(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107038777 B
(45)授权公告日 2020.08.18

(21)申请号 201710198457.1

(22)申请日 2017.03.29

(65)同一申请的已公布的文献号
申请公布号 CN 107038777 A

(43)申请公布日 2017.08.11

(73)专利权人 云丁网络技术(北京)有限公司
地址 100085 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

(72)发明人 唐皓 陈彬 张东胜

(74)专利代理机构 北京金智普华知识产权代理有限公司 11401
代理人 皋吉甫

(51)Int.Cl.
G07C 9/00(2020.01)

(56)对比文件
CN 105894627 A,2016.08.24
CN 105654580 A,2016.06.08
CN 104806085 A,2015.07.29
CN 104537735 A,2015.04.22
CN 103578165 A,2014.02.12
CN 105096419 A,2015.11.25
WO 2016023558 A1,2016.02.18
WO 2016130386 A1,2016.08.18

审查员 袁蔚涛

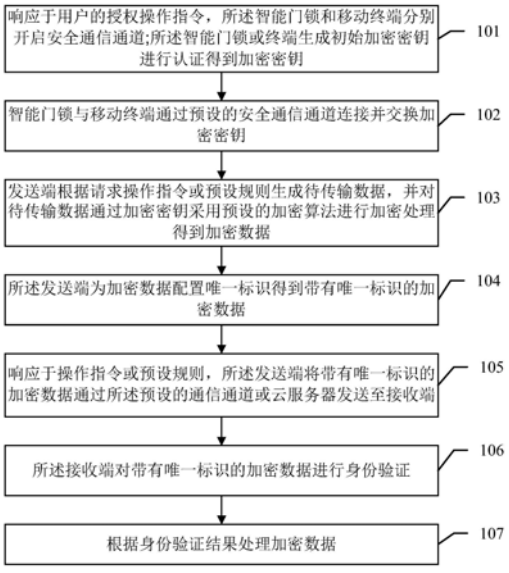
权利要求书2页 说明书14页 附图3页

(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

(57)摘要

本发明公开了一种基于智能门锁系统的安全通信方法,属于智能家居和安防技术领域。所述智能门锁系统包括智能门锁、移动终端分别与云服务器远程通信连接,所述方法包括: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;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;发送端将带有唯一标识的加密数据通过云服务器发送至接收端;接收端对带有唯一标识的加密数据进行身份验证,根据身份验证结果处理加密数据。本申请的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。



CN 107038777 B

1.一种基于智能门锁系统的安全通信方法,其特征在于,所述智能门锁系统包括智能门锁、移动终端分别与云服务器远程通信连接,所述方法包括:

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;所述预设的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;

发送端根据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;所述发送端为智能门锁或终端;

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;

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;所述接收端为终端或智能门锁,所述预设通信通道为短距离无线通信或近场通信通道;

所述接收端对带有唯一标识的加密数据进行身份验证,根据身份验证结果处理加密数据;所述接收端为终端或智能门锁。

2.根据权利要求1所述的基于智能门锁系统的安全通信方法,其特征在于,智能门锁与移动终端通过预设的通信通道连接并交换加密密钥之前还包括:

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。

3.根据权利要求1所述的基于智能门锁系统的安全通信方法,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.根据权利要求3所述的基于智能门锁系统的安全通信方法,其特征在于,根据身份验证结果处理加密数据包括:

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;

若验证签名匹配,则验证预设密钥值是否合法;

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。

5.根据权利要求1所述的基于智能门锁系统的安全通信方法,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:

发送端通过发送端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做为验证签名得到加密数据。

6.根据权利要求5所述的基于智能门锁系统的安全通信方法，其特征在于，根据身份验证结果处理加密数据包括：

若身份验证结果为验证结果匹配，则所述接收端采用接收端存储的公开密钥对加密数据的验证签名进行验证；

若验证签名匹配，则验证预设密钥值是否合法；

若预设密钥值合法，则接收端通过接收端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。

7.根据权利要求1或2或3或5中任一项所述的基于智能门锁系统的安全通信方法，其特征在于，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：

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该唯一标识匹配的加密密钥；

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。

8.根据权利要求1所述的基于智能门锁系统的安全通信方法，其特征在于，所述方法还包括：

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；

响应于用户的授权操作指令，智能门锁删除本地保存的指定加密密钥信息；

或云服务器响应于用户的远程授权操作指令，删除指定移动终端保存的加密密钥信息。

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

技术领域

[0001] 本发明涉及一种基于智能门锁系统的安全通信方法，属于智能家居和安防技术领域。

背景技术

[0002] 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App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。

[0003] 针对这一问题，目前已有的解决方法包括以下方式：

[0004] (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。

[0005] (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。

[0006] (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。

[0007] 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

[0008] 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：

[0009] 一种基于智能门锁系统的安全通信方法，所述方法包括：

[0010] 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；所述预设的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；

[0011] 发送端根据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；所述发送端为智能门锁或终端；

[0012] 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；

[0013] 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；所述接收端为终端或智能门锁，所述预设通信通道为短距离无线通信或近场通信通道；包括WIFI局域网、蓝牙、zigbee或近场通信(NFC)中

的一种；

[0014] 所述接收端对带有唯一标识的加密数据进行身份验证，根据身份验证结果处理加密数据；所述接收端为终端或智能门锁。

[0015] 进一步的，智能门锁与移动终端通过预设的通信通道连接并交换加密密钥之前还包括：

[0016] 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；

[0017] 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；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。

[0018] 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：

[0019] 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；

[0020] 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；

[0021] 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。

[0022] 进一步的，根据身份验证结果处理加密数据包括：

[0023] 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；

[0024] 若验证签名匹配，则验证预设密钥值是否合法；

[0025] 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。

[0026] 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：

[0027] 发送端通过发送端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；

[0028] 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；

[0029] 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做为验证签名得到加密数据。

[0030] 进一步的，根据身份验证结果处理加密数据包括：

[0031] 若身份验证结果为验证结果匹配，则所述接收端采用接收端存储的公开密钥对加密数据的验证签名进行验证；

[0032] 若验证签名匹配，则验证预设密钥值是否合法；

[0033] 若预设密钥值合法，则接收端通过接收端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。

[0034] 进一步的，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：

[0035] 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；

[0036] 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；

[0037] 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。

[0038] 进一步的,所述方法还包括:

[0039] 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;

[0040] 响应于用户的授权操作指令,智能门锁删除本地保存的指定加密密钥信息;

[0041] 或云服务器响应于用户的远程授权操作指令,删除指定移动终端保存的加密密钥信息。

[0042] 本发明还提供一种智能门锁系统,包括:

[0043] 智能门锁,设有预设的加密算法用于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;

[0044] 移动终端,所述移动终端内设置有用于控制所述智能门锁的APP,所述移动终端还设有蓝牙通信模块、zigbee通信模块或近场通信(NFC)通信模块中的至少一种;所述移动终端的设有预设的与智能门锁相同的加密算法用于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;

[0045] 云服务器,用于智能门锁与移动终端远程数据传输。

[0046] 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;

[0047] 所述移动终端的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。

[0048] 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。

[0049] 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

[0050] 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：

[0051] 图1为本申请的智能门锁系统的结构示意图；

[0052] 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；

[0053] 图3为本申请的步骤S103的一种实施例流程示意图；

[0054] 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

[0055] 本发明实施例提供了一种智能门锁的开锁方法。

[0056] 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。

[0057] 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。

[0058] 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：

[0059] 本申请的智能门锁系统包括：所述智能门锁、移动终端分别与云服务器远程通信连接；

[0060] 所述智能门锁设有预设的加密算法用于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；

[0061] 所述移动终端设有蓝牙通信模块、zigbee通信模块或近场通信(NFC)通信模块中的至少一种；所述移动终端设有预设的与智能门锁相同的加密算法用于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；

[0062] 云服务器用于智能门锁与移动终端远程数据传输。

[0063] 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；

[0064] 所述移动终端的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。

[0065] 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。

[0066] 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:

[0067] 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;所述预设的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。

[0068] 在本申请的实施方式中,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,IPD,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。

[0069] 步骤S103:发送端根据请求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;

[0070] 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算法。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;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,则根据请求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向智能门锁发出控制请求指令等,则移动终端作为发送端,智能门锁作为接收端;例如移动终端的控制请求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,则将该控制请求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。

[0071] 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。

[0072] 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;

[0073] 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。

[0074] 步骤S105：响应于请求指令或预设规则，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；所述接收端为终端或智能门锁，所述预设通信通道为短距离无线通信或近场通信通道；

[0075] 具体的响应于如步骤S103中的请求指令或预设规则，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；这里的预设的通信通道包括但不限于WIFI局域网、蓝牙、zigbee或近场通信(NFC)中的一种。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的通信通道发送给智能门锁。

[0076] 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的通信通道发送移动终端。

[0077] 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；

[0078] 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：

[0079] 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；

[0080] 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，则提取器唯一标识(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。)

[0081] 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；

[0082] 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。

[0083] 步骤S1063：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。

[0084] 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。

[0085] 步骤S107：所述接收端根据身份验证结果处理加密数据；所述接收端为终端或智能门锁。

[0086] 具体的，当份验证结果为确认是绑定的发送端发来的加密数据则进行解密和进一步处理；当身份验证结果为确认是非绑定的发送端发来的，则不作解密并生成报警信息。

[0087] 其中，本申请的方法还包括：

[0088] 步骤S101: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;

[0089] 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;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。。

[0090] 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。

[0091] 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:

[0092] 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;

[0093] 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发来的请求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。

[0094] 步骤S1032a:为初始加密数据配置预设密钥值;

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 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:

[0099] 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;

[0100] 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。

[0101] 步骤S1072a若验证签名匹配,则验证预设密钥值是否合法;

[0102] 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。

[0103] 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。

[0104] 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。

[0105] 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;

[0106] 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。

[0107] 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。

[0108] 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。

[0109] 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:

[0110] 步骤S1031b:发送端通过发送端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;

[0111] 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。

[0112] 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;

[0113] 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。

[0114] 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做为验证签名得到加密数据。

[0115] 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但,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。

[0116] 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:

[0117] 步骤S1071b:若身份验证结果为验证结果匹配,则所述接收端采用接收端存储的公开密钥对加密数据的验证签名进行验证;

[0118] 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。

[0119] 步骤S1072b:若验证签名匹配,则验证预设密钥值是否合法;

[0120] 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。

[0121] 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。

[0122] 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。

[0123] 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;

[0124] 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。

[0125] 步骤S1073b:若预设密钥值合法,则接收端通过接收端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。

[0126] 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。

[0127] 可选地,所述基于智能门锁系统的安全通信方法还包括:

[0128] 步骤1081: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;

[0129] 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,则用户通过设有智能门锁APP的移动终端,登陆输入账户登陆验证信息,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。

[0130] 步骤1082:响应于用户的授权操作指令,智能门锁删除本地保存的指定加密密钥信息;

[0131] 和/或云服务器响应于用户的远程授权操作指令,删除指定移动终端保存的加密密钥信息。

[0132] 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。

[0133] 实施例1:

[0134] 一种基于智能门锁系统的安全通信方法,包括如下步骤:

[0135] (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;

[0136] 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;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。

[0137] 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

[0138] (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；

[0139] (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。

[0140] (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。

[0141] (5)响应于操作指令，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。

[0142] (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。

[0143] (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。

[0144] 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。

[0145] 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。

[0146] 实施例2

[0147] 一种基于智能门锁系统的安全通信方法，包括如下步骤：

[0148] (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；

[0149] 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；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。

[0150] 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。

[0151] (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；

[0152] (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。

[0153] (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。

[0154] (5)响应于预设规则，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。

[0155] (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。

[0156] (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；

[0157] 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。

[0158] 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。

[0159] 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。

[0160] 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。

[0161] 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。

[0162] 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。

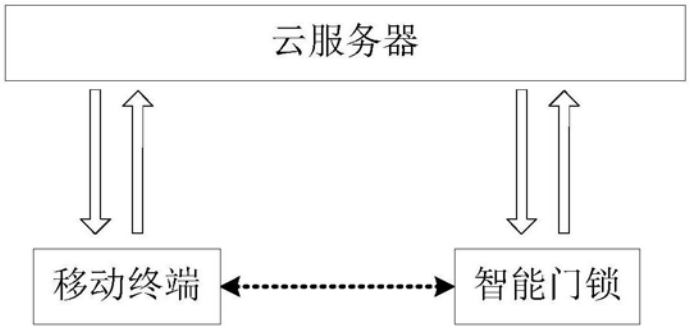


图1

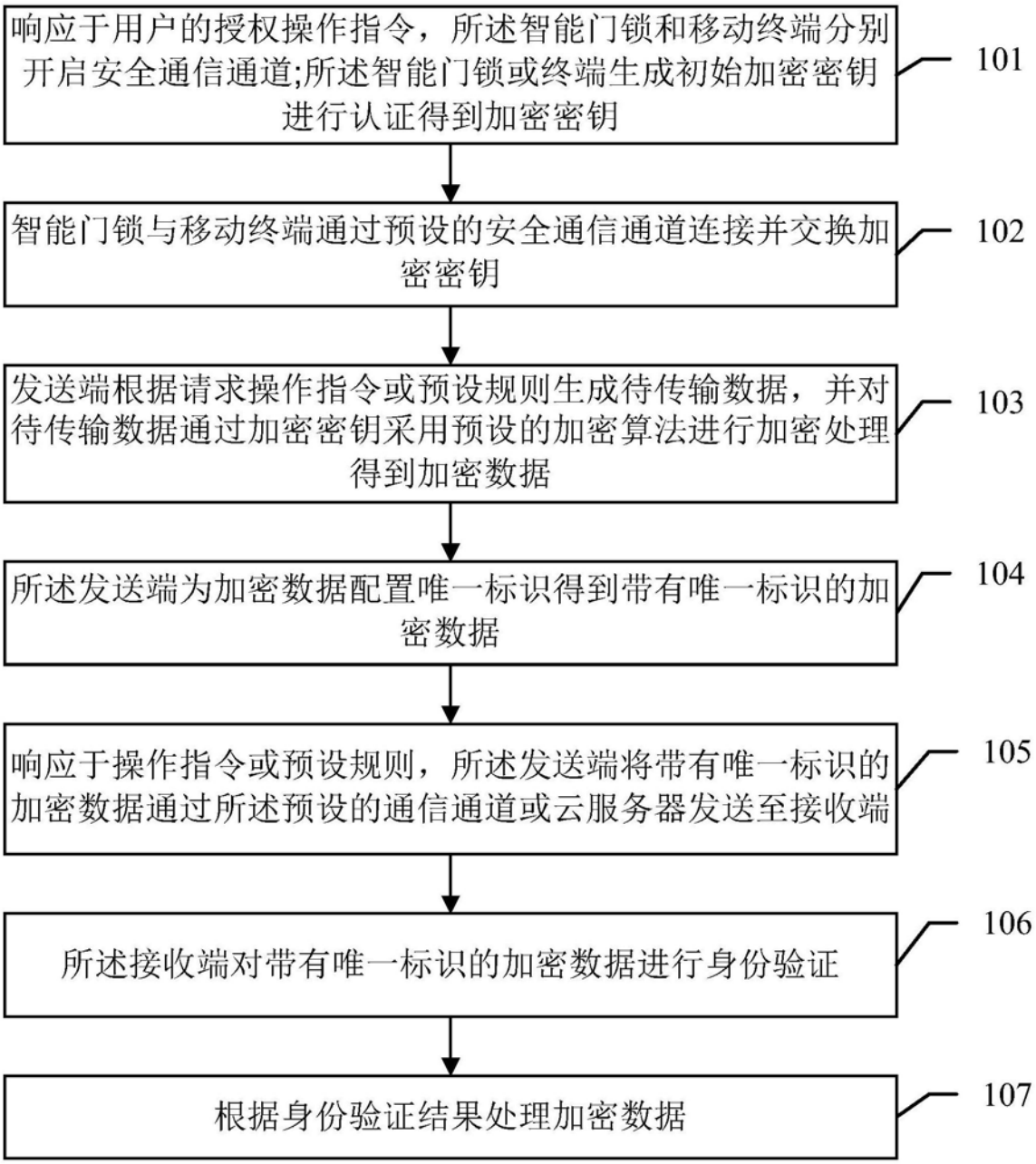

响应于用户的授权操作指令，所述智能门锁和移动终端分别开启安全通信通道;所述智能门锁或终端生成初始加密密钥进行认证得到加密密钥
101
智能门锁与移动终端通过预设的安全通信通道连接并交换加密密钥
102
发送端根据请求操作指令或预设规则生成待传输数据，并对待传输数据通过加密密钥采用预设的加密算法进行加密处理得到加密数据
103
所述发送端为加密数据配置唯一标识得到带有唯一标识的加密数据
104
响应于操作指令或预设规则，所述发送端将带有唯一标识的加密数据通过所述预设的通信通道或云服务器发送至接收端
105
所述接收端对带有唯一标识的加密数据进行身份验证
106
根据身份验证结果处理加密数据
107

图2

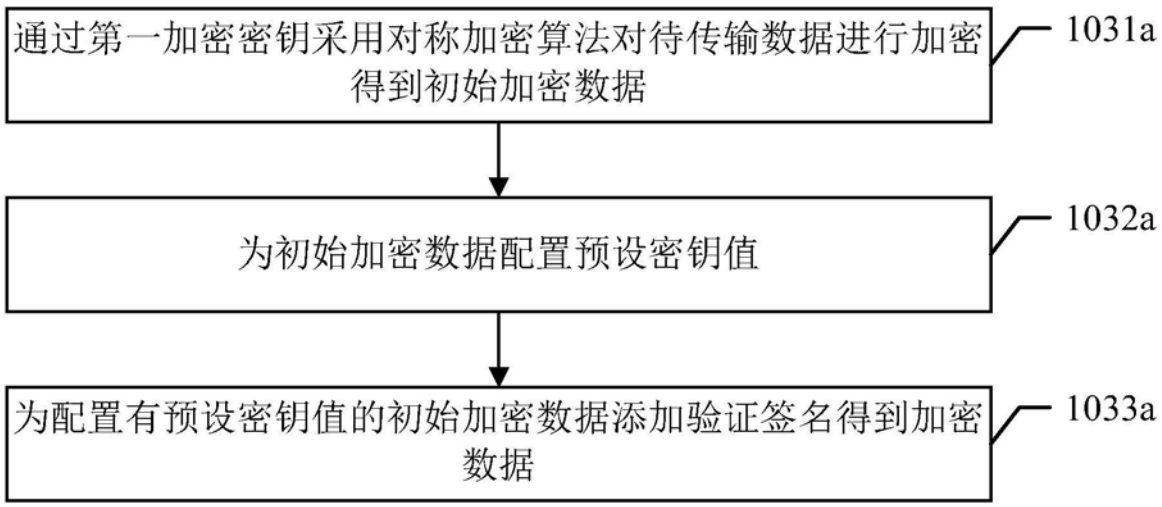

通过第一加密密钥采用对称加密算法对待传输数据进行加密得到初始加密数据
1031a
为初始加密数据配置预设密钥值
1032a
为配置有预设密钥值的初始加密数据添加验证签名得到加密数据
1033a

图3

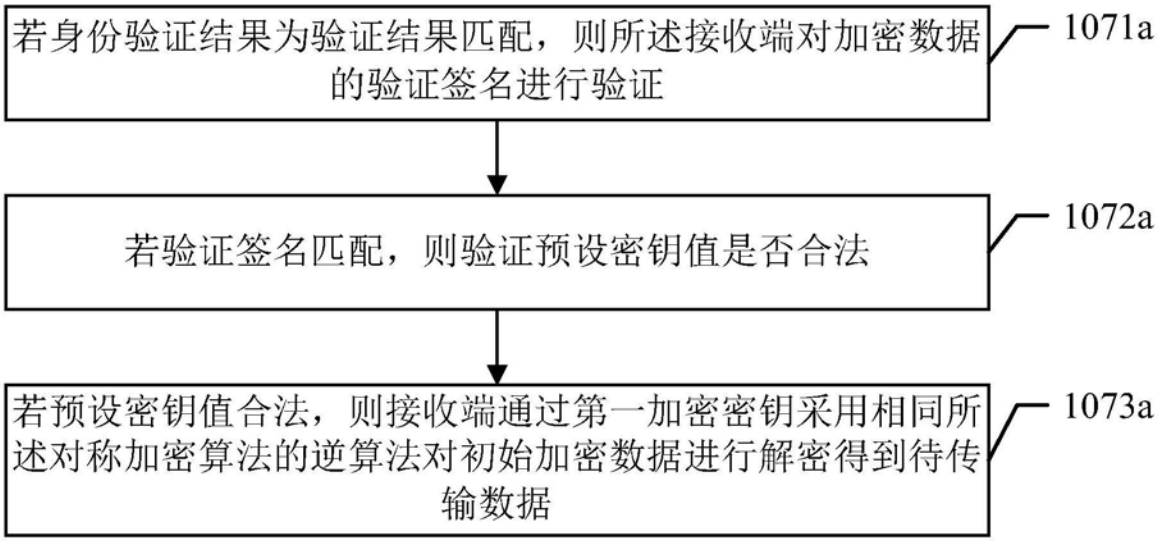

若身份验证结果为验证结果匹配，则所述接收端对加密数据的验证签名进行验证
1071a
若验证签名匹配，则验证预设密钥值是否合法
1072a
若预设密钥值合法，则接收端通过第一加密密钥采用相同所述对称加密算法的逆算法对初始加密数据进行解密得到待传输数据
1073a

图4