希值，并将第二哈希值与在通信适配器本地基于认证密钥对第二随机数进行哈希运算所得的第三哈希值进行对比，若第二哈希值与第三哈希值相同，则完成通信适配器与第一交互设备间的双向认证。

在一个实施例中，如图 10 所示，装置还包括：

接收模块 904，还用于接收第一交互设备发送的序列号获取请求；

获取模块 910，用于获取序列号获取请求指定的设备序列号；

发送模块 908，还用于向第一交互设备反馈获取的设备序列号，以使第一交互设备基于反馈的设备序列号生成第一交互设备上的认证密钥；

生成模块 912，用于依据获取的设备序列号生成通信适配器上的认证密钥；第一交互设备上的认证密钥与通信适配器上的认证密钥相同。

在一个实施例中，第一交互设备上的认证密钥，是基于第一交互设备存储的序列号加密密钥对反馈的设备序列号进行加密所得的；

生成模块 912，还用于获取在通信适配器存储的序列号加密密钥；基于序列号加密密钥对获取的设备序列号进行加密，得到通信适配器上的认证密钥。

在一个实施例中，通信适配器和第一交互设备均存储有认证密钥；认证密钥是根据通信适配器的设备序列号生成的；

接收模块 904，还用于当第一交互设备基于自身存储的认证密钥映射得到工作密钥、并通过所得的工作密钥对交互数据进行加密得到加密交互数据后，接收第一交互设备发送的对所示交互数据进行加密得到的加密交互数据；

解密模块 906, 还用于根据在通信适配器存储的认证密钥映射得到工作密钥, 基于所得的工作密钥对加密交互数据进行解密。

在一个实施例中, 发送模块 908, 还用于将解密所得的交互数据, 转换为与原生适配设备节点的通信协议匹配的目标交互数据; 通过所模拟的由第二交互设备能够识别的设备节点, 将经过格式转换后的目标交互数据传输至第二交互设备。

在一个实施例中, 设备节点包括人机交互键盘节点和人机交互控制器节点;

发送模块 908, 还用于当目标交互数据属于控制类型数据时, 将目标交互数据上报至人机交互控制器节点, 以使第二交互设备通过人机交互控制器节点获取目标交互数据; 当目标交互数据属于交易类型数据时, 将目标交互数据上报至人机交互键盘节点, 以使第二交互设备通过人机交互键盘节点获取目标交互数据。

在一个实施例中, 如图 10 所示, 该装置还包括:

触发模块 914, 用于当加密交互数据或从第二交互设备接收的控制数据属于恶意攻击包, 或者接收到的来源于网络侧终端的网络数据包属于恶意攻击包时, 则触发安全事件; 安全事件用于禁用通信适配器。

上述实施例中, 在进行数据传输之前, 先完成通信适配器与第一交互设备间的双向认证, 从而可以确保数据传输的双方设备是可靠的, 避免了数据传输至未认证的设备而出现信息安全的问题。在完成双向认证之后, 通信适配器开始接收第一交互设备发送的经过加密的加密交互数据, 且该加密交互数据是依据基于双向认证时所采用的认证密钥映射所得的工作密钥对交互数据进行加密所得, 从而可以有效地确保交互数据在传输过程中的安全性。此外, 通信适配器通过基于自身存储的认证密钥映射得到的工作密钥对加密交互数据进行解密, 通过所模拟的由第二交互设备能够识别的设备节点, 基于第二交互设备的原生适配设备节点的通信协议, 向第二交互设备传输解密所得的交互数据, 避免了在第一交互设备和第二交互设备双方上进行数据加密和解密的过程, 从而无需对两种不同设备上的软件进行适配, 有利于提高软件的通用性, 有利于提高第一交互设备和第二交互设备之间的交互效果。而且, 由于通信适配器模拟的设备节点能够被第二交互设备识别, 而且所采用的通信协议是第二交互设备原生适配的, 从而通信适配器在与第二交互设备电连接时, 无需安装驱动即可实现通信适配器与第二交互设备之间兼容, 实现了通信适配器即插即用的效果, 避免了数据传输之前的准备工作, 有利于提高数据传输的整体工作效率。

在一个实施例中, 设备节点包括人机交互控制器节点; 如图 10 所示, 该装置还包括:

接收模块 904, 还用于通过人机交互控制器节点接收第二交互设备发送的控制数据;

转换模块 916, 用于将控制数据转换为串口控制数据;

加密模块 918, 用于根据在通信适配器上对认证密钥进行映射得到的工作密钥, 对串口控制数据进行加密, 得到加密控制数据;

发送模块 908, 还用于将加密控制数据传输给第一交互设备; 加密控制数据, 用于指示第一交互设备通过映射认证密钥得到的工作密钥, 对加密控制数据解密, 以根据解密所得的控制数据执行控制操作。

上述实施例中，利用工作密钥对来自于第二交互设备的控制数据进行加密，然后将加密所得的加密控制数据传输给第一交互设备，而且第一交互设备利用映射认证密钥得到的工作密钥对加密控制数据解密，而该工作密钥是对认证密钥映射所得的工作密钥，从而可以有效地确保交互数据在传输过程中的安全性。

关于数据传输装置的具体限定可以参见上文中对于数据传输方法的限定，在此不再赘述。上述数据传输装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一个实施例中，提供了一种计算机设备，该计算机设备可以是蓝牙适配器，其内部结构图可以如图 11 所示。该计算机设备包括通过系统总线连接的处理器、存储器和网络接口。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存。该非易失性存储介质存储有操作系统、计算机可读指令和数据库。该内存为易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的数据库用于存储交互数据、认证密钥和工作密钥等。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种数据传输方法。

本领域技术人员可以理解，图 11 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

在一个实施例中，还提供了一种计算机设备，包括存储器和处理器，存储器中存储有计算机可读指令，该处理器执行计算机可读指令时实现上述各方法实施例中的步骤。

在一个实施例中，提供了一种计算机可读存储介质，存储有计算机可读指令，该计算机可读指令被处理器执行时实现上述各方法实施例中的步骤。

在一个实施例中，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指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述各方法实施例中的步骤。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory, ROM）、磁带、软盘、闪存或光存储器等。易失性存储器可包括随机存取存储器（Random Access Memory, RAM）或外部高速缓冲存储器。作为说明而非局限，RAM 可

以是多种形式，比如静态随机存取存储器（Static Random Access Memory, SRAM）或动态随机存取存储器（Dynamic Random Access Memory, DRAM）等。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

权利要求书

1、一种数据传输方法，其特征在于，执行于通信适配器，所述方法包括：

与第一交互设备进行双向认证；

当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；

通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

2、根据权利要求1所述的方法，其特征在于，所述与第一交互设备进行双向认证包括：

接收所述第一交互设备发送的第一挑战码；

基于所述认证密钥对所述第一挑战码进行解密，得到第一随机数；所述第一随机数是由所述第一交互设备生成的随机数；

对所述第一随机数进行哈希运算，得到第一哈希值；

生成第二随机数，并基于所述认证密钥加密所述第一哈希值和第二随机数，得到第二挑战码；

向所述第一交互设备发送所述第二挑战码，以使所述第一交互设备基于所述认证密钥解密所述第二挑战码得到第一哈希值，将所述第一哈希值与所述第一交互设备基于所述认证密钥对所述第一随机数加密所得的第二哈希值进行对比，若所述第一哈希值和所述第二哈希值相同，则对解密所述第二挑战码所得的第二随机数进行哈希运算，将哈希运算所得的第二哈希值进行返回；

接收所述第一交互设备返回的所述第二哈希值，并将所述第二哈希值与在所述通信适配器本地基于所述认证密钥对所述第二随机数进行哈希运算所得的第三哈希值进行对比，若所述第二哈希值与所述第三哈希值相同，则完成所述通信适配器与所述第一交互设备间的双向认证。

3、根据权利要求2所述的方法，其特征在于，所述方法还包括：

接收所述第一交互设备发送的序列号获取请求；

获取所述序列号获取请求指定的设备序列号；

向所述第一交互设备反馈获取的设备序列号，以使所述第一交互设备基于反馈的所述设备序列号生成所述第一交互设备上的认证密钥；

依据获取的所述设备序列号生成所述通信适配器上的认证密钥；所述第一交互设备上的认证密钥与所述通信适配器上的认证密钥相同。

4、根据权利要求3所述的方法，其特征在于，所述第一交互设备上的认证密钥，是基于所述第一交互设备存储的序列号加密密钥对反馈的所述设备序列号进行加密所得的；

所述依据获取的设备序列号生成所述通信适配器上的认证密钥包括：

获取在所述通信适配器存储的所述序列号加密密钥；

基于所述序列号加密密钥对获取的设备序列号进行加密，得到通信适配器上的认证密钥。

5、根据权利要求2所述的方法，其特征在于，所述通信适配器和所述第一交互设备均存储有所述认证密钥；所述认证密钥是根据所述通信适配器的设备序列号生成的；所述接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据包括：

当所述第一交互设备基于自身存储的认证密钥映射得到工作密钥、并通过所得的工作密钥对交互数据进行加密得到加密交互数据后，接收所述第一交互设备发送的对所述交互数据进行加密得到的所述加密交互数据；

所述根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密包括：

根据在所述通信适配器存储的认证密钥映射得到工作密钥，基于所得的工作密钥对所述加密交互数据进行解密。

6、根据权利要求1所述的方法，其特征在于，所述通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据包括：

将解密所得的交互数据，转换为与原生适配所述设备节点的通信协议匹配的目标交互数据；

通过所模拟的由第二交互设备能够识别的设备节点，将经过格式转换后的目标交互数据传输至所述第二交互设备。

7、根据权利要求6所述的方法，其特征在于，所述设备节点包括人机交互键盘节点和人机交互控制器节点；所述通过所模拟的由第二交互设备能够识别的设备节点，将经过格式转换后的交互数据传输至所述第二交互设备包括：

当所述目标交互数据属于控制类型数据时，将所述目标交互数据上报至所述人机交互控制器节点，以使所述第二交互设备通过所述人机交互控制器节点获取所述目标交互数据；

当所述目标交互数据属于交易类型数据时，将所述目标交互数据上报至所述人机交互键盘节点，以使所述第二交互设备通过所述人机交互键盘节点获取所述目标交互数据。

8、根据权利要求1至7任一项所述的方法，其特征在于，所述设备节点包括人机交互控制器节点；所述方法还包括：

通过所述人机交互控制器节点接收所述第二交互设备发送的控制数据；

将所述控制数据转换为串口控制数据；

根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述串口控制数据进行加密，得到加密控制数据；

将所述加密控制数据传输给所述第一交互设备；所述加密控制数据，用于指示所述第一交互设备通过映射所述认证密钥得到的工作密钥，对所述加密控制数据解密，以根据解密所得的控制数据执行控制操作。

9、根据权利要求1至7任一项所述的方法，其特征在于，所述方法还包括：

当所述加密交互数据或从所述第二交互设备接收的控制数据属于恶意攻击包，或者接收到的来源于网络侧终端的网络数据包属于所述恶意攻击包时，则
触发安全事件；所述安全事件用于禁用所述通信适配器。

10、一种数据传输装置，其特征在于，所述装置包括：

认证模块，用于与第一交互设备进行双向认证；

接收模块，用于当完成双向认证后，接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；所述工作密钥是由所述第一交互设备对双向认证时所采用的认证密钥进行映射得到的；

解密模块，用于根据在通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；

发送模块，用于通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

11、一种数据传输系统，其特征在于，所述系统包括：第一交互设备、第二交互设备以及与所述第一交互设备无线连接、且与所述第二交互设备电连接的通信适配器；

所述通信适配器，用于对所述第一交互设备进行认证；

所述第一交互设备，用于当所述通信适配器完成认证时，对所述通信适配器进行认证，并在认证完成后，基于对双向认证时所采用的认证密钥进行映射得到的工作密钥加密交互数据，得到加密交互数据；

所述通信适配器，还用于接收所述第一交互设备所发送的基于工作密钥加密交互数据得到的加密交互数据；

所述通信适配器，还用于根据在所述通信适配器上对所述认证密钥进行映射得到的工作密钥，对所述加密交互数据进行解密；

所述第二交互设备，用于识别所述通信适配器所模拟的设备节点；

所述通信适配器，还用于通过所模拟的由第二交互设备能够识别的设备节点，基于所述第二交互设备的原生适配所述设备节点的通信协议，向所述第二交互设备传输解密所得的交互数据。

12、根据权利要求 11 所述的系统，其特征在于，

所述通信适配器，还用于接收所述第一交互设备发送的第一挑战码；基于所述认证密钥对所述第一挑战码进行解密，得到第一随机数；所述第一随机数是由所述第一交互设备生成的随机数；对所述第一随机数进行哈希运算，得到第一哈希值；生成第二随机数，并基于所述认证密钥加密所述第一哈希值和第二随机数，得到第二挑战码；向所述第一交互设备发送所述第二挑战码；

所述第一交互设备，还用于基于所述认证密钥解密接收的第二挑战码得到第一哈希值，将所述第一哈希值与所述第一交互设备基于所述认证密钥对所述第一随机数加密所得的第二

哈希值进行对比，若所述第一哈希值和所述第二哈希值相同，则对解密所述第二挑战码所得的第二随机数进行哈希运算，将哈希运算所得的第二哈希值进行返回；

所述通信适配器，还用于接收所述第一交互设备返回的所述第二哈希值，并将所述第二哈希值与在所述通信适配器本地基于所述认证密钥对所述第二随机数进行哈希运算所得的第三哈希值进行对比，若所述第二哈希值与所述第三哈希值相同，则完成所述通信适配器与所述第一交互设备间的双向认证。

13、根据权利要求 11 所述的系统，其特征在于，所述通信适配器，还用于将解密所得的交互数据，转换为与原生适配所述设备节点的通信协议匹配的目标交互数据；通过所模拟的由第二交互设备能够识别的设备节点，将经过格式转换后的目标交互数据传输至所述第二交互设备。

14、一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现权利要求 1 至 9 中任一项所述的方法的步骤。

15、一种计算机可读存储介质，存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现权利要求 1 至 9 中任一项所述的方法的步骤。