(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
2018 年 10 月 4 日 (04.10.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/177188 A1

(51) 国际专利分类号:
G07C 9/00 (2006.01)

(21) 国际申请号: PCT/CN2018/079999

(22) 国际申请日: 2018 年 3 月 22 日 (22.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710198457.1 2017年3月29日 (29.03.2017) CN

(71) 申请人: 云丁网络技术（北京）有限公司 (YUN DING NETWORK TECHNOLOGY (BEIJING) CO., LTD.) [CN/CN]; 中国北京市昌平区回龙观东大街388号回龙观创客广场A座5层, Beijing 102208 (CN)。

(72) 发明人: 唐皓 (TANG, Hao); 中国北京市昌平区回龙观东大街388号回龙观创客广场A座5层, Beijing 102208 (CN)。 陈彬 (CHEN, Bin); 中国北京市昌平区回龙观东大街388号回龙观创客广场A座5层, Beijing 102208 (CN)。 张东胜 (ZHANG, Dongsheng); 中国北京市昌平区回龙观东大街388号回龙观创客广场A座5层, Beijing 102208 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

WO 2018/177188 A1

(54) **Title:** SECURE COMMUNICATION METHOD BASED ON SMART DOOR LOCK SYSTEM AND SMART DOOR LOCK SYSTEM THEREOF

(54) **发明名称:** 一种基于智能门锁系统的安全通信方法及其智能门锁系统

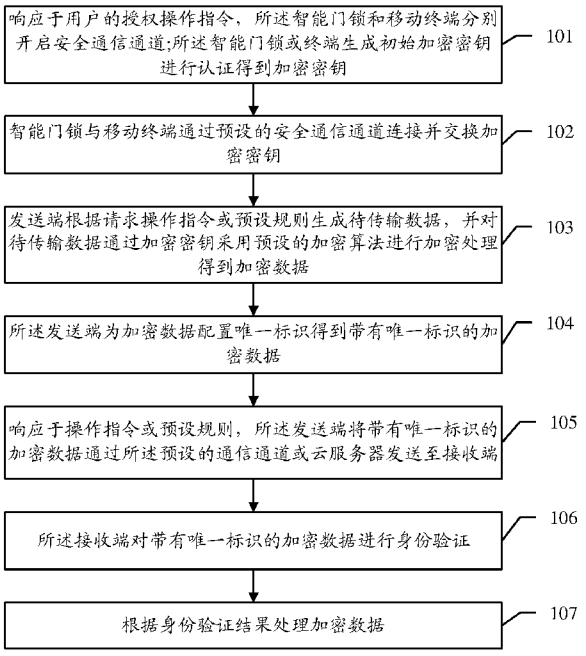

图 2

101 A SMART DOOR LOCK AND A MOBILE TERMINAL SEPARATELY ACTIVATE A SECURE COMMUNICATION CHANNEL IN RESPONSE TO AN AUTHORIZED OPERATION INSTRUCTION OF USERS; AND THE SMART DOOR LOCK OR THE MOBILE TERMINAL GENERATES AN INITIAL ENCRYPTION KEY FOR AUTHENTICATION TO OBTAIN AN ENCRYPTION KEY

102 THE SMART DOOR LOCK AND THE MOBILE TERMINAL ARE CONNECTED AND EXCHANGE THE ENCRYPTION KEY VIA A PRESET SECURE COMMUNICATION CHANNEL

103 A SENDING END GENERATES, ACCORDING TO A REQUEST OPERATION INSTRUCTION OR A PRESET RULE, DATA TO BE TRANSMITTED, AND ENCRYPTS THE DATA TO BE TRANSMITTED BY USING A PRESET ENCRYPTION ALGORITHM VIA THE ENCRYPTION KEY TO OBTAIN ENCRYPTED DATA

104 THE SENDING END CONFIGURES A UNIQUE IDENTIFIER FOR THE ENCRYPTED DATA TO OBTAIN ENCRYPTED DATA WITH THE UNIQUE IDENTIFIER

105 THE SENDING END SENDS THE ENCRYPTED DATA WITH THE UNIQUE IDENTIFIER TO A RECEIVING END VIA THE PRESET COMMUNICATION CHANNEL OR A CLOUD SERVER IN RESPONSE TO AN OPERATION INSTRUCTION OR A PRESET RULE

106 THE RECEIVING END AUTHENTICATES THE ENCRYPTED DATA WITH THE UNIQUE IDENTIFIER

107 PROCESS THE ENCRYPTED DATA ACCORDING TO AN AUTHENTICATION RESULT

(57) **Abstract:** Provided is a secure communication method based on a smart door lock system, the smart door lock system comprising a smart door lock and a mobile terminal. The method comprises: a sending end generating data to be transmitted and encrypting the data by using a preset encryption algorithm via an encryption key to obtain encrypted data (103), the encryption key being obtained through connection and exchange between the smart door lock and the mobile terminal via a preset secure communication channel (102); the sending end configuring a unique identifier for the encrypted data (104); sending encrypted data with the unique identifier to a receiving end (105), such that the receiving end authenticates the encrypted data with the unique identifier (106); and processing, according to

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

an authentication result, the encrypted data by means of the encryption key obtained through exchange (107). In the method, since a server does not save any key, the server cannot understand data forwarded by itself, such that data encryption, identity authentication, and anti-replay and anti-tamper functions in the communication between the smart door lock and the mobile terminal are still effective even if the server is broken, thereby ensuring data security.

(57) 摘要: 一种基于智能门锁系统的安全通信方法，智能门锁系统包括智能门锁和移动终端，方法包括：发送端生成待传输数据并通过加密密钥采用预设的加密算法进行加密得到加密数据(103)；其中，加密密钥为智能门锁与移动终端通过预设的安全通信通道连接并交换得到(102)；发送端为加密数据配置唯一标识(104)，将带有唯一标识的加密数据发送至接收端(105)以便接收端对带有唯一标识的加密数据进行身份验证(106)，根据身份验证结果利用交换得到的加密密钥处理加密数据(107)。本方法由于服务器不保存任何密钥，则服务器无法理解由其转发的数据，即使服务器被攻破，智能门锁与移动终端的通信中的数据加密、身份验证、防重放防篡改依然有效，保证了数据的安全性。

一种基于智能门锁系统的安全通信方法及其智能门锁系统

本申请要求于 2017 年 03 月 29 日提交中国专利局、申请号为201710198457.1、申请名称为“一种基于智能门锁系统的安全通信方法及其智能门锁系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及一种安全通信方法，属于智能家居和安防技术领域。

背景技术

现有市场中大部分智能门锁均具备联网功能；使得智能门锁的信息可以上报给服务器，从而转发到用户使用的应用程序(Application，APP)等工具上；用户也可以远程通过服务器下发密码、设置权限等。随着智能门锁的安装量越大，远程通信的安全性就越重要。服务器作为转发的核心，被攻击的风险很大。进而导致门锁被攻击导致密码泄露或被打开等严重事故。

针对这一问题，目前已有的解决方法包括以下方式：

（1）禁止远程开锁功能。但是智能门锁一般可以远程下发密码、蓝牙密钥等，如果服务器被攻破，可以通过下发密码、蓝牙密钥的方式，获得开锁权限，而后在本地执行开锁操作。

（2）门锁与服务器之间采用加密通信，用户 APP 与服务器也采用 https 等加密方式。该方法虽然杜绝了通信链路上的数据抓取，但因为服务器上保存了密码、蓝牙密钥等关键信息，攻击者可以从服务器获得密码和蓝牙密钥。同时因为没有身份验证、防重放、防篡改功能，无法解决服务器被攻击后，下发相关命令给门锁或者手机客户端。

（3）服务器与手机客户端、门锁端的通信中，进一步增加防重放、防篡改功能。但因为服务器被攻破后，可以模拟服务器与两端的正常通信，对服务器端的身份校验无法拦截。

目前，市场上未发现能够实现可保证服务器端或者内部人员也无法从服务器端获得用户的传输信息，或即使服务器被攻破，门锁与手机客户端的通信中的身份验证、防重放、防篡改依然有效的安全的基于智能门锁的通信方法。

发明内容

本发明的目的就是克服上述缺点，提出一种基于智能门锁系统的安全通信方法，所采用的技术方案如下：

本申请第一方面提供了一种安全通信方法，所述方法应用于智能门锁系统，所述智能门锁系统包括智能门锁和移动终端，所述方法包括：

发送端根据操作指令或预设规则生成待传输数据，并对所述待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据；所述发送端为智能门锁或移动终端；所述加密密钥为所述智能门锁与所述移动终端通过预设的安全通信通道连接并交换得到；所述安全通信通道为经所述智能门锁和所述移动终端授权触发的短距离无线通信通道或近场通信通道；

所述发送端为所述加密数据配置唯一标识得到带有唯一标识的加密数据；

所述发送端将所述带有唯一标识的加密数据发送至接收端 以便所述接收端所述对带有唯一标识的加密数据进行身份验证，并根据身份验证结果，利用交换得到的加密密钥对所述加密数据进行解密处理；

其中，所述发送端为智能门锁时，所述接收端为移动终端；所述发送端为移动终端时，所述接收端为智能门锁。

进一步的，所述发送端将所述带有唯一标识的加密数据发送至接收端包括：

所述发送端将所述带有唯一标识的加密数据通过预设通信通道或云服务器发送至接收端；所述预设通信通道为短距离无线通信或近场通信信道。

进一步的，所述加密密钥为所述智能门锁或终端响应于用户的授权操作指令，生成初始加密密钥，并由所述智能门锁和所述移动终端对所述初始加密密钥进行认证得到；其中，所述初始加密密钥为所述智能门锁或所述移动终端自动生成或手动输入的密钥；所述初始加密密钥通过所述安全通信通道在所述智能门锁和所述移动终端之间进行传输。

进一步的，所述加密密钥为第一加密密钥；所述对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括：

通过所述第一加密密钥采用对称加密算法对待传输数据进行加密得到初始加密数据；

为所述初始加密数据配置预设密钥值；所述预设密钥值为当前时间戳、计数器值和随机码中的至少一种；

为配置有所述预设密钥值的初始加密数据添加验证签名得到加密数据。

进一步的，所述发送端和接收端分别保存的加密密钥包括一公开密钥和一私有密钥；所述对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括：

发送端通过自身保存的所述公开密钥采用非对称加密算法对待传输数据进行加密得到初始加密数据；

为所述初始加密数据配置预设密钥值；所述预设密钥值为当前时间戳、计数器值和随机码中的至少一种；

为配置有所述预设密钥值的初始加密数据添加发送端保存的所述私有密钥作为验证签名得到加密数据。

进一步的，所述方法还包括：

备用移动终端获取账户登录验证信息，所述账户登录验证信息为用于验证用户身份的信息；所述备用移动终端为所述移动终端的备用设备；

若所述账户登录验证信息通过，则所述备用移动终端响应于用户的授权删除操作，向智能门锁发出第一删除指令，用于指示所述智能门锁删除本地保存的指定加密密钥信息；和/或，所述备用移动终端响应于用户的远程授权删除操作，向云服务器发出第二删除指令，用于指示所述云服务器删除所述移动终端保存的加密密钥信息。

本申请第二方面提供了一种安全通信方法，所述方法应用于智能门锁系统，所述智能门锁系统包括智能门锁和移动终端，所述方法包括：

所述接收端接收所述发送端发送的带有唯一标识的加密数据；所述发送端为智能门锁时，所述接收端为移动终端；所述发送端为移动终端时，所述接收端为智能门锁；所述带有唯一标识的加密数据为所述发送端根据操作指令或预设规则生成待传输数据，并对所述待传输数据通过加密密钥采用预设的加密算法进行加密，并配置唯一标识得到；所述加密密钥为所述智能门锁与所述移动终端通过预设的安全通信通道连接并交换得到；所述安全通信通道为经所述智能门锁和所述移动终端授权触发的短距离无线通信通道或近场通信通道；

所述接收端对所述带有唯一标识的加密数据进行身份验证，得到身份验证结果；

所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述加密数据进行解密处理得到所述待传输数据。

进一步的，所述加密密钥为第一加密密钥，所述加密数据为所述发送端通过所述第一加密密钥采用对称加密算法对所述待传输数据进行加密得到初始加密数据，为所述初始加密数据配置预设密钥值，为配置有所述预设密钥值的初始加密数据添加验证签名得到；

则所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述加密数据进行解密处理得到所述待传输数据包括：

若所述身份验证结果匹配，则所述接收端对所述加密数据的所述验证签名进行验证；

若所述验证签名匹配，则验证所述预设密钥值是否合法；

若所述预设密钥值合法，则所述接收端从所述加密数据中获取所述初始加密数据，并通过所述第一加密密钥采用所述对称加密算法的逆算法对所述初始加密数据进行解密得到所述待传输数据。

进一步的，所述发送端和所述接收端分别保存的加密密钥包括一公开密钥和一私有密钥；所述加密数据为所述发送端通过自身保存的所述公开密钥采用非对称加密算法对所述待传输数据进行加密得到初始加密数据，为所述初始加密数据配置预设密钥值，为配置有所述预设密钥值的初始加密数据添加所述发送端保存的所述私有密钥作为验证签名得到；

则所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述加密数据进行解密处理得到所述待传输数据包括：

若所述身份验证结果为匹配，则所述接收端采用自身存储的公开密钥对所述加密数据的所述验证签名进行验证；

若所述验证签名匹配，则验证所述预设密钥值是否合法；

若所述预设密钥值合法，则所述接收端从所述加密数据中获取所述初始加密数据，并通过自身存储的所述私有密钥采用所述非对称加密算法对所述初始加密数据进行解密得到所述待传输数据。

进一步的，所述接收端对所述带有唯一标识的加密数据进行身份验证包括：

所述接收端提取所述带有唯一标识的加密数据中的唯一标识；

根据所述唯一标识分析得到与所述唯一标识匹配的加密密钥；

根据所述加密密钥确定身份验证结果。

本发明第三方面还提供一种智能门锁系统，包括：

智能门锁，用于通过预设的加密算法，采用加密密钥对待传输数据进行加密以及对接收到的加密数据进行解密；所述智能门锁设有短距离无线通信模块；

移动终端，用于通过预设的与所述智能门锁相同的加密算法，采用所述加密密钥对所述待传输数据进行加密以及对接收到的所述加密数据进行解密；所述移动终端还用于控制所述智能门锁，所述移动终端设有短距离无线通信模块，用于和所述智能门锁通信。

进一步的，所述智能门锁还包括配置模式启动模块，用于启动配置模式进行加密密钥的生成和交换，所述配置模式启动模块包括：配置按钮、配置模式触摸键、用于输入管理员密码的触摸屏或用于输入管理员权限的指纹的指纹采集器中的至少一种。

进一步的，所述移动终端控制所述智能门锁具体包括通过用于控制智能门锁的 APP 对所述智能门锁进行控制，所述用于控制智能门锁的 APP 内还设置有启动配置模式的虚拟按键用于启动移动终端的配置模式。

本申请的基于智能门锁系统的安全通信方法，所述智能门锁和移动终端均是在用户授权的情况下触发安全通信，即所述智能门锁与每个移动终端的 APP 均是在获得授权许可的前提下通过短距离无线通信通道或近场通信通道发送和交换加密密钥，保证安全性的密钥交换；并在智能门锁端和每个移动终端的 APP 设置有相同或匹配的加密算法，在本地进行加密和解密过程，实现端到端的数据加密的通信方式。可以保证服务器端或者智能门锁厂家的内部工作人员亦无法从服务器端获得用户的传输信息，保证即使服务器被攻破，门锁与手机客户端的通信中的数据加密、身份验证、防重放、防篡改依然有效，进一步保证了用户信息的安全性。且由于加密密钥的生成和交换均在移动终端和智能门锁本地通过短距离无线通信或近场通信通道完成，则服务器中不包含任何相关密钥，服务器也无法理解由其转发的数据，保证了数据的安全性；即使服务器被攻击，服务器、或者与服务器通信的链路上，有人伪造命令发给手机客户端或者门锁，因为身份验证无法通过，手机客户端或者门锁均不会响应；服务器或者与服务器通信的链路上有人重放或者篡改命令，手机客户端或者门锁均可以分析并不做响应。如果发生了以上攻击，手机客户端或者门锁必要时向服务

器报警或者本地报警。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为本申请的智能门锁系统的结构示意图；

图 2 为本申请的基于智能门锁系统的安全通信方法的流程示意图；

图 3 为本申请的步骤 S103 的一种实施例流程示意图；

图 4 为本申请的步骤 S107 的一种实施例流程示意图。

具体实施方式

本发明实施例提供了一种智能门锁的开锁方法。

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。下面将参照附图更详细地描述本公开的示例

性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

请参阅图 1 本申请的智能门锁系统的结构示意图，如图 1 所示：

本申请的智能门锁系统包括：智能门锁和移动终端；

所述智能门锁，用于通过预设的加密算法，采用加密密钥对待传输数据进行加密以及对接收到的加密数据进行解密；所述智能门锁设有短距离无线通信模块；蓝牙通信模块、紫蜂协议（zigbee）通信模块或近场通信（NFC）通信模块中的至少一种；

所述移动终端，用于通过预设的与所述智能门锁相同的加密算法，采用所述加密密钥对所述待传输数据进行加密以及对接收到的所述加密数据进行解密；所述移动终端还用于控制所述智能门锁，所述移动终端设有短距离无线通信模块，用于和所述智能门锁通信。

其中，短距离无线通信模块可以包括蓝牙通信模块、zigbee 通信模块或近场通信（NFC）通信模块中的至少一种。基于该短距离无线通信模块，可以建立预设通信信道，预设通信通道可以为短距离无线通信或近场通信信道。智能门锁和移动终端可以通过预设通信信道进行数据传输，例如，智能门锁或移动终端可以通过该预设通信传输加密数据。

在本申请实施例一些可能的实现方式中，智能门锁系统还可以包括云服务器，移动终端和智能门锁可以通过云服务器进行远程数据传输。

所述智能门锁还包括配置模式启动模块，用于启动配置模式进行加密密钥的生成和交换，所述配置模式模块包括：配置按钮、配置模式触摸键、用于输入管理员密码的触摸屏或用于输入管理员权限的指纹的指纹采集器中的至少一种。

所述移动终端可以通过用于控制智能门锁的 APP 对智能门锁进行控制，其中，用于控制智能门锁的 APP 内还设置有启动配置模式的虚拟按键，用于启动移动终端的配置模式。

所述智能门锁系统用于实现以下基于智能门锁系统的安全通信方法。

请参阅图 2，图 2 为本申请的基于智能门锁系统的安全通信方法的流程示意图；如图 2 所示：为本申请实施例提供的一种基于上述智能门锁系统的安全

通信方法，包括:

步骤 S102: 智能门锁与移动终端通过预设的安全通信通道连接并交换加密密钥; 所述安全通信通道为经智能门锁和移动终端授权触发的通信通道，所述通信通道采用短距离无线通信通道或近场通信通道; 例如，可以包括 WIFI 局域网、蓝牙、zigbee 或 NFC 等中的一种。

在本申请的实施方式中，一个智能门锁可以对应多个移动终端，用户可以通过多个移动终端的任意一个实现对智能门锁的控制。如一个智能门锁与 3 个移动终端绑定，则每个移动终端各安装一智能门锁的 APP，每个 APP 可以对应一个账户，则智能门锁和安设有智能门锁 APP 的移动终端经智能门锁和移动终端授权触发的通信通道，例如智能门锁和移动终端设置的智能门锁 APP 均经授权进入配置模式，则触发通过短距离无线通信通道或近场通信通道分别交换一个独立的加密密钥; 这里的加密密钥用于对待传输数据进行加密。这里的移动终端包括但不限于: 智能手机，平板电脑（IPAD），智能手表或预设有智能门锁 APP 的手环、小型控制器等; 所述智能门锁和移动终端可根据设置需要配置通信模块。例如安设有智能门锁 APP 的手机 A 开启蓝牙模块，所述智能门锁也开启蓝牙模块，通过蓝牙通信交换预生成的加密密钥。由于加密密钥的生成和交换均在移动终端和智能门锁本地通过短距离无线通信或近场通信通道完成，则服务器中包含任何相关密钥，服务器也无法理解由其转发的数据，保证了数据的安全性。

步骤 S103: 发送端根据操作指令或预设规则生成待传输数据，对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据; 所述发送端为智能门锁或终端。

具体的，智能门锁和移动终端内置有相同的加密算法，在有些情况下，还内置有与加密算法相对应的逆算法，如此，可以在智能门锁和移动终端本地进行加密和解密，实现端到端的数据加密的通信方式，降低信息泄露的风险。其中，移动终端内置加密算法，可以通过移动终端预装的智能门锁 APP 中实现。

在本申请的实施例中，发送端可以为智能门锁或移动终端中的一个; 当移动终端为发送端时，智能门锁可以为接收端，当智能门锁为发送端时，移动终端可以为接收端，发送端和接收端可以根据需求进行设置，本实施例对此不作限定。发送端可以根据操作指令或预设规则生成待传输数据，通过加密密钥采用预设的加密算法进行加密处理得到加密数据。其中，操作指令为请求数据或

请求执行设定动作的指令，作为本申请的一些示例，操作指令可以为请求下发开锁密码、请求蓝牙密钥、远程开锁、删除密码等指令，预设规则可以理解为预先设定的规则，例如预设的时间规则，如每次开锁时，每 12h 等等。待传输数据即为需要在智能门锁与移动终端之间安全传输的数据。在本实施例中，待传输数据可以为智能门锁密码，蓝牙钥匙，开锁记录，历史记录，传感器状态等。

而上述待传输数据一般具有敏感性，对传输的安全性要求较高，因此，可以通过加密密钥采用预设的加密算法进行加密处理，得到加密数据，如此，可以将待传输数据以密文的形式在智能门锁和移动终端之间进行传输。

例如访客 A 希望现在能够开锁进入屋内，则用户可在移动终端通过预装的智能门锁 APP 经云服务器向智能门锁下发开锁密码，则移动终端作为发送端，而智能门锁作为接收端，则移动终端将开锁密码作为待传输数据，将待传输数据按照预设的加密算法进行加密处理即得到加密数据。

或者，移动终端通过预装的智能门锁 APP 经云服务器向智能门锁发出下发开锁钥匙的请求，则移动终端作为接收端，而智能门锁作为发送端，当智能门锁接收到移动终端发送的请求蓝牙钥匙等指令时，则根据操作指令生成对应的蓝牙钥匙作为待传输数据，将待传输数据按照预设的加密算法进行加密处理即得到加密数据。

又例如移动终端可以通过内置的智能门锁 APP 向智能门锁发出操作指令等，则移动终端作为发送端，智能门锁作为接收端；例如移动终端的操作指令为控制添加密码、蓝牙密钥等；远程开锁；删除密码、蓝牙密钥、指纹等，则将该操作指令作为待发送数据并根据预设的加密算法进行加密得到加密数据。

在本申请中的另一个实施例为，智能门锁作为发送端，按照用户的预设规则（例如每 12h 发送一次或每次开门后上传、定时补传等）向指定的移动终端发送指定的数据（例如开锁记录，历史记录、门上的传感器状态，甚至家中是否有人的情况等）；即智能门锁作为发送端按照预设的加密算法对准备发送的开锁记录进行加密处理即得到加密数据，按照预设规则（例如每 12h 发送一次或每次开门后上传、定时补传等）将开锁记录处理形成加密数据。

步骤 S104：所述发送端为加密数据配置唯一标识得到带有唯一标识的加密数据。

具体的是发送端将加密数据配置唯一标识得到带有唯一标识的加密数据，

该唯一标识用于表征发送端的身份，在身份验证中进行标识匹配，所述唯一标识例如可以是发送端的 MAC 地址，IP 地址，特定标签，用户名或用户 ID 等等。

步骤 S105：所述发送端将带有唯一标识的加密数发送至接收端。

在本实施例中，发送端可以将带有唯一标识的加密数据通过所述预设通信通道或云服务器发送至接收端；这里的预设通信通道为短距离无线通信通道或近场通信信道，包括但不限于 WIFI 局域网、蓝牙、zigbee 或近场通信（NFC）中的一种。其中，通过预设通信通道可以实现本地控制，通过云服务器可以实现远程控制。

例如：访客 A 希望现在能够开锁进入屋内，则用户可在移动终端通过预装的智能门锁 APP 经云服务器向智能门锁下发开锁密码，则移动终端作为发送端，而智能门锁作为接收端，则移动终端将开锁密码作为待传输数据，将待传输数据按照预设的加密算法进行加密处理即得到加密数据，并为该加密数据配置唯一标识后通过云服务器或预设通信通道发送给智能门锁。

在本申请中的另一个实施例为，智能门锁作为发送端，按照用户的预设规则（例如每 12h 发送一次）向指定的移动终端发送指定的数据（例如开锁记录）；即智能门锁作为发送端按照预设的加密算法对准备发送的开锁记录进行加密处理即得到加密数据，按照预设规则（例如每 12h）将开锁记录处理形成加密数据并配置唯一标识后通过云服务器或预设通信通道发送移动终端。

步骤 S106：所述接收端对带有唯一标识的加密数据进行身份验证；

具体的所述接收端对带有唯一标识的加密数据进行身份验证包括：

步骤 S1061：所述接收端提取所述带有唯一标识的加密数据中的唯一标识；

移动终端或者智能门锁作为接收端，对带有唯一标识的加密数据进行提取，得到其携带的唯一标识；例如发送端发送的带有唯一标识的加密数据，则接收端提取其唯一标识（例如提取到的唯一标识可以是发送端的 MAC 地址，IP 地址，特定标签，用户名或用户 ID 等等。）

步骤 S1062：根据所述唯一标识分析得到与该唯一标识匹配的加密密钥；

根据提取到的唯一标识进行匹配得到该唯一标识对应的加密密钥；其中移动终端或智能门锁端均保存有唯一标识与加密密钥的对应关系，可根据唯一标识匹配得到该标识对应的加密密钥；例如，可以在移动终端和智能门锁端均保

存有唯一标识和加密密钥的对应关系表；当根据唯一标识进行匹配查找时，即可得到其对应的加密密钥。

步骤 S1063：根据所述加密密钥确定身份验证结果。

具体的，根据匹配得到的加密密钥验证是否与接收端内存在的加密密钥相同或对应匹配，如相同或对应匹配，则身份验证结果为确认是绑定的发送端发来的加密数据。如不相同或不匹配，则身份验证结果为确认是非绑定的发送端发来的。本申请增加身份验证步骤以进一步保证通信安全。

步骤 S107：所述接收端根据身份验证结果，利用交换得到的加密密钥对加密数据进行解密处理。

具体的，当身份验证结果为匹配，也即确认是与接收端绑定的发送端发来的加密数据，则利用交换得到的加密密钥对加密数据进行解密处理，得到待传输数据；当身份验证结果为不匹配，也即确认是非绑定的发送端发来的，则不作解密，还可以进一步生成报警信息。

其中，本申请的方法还包括：

步骤 S101：响应于用户的授权操作指令，所述智能门锁或所述移动终端生成初始加密密钥，所述智能门锁和所述移动终端对所述初始加密密钥进行认证得到加密密钥。

其中，初始加密密钥可以为智能门锁或移动终端自动生成或手动输入的密钥；在生成初始加密密钥后，可以通过安全通信信道传输初始加密密钥，如此，智能门锁和移动终端均获得初始加密密钥，智能门锁和移动终端可以对初始加密密钥进行认证得到加密密钥。

具体的，用户的授权操作指令例如可以是用户手动按下配置按钮或配置模式触摸键或在智能门锁本地输入已设定的管理员密码或输入管理员权限的指纹等（相当于智能门锁开启配置模式），用户在终端开启 APP 进入配置模式，通过配置模式经用户授权确认开启安全通信通道；智能门锁和移动终端可采用 WIFI 局域网、蓝牙、zigbee 或近场通信（NFC）中的一种作为安全通信通道连接，则可由任意一方生成初始加密密钥经过相互认证后得到加密密钥。例如：用户在智能门锁端按下启动配置按钮，并输入已认证的管理员密码，同时用户在手机端打开智能门锁的 APP 进入配置模式，智能门锁和手机经用户授权确认通过蓝牙通信连接，可以由智能门锁生成初始加密密钥，通过蓝牙通信通道发送至手机 APP，手机 APP 进行确认或对初始加密密钥进行修改后与智能门

锁进行交换；或智能门锁和手机 APP 分别生成一对公钥和私钥并进行交换。

在上述实施例中，对待传输数据进行加密可以有多种实现方式，例如，可以采用对称加密的方式，也可采用非对称加密的方式进行加密。下面结合具体实施例对不同加密方式的加密、解密过程进行详细说明。

可选地，如图 3 所示，所述加密密钥为第一加密密钥；所述步骤 S103 对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括：

步骤 S1031a：通过第一加密密钥采用对称加密算法对待传输数据进行加密得到初始加密数据。

具体的，所述第一加密密钥为分别保存在智能门锁和移动终端的加密密钥；例如有 2 个移动终端与智能门锁绑定，则移动终端 A 与智能门锁保存有相同的加密密钥（例如可以为 KeyA）；移动终端 B 与智能门锁保存有相同的加密密钥（例如可以为 KeyB）。其中一种实施方式为：当移动终端 A 作为发送端时，则将生成的待传输数据采用加密密钥 KeyA 通过对称加密算法进行加密得到初始加密数据 A。其中另一种实施方式为，智能门锁作为发送端，其根据移动终端 B 发来的操作指令生成待传输数据，则将该待传输数据采用加密密钥 KeyB 通过对称加密算法进行加密得到初始加密数据 B。

步骤 S1032a：为初始加密数据配置预设密钥值；

具体的为上述步骤得到的初始加密数据配置预设的密钥值，所述预设密钥值为当前时间戳 timestamp、计数器 count 值和随机码中的至少一种；例如当前时间为 2016-08-11-20：21，则将此作为预设的密钥值配置到初始加密数据中。

步骤 S1033a：为配置有预设密钥值的初始加密数据添加验证签名得到加密数据。

具体的签名可以根据哈希算法生成哈希值作为签名，用于在解密时验证加密数据的完整性。

则可选地，如图 4 所示：所述步骤 S107 根据身份验证结果处理加密数据包括：

步骤 S1071a 若身份验证结果为验证结果匹配，则所述接收端对加密数据的验证签名进行验证；

具体的接收端校验签名的完整性，防止被篡改，保证数据的完整性。

步骤 S1072a 若验证签名匹配，则验证预设密钥值是否合法；

具体的若验证签名匹配，则接收端分析带有预设密钥值的验证预设密钥值例如时间戳 timestamp、计数器 count 值或随机码是否合法；具体的是将预设密钥值与接收端本地当前的数据或保存的数据或生成的数据做比对。其中一个实施例为：当智能门锁作为接收端时，所述智能门锁将时间戳与智能门锁内的时钟模块保存的时间做对比；所述时钟模块内部用纽扣电池长期供电的时钟芯片，例如智能门锁使用 5 号干电池供电，即使更换 5 号电池前后，门锁内部的时钟依然保持，时钟模块中的时间为自动匹配更新的标准时间；例如现在时间为 17：00，则时钟模块的时间也为 17:00。

所述智能锁将时间戳与智能门锁内的时钟模块保存的时间做对比，如果偏差即加密数据带有的时间戳与时钟模块保存的时间的差值超过限定阈值，则判断所述加密数据是非法的数据包，将验证结果通过蓝牙或 zigbee 等反馈至所述移动终端；一般设定阈值可根据情况设定在 15min～60min 内，例如设定限定阈值为 20min；则如果偏差超过 20min，则判断所述加密数据是非法的数据包，则检查结果为所述带有预设的密钥值的加密数据不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述移动终端。

如果偏差未超过限定阈值，则检查结果为所述带有预设的密钥值的加密数据合法。同样的，当所述移动终端作为接收端时，则与移动终端的当前时间值进行比较验证，在此不再赘述。

其中另一个实施例为：所述预设的密钥值为计数器值。则当所述智能门锁作为接收端时，所述智能门锁将所述带有预设的密钥值的加密数据带有的计数器 count 值与本地保存的计数器 count 值比较；

如果所述加密数据带有的计数器值大于本地保存的值，则检查结果为所述带有计数器 count 值的开锁验证码合法；如果所述智能门锁发送的计数器值小于等于本地保存的值，则认为是数据包被重新播放，则检查结果为所述带有计数器值的加密数据为不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述移动终端。移动终端作为接收端方式相同，在此不做赘述。

步骤 S1073a 若预设密钥值合法，则接收端通过第一加密密钥采用相同所述对称加密算法的逆算法对初始加密数据进行解密得到待传输数据。

具体地，经接收端验证配置有预设密钥值的初始加密数据的预设密钥值的合法性，若预设密钥值合法，则接收端通过本地保存的第一加密密钥采用相同

所述对称加密算法的逆算法对初始加密数据进行解密得到待传输数据。；例如本地保存的相同第一加密密钥为 KeyA，则采用 KeyA 通过相同对称加密算法的逆算法对初始加密数据进行解密得到待传输数据。

可选地，所述加密密钥包括一公开密钥和一私有密钥；所述步骤 S103 对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括:

步骤 S1031b: 发送端通过自身保存的所述公开密钥采用非对称加密算法对待传输数据进行加密得到初始加密数据;

具体的，所述发送端和接收端分别保存的加密密钥包括一公开密钥和一私有密钥，如发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。例如智能门锁作为发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则移动终端作为接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。则智能门锁作为发送端通过其保存的公开密钥 pub B 采用非对称加密算法对待传输数据进行加密得到初始加密数据。

步骤 S1032b: 为初始加密数据配置预设密钥值；所述预设密钥值为当前时间戳、计数器值和随机码中的至少一种;

具体的为上述步骤的到的初始加密数据配置预设的密钥值，所述预设密钥值为当前时间戳 timestamp、计数器 count 值和随机码中的至少一种；例如当前时间为 2016-08-11-20: 21，则将此作为预设的密钥值配置到初始加密数据中。

步骤 S1033b: 为配置有预设密钥值的初始加密数据添加发送端保存的所述私有密钥作为验证签名得到加密数据。

具体的，如上所述如发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。例如智能门锁作为发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则移动终端作为接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。举例说明，智能门锁作为发送端，则为配有有预设密钥值的初始加密数据添加智能门锁本地保存的私有密钥 pri A 作为验证签名得到加密数据。

则可选地，所述步骤 S107 根据身份验证结果处理加密数据包括:

步骤 S1071b: 若身份验证结果为验证结果匹配，则所述接收端采用自身

存储的公开密钥对加密数据的验证签名进行验证;

具体的，若身份验证结果为验证结果匹配，则所述接收端采用本地存储的公开密钥对加密数据的验证签名进行验证。例如接收端是移动终端，如前所述移动终端本地存储的加密密钥为私有密钥 pri B 和公开密钥 pubA。则移动终端采用本地存储的 pub A 对加密数据中携带的签名 pri A 进行验证。如经验证其为与本地存储的公开密钥 pub A 对应的私有密钥 pri A，则验证签名匹配，若非本地存储的公开密钥 pub A 对应的私有密钥，则验证签名结果为不匹配。

步骤 S1072b: 若验证签名匹配，则验证预设密钥值是否合法;

具体的若验证签名匹配，则接收端分析带有预设密钥值的验证预设密钥值例如时间戳 timestamp、计数器 count 值或随机码是否合法; 具体的是将预设密钥值与接收端本地当前的数据或保存的数据或生成的数据做比对。其中一个实施例为: 当智能门锁作为接收端时，所述智能门锁将时间戳与智能门锁内的时钟模块保存的时间做对比; 所述时钟模块内部用纽扣电池长期供电的时钟芯片，例如智能门锁使用 5 号干电池供电，即使更换 5 号电池前后，门锁内部的时钟依然保持，时钟模块中的时间为自动匹配更新的标准时间; 例如现在时间为 17: 00，则时钟模块的时间也为 17:00。

所述智能锁将时间戳与智能门锁内的时钟模块保存的时间做对比，如果偏差即加密数据带有的时间戳与时钟模块保存的时间的差值超过限定阈值，则判断所述加密数据是非法的数据包，将验证结果通过蓝牙或 zigbee 等反馈至所述移动终端; 一般设定阈值可根据情况设定在 15min ~ 60min 内，例如设定限定阈值为 20min; 则如果偏差超过 20min，则判断所述加密数据是非法的数据包，则检查结果为所述带有预设的密钥值的加密数据不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述移动终端。

如果偏差未超过限定阈值，则检查结果为所述带有预设的密钥值的加密数据合法。同样的，当所述移动终端作为接收端时，则与移动终端的当前时间值进行比较验证，在此不再赘述。

其中另一个实施例为: 所述预设的密钥值为计数器值。则当所述智能门锁作为接收端时，所述智能门锁将所述带有预设的密钥值的加密数据带有的计数器 count 值与本地保存的计数器 count 值比较;

如果所述加密数据带有的计数器值大于本地保存的值，则检查结果为所述带有计数器 count 值的开锁验证码合法; 如果所述智能门锁发送的计数器值小

于等于本地保存的值，则认为是数据包被重新播放，则检查结果为所述带有计数器值的加密数据为不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述移动终端。移动终端作为接收端方式相同，在此不做赘述。

步骤 S1073b：若预设密钥值合法，则接收端通过自身存储的私有密钥采用相同所述非对称加密算法对初始加密数据进行解密得到待传输数据。

由于待传输的数据加密，以及为防止被重新播放而加入预设的密钥值，以及为防止不法人员对数据进行篡改而配置的签名以保证数据完整性等都是在本地完成，则可以保证服务器端或者智能门锁厂家的内部工作人员亦无法从服务器端获得用户的传输信息，保证即使服务器被攻破，门锁与手机客户端的通信中的身份验证、防重放、防篡改依然有效，进一步保证了用户信息的安全性。

步骤 S1071a-S1073a 和步骤 S1071b-S1073b 为接收端对加密数据进行解密的一些具体实施方式，在本申请实施例一些可能的实现方式中，接收端接收发送端发送的带有唯一标识的加密数据，然后对所述带有唯一标识的加密数据进行身份验证，得到身份验证结果，接收端可以根据身份验证结果，利用交换得到的加密密钥对加密数据进行解密处理得到待传输数据。根据加密数据的加密方式不同，对加密数据进行解密的方式可以是不同的，本申请实施例对此不作限定。

在有些情况下，如用户丢失了移动终端时，还可以通过登陆备用移动终端，发起授权删除操作，指示智能门锁和/或云服务器删除相关加密密钥信息，防止丢失的移动终端中加密密钥信息泄露，减小安全隐患。

可选地，所述基于智能门锁系统的安全通信方法还包括：

步骤 1081：备用移动终端获取账户登录验证信息，所述账户登录验证信息为用于验证用户身份的信息；所述备用移动终端为所述移动终端的备用设备。

本申请的一个实施例为，当用户丢失预设有 APP 并保存有加密密钥的移动终端时，则用户可以通过设有智能门锁 APP 的备用移动终端，输入账户登陆验证信息实现账户登录，其中，账户登录验证信息包括但不限于：用户身份信息（用户名，用户 ID 等用户按照规则自行设定的用户身份标识信息），密码和验证码等。

步骤 1082：若所述账户登录验证信息通过，则所述备用移动终端响应于用户的授权删除操作，向智能门锁发出第一删除指令，用于指示所述智能门锁

删除本地保存的指定加密密钥信息；和/或，所述备用移动终端响应于用户的远程授权删除操作，向云服务器发出第二删除指令，用于指示所述云服务器删除所述移动终端保存的加密密钥信息。

具体的，用户通过账户登陆认证后，可与智能门锁通过短距离无线通信或近场通信的连接方式连接，配合操作智能门锁端删除与该账户匹配的原加密密钥信息；同时也可通过云服务器执行丢失移动终端中保存的加密密钥的删除操作。

以上为为本申请实施例提供的一种安全通信方法的具体实现方式，为了便于理解，下面结合具体场景对本申请实施例进行介绍。其中，实施例 1 为移动终端作为发送端，向智能门锁发送开锁密码实现开锁的应用场景实施例，实施例 2 为智能门锁作为发送端，按照预设规则向指定移动终端发送开锁记录、传感器状态等数据的应用场景实施例，接下来对其实现过程进行详细说明。

场景实施例 1:

一种基于智能门锁系统的安全通信方法，包括如下步骤:

（1）响应于用户的授权操作指令，所述智能门锁和移动终端分别开启安全通信通道，所述安全通信通道为经智能门锁和移动终端授权触发的通信通道;

所述智能门锁或移动终端生成初始加密密钥进行认证得到加密密钥；所述初始加密密钥为智能门锁或移动终端自动生成或手动输入的密钥。

具体的，用户的授权操作指令例如可以是用户手动按下配置按钮或配置模式触摸键或在智能门锁本地输入已设定的管理员密码或输入管理员权限的指纹等（相当于智能门锁开启配置模式），用户在终端开启 APP 进入配置模式，通过配置模式经用户授权确认开启安全通信通道；智能门锁和移动终端可采用 WIFI 局域网、蓝牙、zigbee 或近场通信（NFC）中的一种作为安全通信通道连接，则可由任意一方生成初始加密密钥经过相互认证后得到加密密钥。例如：用户在智能门锁端按下启动配置按钮，并输入已认证的管理员密码，同时用户在手机端打开智能门锁的 APP 进入配置模式，智能门锁和手机经用户授权确认通过蓝牙通信连接，可以由智能门锁生成初始加密密钥，通过蓝牙通信通道发送至手机 app，手机 app 进行确认或对初始加密密钥进行修改后与智能门锁进行交换；或智能门锁和手机 APP 分别生成一对公钥和私钥并进行交换

（2）所述智能门锁和移动终端开启蓝牙通信，智能门锁与移动终端预设

的智能门锁 APP 通过蓝牙连接并交换加密密钥;

（3）当移动终端作为发送端根据移动终端预设的智能门锁 APP 的开锁密码生成待传输数据;对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据; 具体的，在智能门锁和移动终端预装的智能门锁 APP 中内置有相同的加密密钥 key A 以及相同的对称加密算法。则移动终端作为发送端，而智能门锁作为接收端，则移动终端将开锁密码作为待传输数据，则将该待传输数据采用加密密钥 KeyA 通过对称加密算法进行加密得到初始加密数据 A; 对初始加密数据 A 配置当前时间戳作为预设的密钥值得到配置有预设密钥值的初始加密数据 A; 为配置有预设密钥值的初始加密数据添加验证签名得到加密数据。

（4）移动终端将加密数据配置唯一标识得到带有唯一标识的加密数据，唯一标识可以是移动终端预设有智能门锁 APP 的用户 ID。

（5）移动终端将带有唯一标识的加密数据通过云服务器发送至智能门锁。

（6）接收数据的智能门锁对带有唯一标识的加密数据进行身份验证。具体的，可以是智能门锁作为接收端，对带有唯一标识的加密数据进行提取其携带的唯一标识; 例如发送端发送的带有唯一标识的加密数据，则提取其唯一标识（例如提取到的唯一标识可以是发送端的 MAC 地址，IP 地址，特定标签，用户名或用户 ID 等等。); 根据提取到的唯一标识进行匹配得到该唯一标识对应的加密密钥; 其中移动终端或智能门锁端均保存有唯一标识与加密密钥的对应关系，可根据唯一标识匹配得到该标识对应的加密密钥; 例如，可以在移动终端和智能门锁端均保存有唯一标识和加密密钥的对应关系表; 当根据唯一标识进行匹配查找时，即可得到其对应的加密密钥。根据所述与该唯一标识匹配的加密密钥确定身份验证结果。具体的根据匹配得到的加密密钥验证是否与接收端内存在的加密密钥相同或对应匹配，如相同或对应匹配，则身份验证结果为确认是绑定的发送端发来的加密数据。如不相同或不匹配，则身份验证结果为确认是非绑定的发送端发来的。本申请增加身份验证步骤以进一步保证通信安全。

（7）若身份验证结果为验证结果匹配，则所述接收端对加密数据的验证签名进行验证; 具体的接收端校验签名的完整性，防止被篡改，保证数据的完整性。具体的若验证签名匹配，则所述智能门锁将时间戳与智能门锁内的时钟模块保存的时间做对比; 所述时钟模块内部用纽扣电池长期供电的时钟芯片，

例如智能门锁使用 5 号干电池供电，即使更换 5 号电池前后，门锁内部的时钟依然保持，时钟模块中的时间为自动匹配更新的标准时间；例如现在时间为 17：00，则时钟模块的时间也为 17:00。

所述智能锁将时间戳与智能门锁内的时钟模块保存的时间做对比，如果偏差即加密数据带有的时间戳与时钟模块保存的时间的差值超过限定阈值，则判断所述加密数据是非法的数据包，将验证结果通过蓝牙或 zigbee 等反馈至所述移动终端；一般设定阈值可根据情况设定在 15min～60min 内，例如设定限定阈值为 20min；则如果偏差超过 20min，则判断所述加密数据是非法的数据包，则检查结果为所述带有预设的密钥值的加密数据不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述移动终端。

如果偏差未超过限定阈值，则检查结果为所述带有预设的密钥值的加密数据合法。若预设密钥值合法，则智能门锁采用本地保存的相同第一加密密钥为 KeyA 通过相同对称加密算法的逆算法对初始加密数据进行解密得到待传输数据。

场景实施例 2

一种基于智能门锁系统的安全通信方法，包括如下步骤：

（1）响应于用户的授权操作指令，所述智能门锁和移动终端分别开启安全通信通道，所述安全通信通道为经智能门锁和移动终端授权触发的通信通道；

所述智能门锁或移动终端生成初始加密密钥进行认证得到加密密钥；所述初始加密密钥为智能门锁或移动终端自动生成或手动输入的密钥。

具体的，用户的授权操作指令例如可以是用户手动按下配置按钮或配置模式触摸键或在智能门锁本地输入已设定的管理员密码或输入管理员权限的指纹等（相当于智能门锁开启配置模式），用户在终端开启 APP 进入配置模式，通过配置模式经用户授权确认开启安全通信通道；智能门锁和移动终端可采用 WIFI 局域网、蓝牙、zigbee 或近场通信（NFC）中的一种作为安全通信通道连接，则可由任意一方生成初始加密密钥经过相互认证后得到加密密钥。例如：用户在智能门锁端按下启动配置按钮，并输入已认证的管理员密码，同时用户在手机端打开智能门锁的 APP 进入配置模式，智能门锁和手机经用户授权确认通过 NFC 通信连接，智能门锁和手机 APP 分别生成一对公钥和私钥并通过 NFC 通信进行交换。

（2）智能门锁与移动终端预设的智能门锁 APP 通过 NFC 连接并交换加密密钥；

（3）当智能门锁作为发送端，例如按照用户的预设规则（例如每 12h 发送一次或每次开门后上传、定时补传等）向指定的移动终端发送指定的数据（例如开锁记录，历史记录、门上的传感器状态，甚至家中是否有人的情况等）；即智能门锁作为发送端按照预设的加密算法对准备发送的开锁记录进行加密处理即得到加密数据。对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据；具体的，智能门锁作为发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B 和非对称加密算法；则移动终端作为接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA 及相同的非对称加密算法。则智能门锁作为发送端通过其保存的公开密钥 pub B 采用非对称加密算法对待传输数据进行加密得到初始加密数据；对初始加密数据配置计数器值作为预设的密钥值得到配置有预设密钥值的初始加密数据；为配置有预设密钥值的初始加密数据添加私有密钥做为验证签名得到加密数据。具体的，如上所述如发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。例如智能门锁作为发送端保存的加密密钥为私有密钥 pri A 和公开密钥 pub B；则移动终端作为接收端对应保存的加密密钥为私有密钥 pri B 和公开密钥 pubA。则这里例如智能门锁作为发送端，则为配有预设密钥值的初始加密数据添加智能门锁本地保存的私有密钥 pri A 作为验证签名得到加密数据。

（4）智能门锁将加密数据配置唯一标识得到带有唯一标识的加密数据，唯一标识可以是智能门锁的 MAC 地址。

（5）智能门锁将带有唯一标识的加密数据通过云服务器发送至移动终端。

（6）接收数据的移动终端对带有唯一标识的加密数据进行身份验证。具体的，可以是智能门锁作为接收端，对带有唯一标识的加密数据进行提取其携带的唯一标识；例如发送端发送的带有唯一标识的加密数据，则提取其唯一标识（例如提取到的唯一标识可以是发送端的 MAC 地址，IP 地址，特定标签，用户名或用户 ID 等等。）；根据提取到的唯一标识进行匹配得到该唯一标识对应的加密密钥；其中移动终端或智能门锁端均保存有唯一标识与加密密钥的对应关系，可根据唯一标识匹配得到该标识对应的加密密钥；例如，可以在移动终端和智能门锁端均保存有唯一标识和加密密钥的对应关系表；当根据唯一标

识进行匹配查找时，即可得到其对应的加密密钥。根据所述与该唯一标识匹配的加密密钥确定身份验证结果。具体的根据匹配得到的加密密钥验证是否与接收端内存在的加密密钥相同或对应匹配，如相同或对应匹配，则身份验证结果为确认是绑定的发送端发来的加密数据。如不相同或不匹配，则身份验证结果为确认是非绑定的发送端发来的。本申请增加身份验证步骤以进一步保证通信安全。

（7）若身份验证结果为验证结果匹配，则所述接收端采用存储的公开密钥对加密数据的验证签名进行验证。具体的，若身份验证结果为验证结果匹配，则所述接收端采用本地存储的公开密钥对加密数据的验证签名进行验证。例如接收端是移动终端，如前所述移动终端本地存储的加密密钥为私有密钥 pri B 和公开密钥 pubA。则移动终端采用本地存储的 pub A 对加密数据中携带的签名 pri A 进行验证。如经验证其为与本地存储的公开密钥 pub A 对应的私有密钥 pri A，则验证签名匹配，若非本地存储的公开密钥 pub A 对应的私有密钥，则验证签名结果为不匹配。若验证签名匹配，则当所述移动终端作为接收端时，所述移动终端将所述带有预设的密钥值的加密数据带有的计数器 count 值与本地保存的计数器 count 值比较；

如果所述加密数据带有的计数器值大于本地保存的值，则检查结果为所述带有计数器 count 值的开锁验证码合法；如果所述智能门锁发送的计数器值小于等于本地保存的值，则认为是数据包被重新播放，则检查结果为所述带有计数器值的加密数据为不合法，并将验证结果通过预设的通信通道或云服务器传输反馈给所述智能门锁并生成预警信息。若预设密钥值合法，则接收端通过存储的私有密钥采用相同所述非对称加密算法对初始加密数据进行解密得到待传输数据。上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

在本申请的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，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，可以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，单元或模块的间接耦合或通信连接，可以是电性或其

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。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

以上所述仅是本申请的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

权 利 要 求

1、一种安全通信方法，其特征在于，所述方法应用于智能门锁系统，所述智能门锁系统包括智能门锁和移动终端，所述方法包括:

发送端根据操作指令或预设规则生成待传输数据，并对所述待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据；所述发送端为所述智能门锁或所述移动终端；所述加密密钥为所述智能门锁与所述移动终端通过预设的安全通信通道连接并交换得到；所述安全通信通道为经所述智能门锁和所述移动终端授权触发的短距离无线通信通道或近场通信通道；

所述发送端为所述加密数据配置唯一标识得到带有唯一标识的加密数据；

所述发送端将所述带有唯一标识的加密数据发送至接收端，以便所述接收端对所述带有唯一标识的加密数据进行身份验证，并根据身份验证结果，利用交换得到的加密密钥对所述加密数据进行解密处理；

其中，所述发送端为智能门锁时，所述接收端为移动终端；所述发送端为移动终端时，所述接收端为智能门锁。

2、根据权利要求 1 所述的方法，其特征在于，所述发送端将所述带有唯一标识的加密数据发送至接收端包括:

所述发送端将所述带有唯一标识的加密数据通过预设通信通道或云服务器发送至接收端；所述预设通信通道为短距离无线通信或近场通信信道。

3、根据权利要求 1 所述的方法，其特征在于，所述加密密钥为所述智能门锁或所述移动终端响应于用户的授权操作指令，生成初始加密密钥，并由所述智能门锁和所述移动终端对所述初始加密密钥进行认证得到；其中，所述初始加密密钥为所述智能门锁或所述移动终端自动生成或手动输入的密钥；所述初始加密密钥通过所述安全通信通道在所述智能门锁和所述移动终端之间进行传输。

4、根据权利要求 1 所述的方法，其特征在于，所述加密密钥为第一加密密钥；所述对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括:

通过所述第一加密密钥采用对称加密算法对待传输数据进行加密得到初始加密数据；

为所述初始加密数据配置预设密钥值；所述预设密钥值为当前时间戳、计数器值和随机码中的至少一种；

为配置有所述预设密钥值的初始加密数据添加验证签名得到加密数据。

5、根据权利要求 1 所述的方法，其特征在于，所述发送端和接收端分别保存的加密密钥包括一公开密钥和一私有密钥；所述对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据包括：

发送端通过自身保存的所述公开密钥采用非对称加密算法对待传输数据进行加密得到初始加密数据；

为所述初始加密数据配置预设密钥值；所述预设密钥值为当前时间戳、计数器值和随机码中的至少一种；

为配置有所述预设密钥值的初始加密数据添加发送端保存的所述私有密钥作为验证签名得到加密数据。

6、根据权利要求 1-5 任意一项所述的方法，其特征在于，所述方法还包括：

备用移动终端获取账户登录验证信息，所述账户登录验证信息为用于验证用户身份的信息；所述备用移动终端为所述移动终端的备用设备；

若所述账户登录验证信息通过，则所述备用移动终端响应于用户的授权删除操作，向智能门锁发出第一删除指令，用于指示所述智能门锁删除本地保存的指定加密密钥信息；和/或，所述备用移动终端响应于用户的远程授权删除操作，向云服务器发出第二删除指令，用于指示所述云服务器删除所述移动终端保存的加密密钥信息。

7、一种安全通信方法，其特征在于，所述方法应用于智能门锁系统，所述智能门锁系统包括智能门锁和移动终端，所述方法包括：

所述接收端接收所述发送端发送的带有唯一标识的加密数据；所述发送端为智能门锁时，所述接收端为移动终端；所述发送端为移动终端时，所述接收端为智能门锁；所述带有唯一标识的加密数据为所述发送端根据操作指令或预设规则生成待传输数据，并对所述待传输数据通过加密密钥采用预设的加密算法进行加密，并配置唯一标识得到；所述加密密钥为所述智能门锁与所述移动终端通过预设的安全通信通道连接并交换得到；所述安全通信通道为经所述智能门锁和所述移动终端授权触发的短距离无线通信通道或近场通信通道；

所述接收端对所述带有唯一标识的加密数据进行身份验证，得到身份验证结果；

所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述

加密数据进行解密处理得到所述待传输数据。

8、根据权利要求 7 所述的方法，其特征在于，所述加密密钥为第一加密密钥，所述加密数据为所述发送端通过所述第一加密密钥采用对称加密算法对所述待传输数据进行加密得到初始加密数据，为所述初始加密数据配置预设密钥值，为配置有所述预设密钥值的初始加密数据添加验证签名得到；

则所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述加密数据进行解密处理得到所述待传输数据包括：

若所述身份验证结果匹配，则所述接收端对所述加密数据的所述验证签名进行验证；

若所述验证签名匹配，则验证所述预设密钥值是否合法；

若所述预设密钥值合法，则所述接收端从所述加密数据中获取所述初始加密数据，并通过所述第一加密密钥采用所述对称加密算法的逆算法对所述初始加密数据进行解密得到所述待传输数据。

9、根据权利要求 7 所述的方法，其特征在于，所述发送端和所述接收端分别保存的加密密钥包括一公开密钥和一私有密钥；所述加密数据为所述发送端通过自身保存的所述公开密钥采用非对称加密算法对所述待传输数据进行加密得到初始加密数据，为所述初始加密数据配置预设密钥值，为配置有所述预设密钥值的初始加密数据添加所述发送端保存的所述私有密钥作为验证签名得到；

则所述接收端根据所述身份验证结果，利用交换得到的所述加密密钥对所述加密数据进行解密处理得到所述待传输数据包括：

若所述身份验证结果为匹配，则所述接收端采用自身存储的公开密钥对所述加密数据的所述验证签名进行验证；

若所述验证签名匹配，则验证所述预设密钥值是否合法；

若所述预设密钥值合法，则所述接收端从所述加密数据中获取所述初始加密数据，并通过自身存储的所述私有密钥采用所述非对称加密算法对所述初始加密数据进行解密得到所述待传输数据。

10、根据权利要求 7 所述的安全通信方法，其特征在于，所述接收端对所述带有唯一标识的加密数据进行身份验证包括：

所述接收端提取所述带有唯一标识的加密数据中的唯一标识；

根据所述唯一标识分析得到与所述唯一标识匹配的加密密钥；

根据所述加密密钥确定身份验证结果。

11、一种智能门锁系统，其特征在于，所述智能门锁系统包括:

智能门锁，用于通过预设的加密算法，采用加密密钥对待传输数据进行加密以及对接收到的加密数据进行解密；所述智能门锁设有短距离无线通信模块;

移动终端，用于通过预设的与所述智能门锁相同的加密算法，采用所述加密密钥对所述待传输数据进行加密以及对接收到的所述加密数据进行解密；所述移动终端还用于控制所述智能门锁，所述移动终端设有短距离无线通信模块，用于和所述智能门锁通信。

12、根据权利要求 11 所述的系统，其特征在于，

所述智能门锁还包括配置模式启动模块，用于启动配置模式进行加密密钥的生成和交换，所述配置模式启动模块包括：配置按钮、配置模式触摸键、用于输入管理员密码的触摸屏或用于输入管理员权限的指纹的指纹采集器中的至少一种。

13、根据权利要求 12 所述的系统，其特征在于，所述移动终端控制所述智能门锁具体包括通过用于控制智能门锁的 APP 对所述智能门锁进行控制，所述用于控制智能门锁的 APP 内还设置有启动配置模式的虚拟按键用于启动移动终端的配置模式。

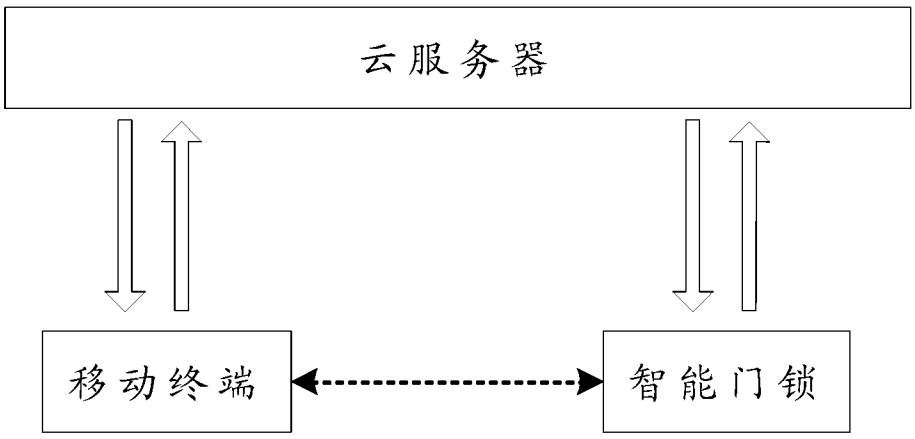

图 1

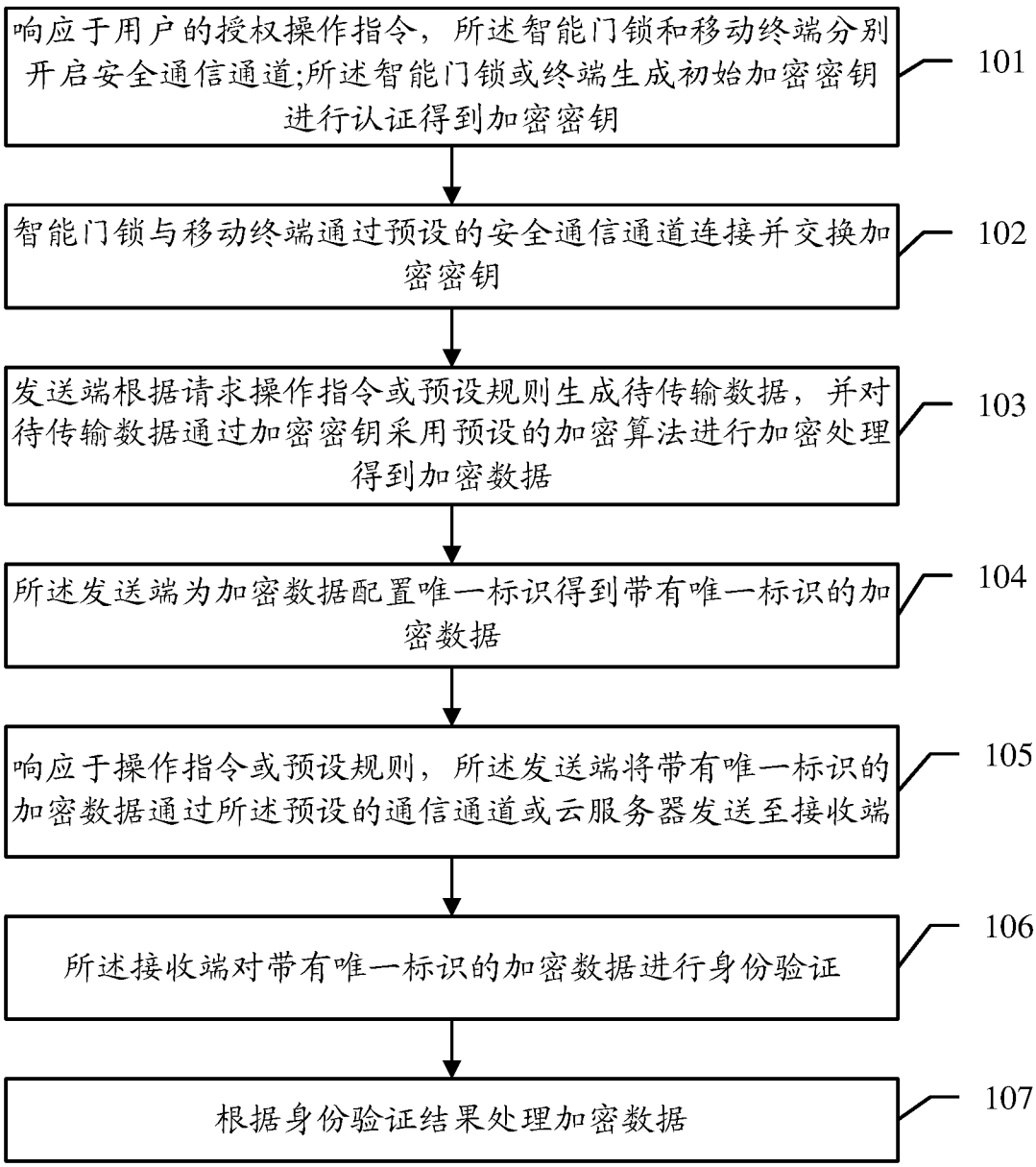
响应于用户的授权操作指令，所述智能门锁和移动终端分别开启安全通信通道;所述智能门锁或终端生成初始加密密钥进行认证得到加密密钥
101
智能门锁与移动终端通过预设的安全通信通道连接并交换加密密钥
102
发送端根据请求操作指令或预设规则生成待传输数据，并对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据
103
所述发送端为加密数据配置唯一标识得到带有唯一标识的加密数据
104
响应于操作指令或预设规则，所述发送端将带有唯一标识的加密数据通过所述预设的通信通道或云服务器发送至接收端
105
所述接收端对带有唯一标识的加密数据进行身份验证
106
根据身份验证结果处理加密数据
107

图 2

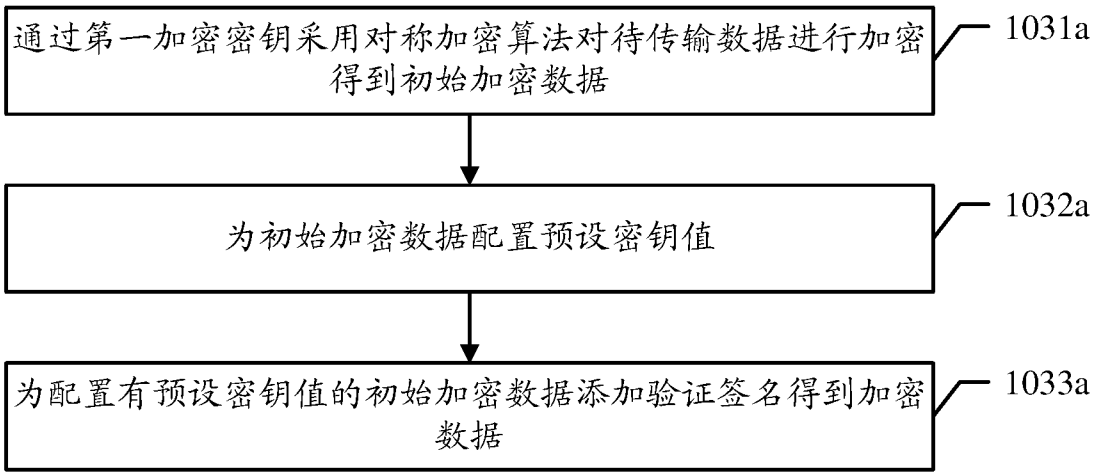
通过第一加密密钥采用对称加密算法对待传输数据进行加密得到初始加密数据
1031a
为初始加密数据配置预设密钥值
1032a
为配置有预设密钥值的初始加密数据添加验证签名得到加密数据
1033a

图 3

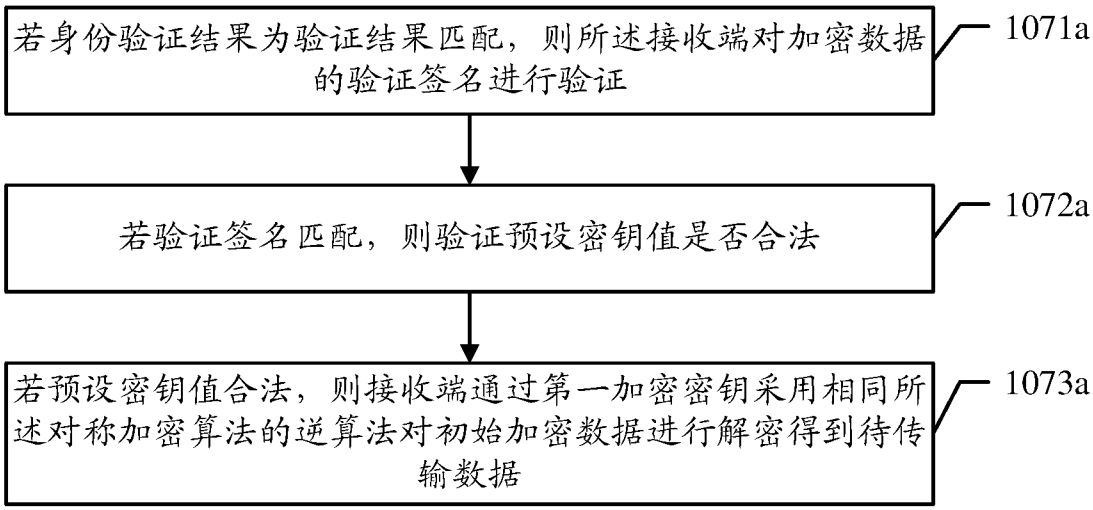
若身份验证结果为验证结果匹配，则所述接收端对加密数据的验证签名进行验证
1071a
若验证签名匹配，则验证预设密钥值是否合法
1072a
若预设密钥值合法，则接收端通过第一加密密钥采用相同所述对称加密算法的逆算法对初始加密数据进行解密得到待传输数据
1073a

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/079999

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00 (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)

G07C9

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; CNABS, VEN, CNKI: 门锁, 移动终端, 密匙, 加密, 解密, 服务器, 标识, 身份, 验证, DOOR, LOCK, MOBILE, TERMINAL, ENCRYPT+, KEY, SERVER, ALGORITHM, AUTHENT+, IDENTIFICATION

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107038777 A (YUNDING NETWORK TECHNOLOGY BEIJING CO., LTD.), 11 August 2017 (11.08.2017), entire document	1-13
X	CN 103578165 A (GAO, Chao), 12 February 2014 (12.02.2014), description, paragraphs 0014-0018, and figure 1	11-13
A	CN 106504391 A (BEIJING IJOURNEY TECHNOLOGY DEVELOPMENT CO., LTD.), 15 March 2017 (15.03.2017), entire document	1-13
A	CN 106408697 A (GUANGDONG JIN DATIAN HOME FURNISHING CO., LTD.), 15 February 2017 (15.02.2017), entire document	1-13
A	CN 104806085 A (YUNDING NETWORK TECHNOLOGY BEIJING CO., LTD.), 29 July 2015 (29.07.2015), entire document	1-13
A	WO 2016023558 A1 (POLY CARE APS), 18 February 2016 (18.02.2016), entire document	1-13
A	US 2016042581 A1 (KU, C.M.), 11 February 2016 (11.02.2016), entire document	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 May 2018	07 June 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer HE, Yi Telephone No. 86-(010)-62085814

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/079999

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107038777 A	11 August 2017	None	
CN 103578165 A	12 February 2014	CN 103578165 B	29 June 2016
CN 106504391 A	15 March 2017	None	
CN 106408697 A	15 February 2017	None	
CN 104806085 A	29 July 2015	CN 104806085 B	18 July 2017
WO 2016023558 A1	18 February 2016	None	
US 2016042581 A1	11 February 2016	US 9892579 B2	13 February 2018

国际检索报告

国际申请号
PCT/CN2018/079999

A. 主题的分类

G07C 9/00(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)

G07C9

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;CNABS,VEN,CNKI:门锁，移动终端，密匙，加密，解密，服务器，标识，身份，验证，DOOR,LOCK,MOBILE,TERMINAL,ENCRYPT+,KEY,SERVER,ALGORITHM,AUTHENT+,IDENTIFICATION

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
PX	CN 107038777 A (云丁网络技术北京有限公司) 2017年 8月 11日 (2017-08-11) 全文	1-13
X	CN 103578165 A (高潮) 2014年 2月 12日 (2014-02-12) 说明书第0014-0018段，附图1	11-13
A	CN 106504391 A (北京爱接力科技发展有限公司) 2017年 3月 15日 (2017-03-15) 全文	1-13
A	CN 106408697 A (广东金大田家居股份有限公司) 2017年 2月 15日 (2017-02-15) 全文	1-13
A	CN 104806085 A (云丁网络技术北京有限公司) 2015年 7月 29日 (2015-07-29) 全文	1-13
A	WO 2016023558 A1 (POLY CARE APS) 2016年 2月 18日 (2016-02-18) 全文	1-13
A	US 2016042581 A1 (KU CHE-MING) 2016年 2月 11日 (2016-02-11) 全文	1-13

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 5月 18日	2018年 6月 7日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 何毅 电话号码 86-(010)-62085814

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/079999

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 107038777 A	2017年 8月 11日	无	
CN 103578165 A	2014年 2月 12日	CN 103578165 B	2016年 6月 29日
CN 106504391 A	2017年 3月 15日	无	
CN 106408697 A	2017年 2月 15日	无	
CN 104806085 A	2015年 7月 29日	CN 104806085 B	2017年 7月 18日
WO 2016023558 A1	2016年 2月 18日	无	
US 2016042581 A1	2016年 2月 11日	US 9892579 B2	2018年 2月 13日