(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113282944 B
(45)授权公告日 2023.03.10

(21)申请号 202110723577.5
(22)申请日 2021.06.29
(65)同一申请的已公布的文献号
申请公布号 CN 113282944 A
(43)申请公布日 2021.08.20
(73)专利权人 珠海优特电力科技股份有限公司
地址 519085 广东省珠海市高新区金鸿七路68号
(72)发明人 杨绍华 阳仲伯 陈华
(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
专利代理师 彭星
(51)Int.Cl.
*G06F 21/60*(2013.01)
*G06F 21/31*(2013.01)
*G06F 21/45*(2013.01)

(56)对比文件
CN 109905235 A,2019.06.18
CN 107578511 A,2018.01.12
CN 109712278 A,2019.05.03
CN 108055235 A,2018.05.18

审查员 简文雨

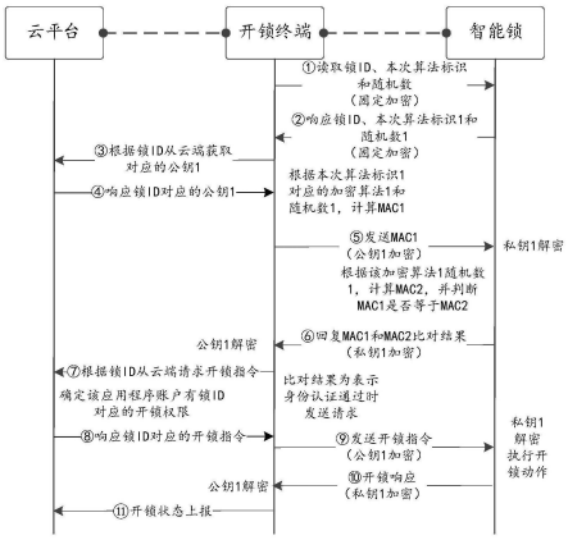
权利要求书4页 说明书13页 附图3页

(54)发明名称

# 智能锁开启方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种智能锁开启方法、装置、电子设备及存储介质，涉及安防技术领域。其应用于智能锁的方法包括：向开锁设备发送智能锁信息，智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；从开锁设备接收第一加密信息，为开锁设备基于锁对应公钥、第一加密算法和第一随机数获得；基于锁对应私钥、第一加密算法和第一随机数确定第一加密信息通过密钥验证；向开锁设备发送验证通过信息；从开锁设备接收开锁指令，基于开锁指令执行开锁动作，开锁指令为开锁设备从云平台接收的与锁身份标识对应的指令。该方法通过智能锁、开锁设备和云平台的通信方式以及非对称加密手段，提高了验证开锁的安全性。




CN 113282944 B

1.一种智能锁开启方法,其特征在于,应用于智能锁,所述方法包括:

向开锁设备发送智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数;

从所述开锁设备接收第一加密信息,所述第一加密信息为所述开锁设备基于锁对应公钥、第一加密算法和所述第一随机数获得,所述第一加密算法为与所述第一加密算法标识对应的加密算法,所述锁对应公钥为所述开锁设备从云平台接收的与所述锁身份标识对应的公钥;

基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证,所述锁对应私钥为所述智能锁从所述云平台获取的与所述锁身份标识对应的私钥;

向所述开锁设备发送验证通过信息;

从所述开锁设备接收开锁指令,基于所述开锁指令执行开锁动作,所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令;

其中,所述开锁设备包括开锁终端和智能钥匙,所述开锁设备通过接收流程接收所述智能锁向开锁设备发送的智能锁信息,所述接收流程包括:

通过所述智能钥匙向所述开锁终端发送智能钥匙信息,所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数;

通过所述开锁终端向所述智能钥匙发送第三加密信息,所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得,所述第三加密算法为与所述第三加密算法标识对应的加密算法,所述钥匙对应公钥为所述开锁终端从所述云平台接收的与所述钥匙身份标识对应的公钥;

通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证,所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥;

通过所述智能钥匙获取所述智能锁发送的智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数。

2.根据权利要求1所述的方法,其特征在于,所述基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证,包括:

采用所述锁对应私钥对所述第一加密信息进行解密,获得第一校验码;

基于所述智能锁本地存储的所述第一加密算法对所述第一随机数加密获得第二校验码;

在所述第一校验码和所述第二校验码相同时,确定所述第一加密信息通过密钥验证。

3.根据权利要求1所述的方法,其特征在于,在所述向开锁设备发送智能锁信息之前,所述方法还包括:

在所述云平台进行注册,以生成所述锁对应公钥和所述锁对应私钥;

从所述云平台获取所述锁对应私钥。

4.一种智能锁开启方法,其特征在于,应用于开锁设备,所述开锁设备包括开锁终端和智能钥匙,所述方法包括:

从智能锁接收智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第

一随机数；

基于所述锁身份标识从云平台接收与所述锁身份标识对应的锁对应公钥；

基于所述锁对应公钥、第一加密算法和所述第一随机数获得第一加密信息，所述第一加密算法为与所述第一加密算法标识对应的加密算法；

发送所述第一加密信息至所述智能锁，以使所述智能锁基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，向所述开锁设备发送验证通过信息；

基于所述验证通过信息从所述云平台获取开锁指令，并将所述开锁指令发送至所述智能锁，所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令；

其中，所述从智能锁接收智能锁信息包括：

通过所述智能钥匙向所述开锁终端发送智能钥匙信息，所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数；

通过所述开锁终端向所述智能钥匙发送第三加密信息，所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得，所述第三加密算法为与所述第三加密算法标识对应的加密算法，所述钥匙对应公钥为所述开锁终端从所述云平台接收的与所述钥匙身份标识对应的公钥；

通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证，所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥；

通过所述智能钥匙获取所述智能锁发送的智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数。

5.根据权利要求4所述的方法，其特征在于，所述智能钥匙和所述开锁终端之间的通信采用所述钥匙对应公钥和所述钥匙对应私钥进行通信加密，所述智能钥匙和所述智能锁之间的通信采用所述锁对应公钥和所述锁对应私钥进行通信加密。

6.根据权利要求4所述的方法，其特征在于，所述基于所述验证通过信息从所述云平台获取开锁指令，包括：

在获取到验证通过信息时，从所述云平台请求所述开锁指令，以使所述云平台确定所述开锁终端具有所述智能锁的开锁权限后，向所述开锁终端发送所述开锁指令；

接收所述云平台发送的所述开锁指令。

7.根据权利要求4所述的方法，其特征在于，在所述从智能锁接收智能锁信息之前，所述方法还包括：

在所述云平台进行注册，以生成所述钥匙对应公钥和所述钥匙对应私钥；

从所述云平台获取所述钥匙对应私钥。

8.根据权利要求1-7中任一项所述的方法，其特征在于，所述智能锁和所述开锁设备中均存储有加密算法标识和加密算法的映射关系。

9.一种智能锁开启装置，其特征在于，应用于智能锁，所述装置包括：

智能锁信息发送模块，用于向开锁设备发送智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；其中，所述开锁设备包括开锁终端和智能钥匙，所述开锁设备通过接收流程接收所述智能锁向开锁设备发送的智能锁信息，所述接收流程包

括:通过所述智能钥匙向所述开锁终端发送智能钥匙信息,所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数;通过所述开锁终端向所述智能钥匙发送第三加密信息,所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得,所述第三加密算法为与所述第三加密算法标识对应的加密算法,所述钥匙对应公钥为所述开锁终端从云平台接收的与所述钥匙身份标识对应的公钥;通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证,所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥;通过所述智能钥匙获取所述智能锁发送的智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数;

加密信息接收模块,用于从所述开锁设备接收第一加密信息,所述第一加密信息为所述开锁设备基于锁对应公钥、第一加密算法和所述第一随机数获得,所述第一加密算法为与所述第一加密算法标识对应的加密算法,所述锁对应公钥为所述开锁设备从云平台接收的与所述锁身份标识对应的公钥;

验证模块,用于基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证;

验证信息发送模块,用于向所述开锁设备发送验证通过信息;

开锁执行模块,用于从所述开锁设备接收开锁指令,基于所述开锁指令执行开锁动作,所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

10.一种智能锁开启装置,其特征在于,应用于开锁设备,所述装置包括:

智能锁信息接收模块,用于从智能锁接收智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数;其中,所述智能锁信息接收模块还用于:通过智能钥匙向开锁终端发送智能钥匙信息,所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数;通过所述开锁终端向所述智能钥匙发送第三加密信息,所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得,所述第三加密算法为与所述第三加密算法标识对应的加密算法,所述钥匙对应公钥为所述开锁终端从云平台接收的与所述钥匙身份标识对应的公钥;通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证,所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥;通过所述智能钥匙获取所述智能锁发送的智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数;

公钥接收模块,用于基于所述锁身份标识从云平台接收与所述锁身份标识对应的锁对应公钥;

加密信息确定模块,用于基于所述锁对应公钥、第一加密算法和所述第一随机数获得第一加密信息,所述第一加密算法为与所述第一加密算法标识对应的加密算法;

加密信息发送模块,用于发送所述第一加密信息至所述智能锁,以使所述智能锁基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证,向所述开锁设备发送验证通过信息;

开锁指令转发模块,用于基于所述验证通过信息从所述云平台获取开锁指令,并将所述开锁指令发送至所述智能锁,所述开锁指令为所述开锁设备从所述云平台接收的与所述

锁身份标识对应的指令。

# 智能锁开启方法、装置、电子设备及存储介质

## 技术领域

[0001] 本申请涉及安防技术领域，具体而言，涉及一种智能锁开启方法、装置、电子设备及存储介质。

## 背景技术

[0002] 目前的智能钥匙和智能锁，大多数采用开锁指令作为权限的具体体现形式，应用程序从云端获取开锁指令，并下发给智能钥匙和智能锁进行验证开锁，整个通信过程全靠数据加密进行保护，如密钥泄露，除用户外的设备能够直接通过密钥完成开锁，存在开锁验证流程安全性较低的问题。

## 发明内容

[0003] 有鉴于此，本申请实施例的目的在于提供一种智能锁开启方法、装置、电子设备及存储介质，以改善现有技术中存在的开锁验证流程安全性较低的问题。

[0004] 本申请实施例提供了一种智能锁开启方法，应用于智能锁，所述方法包括：向开锁设备发送智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；从所述开锁设备接收第一加密信息，所述第一加密信息为所述开锁设备基于锁对应公钥、第一加密算法和所述第一随机数获得，所述第一加密算法为与所述第一加密算法标识对应的加密算法，所述锁对应公钥为所述开锁设备从云平台接收的与所述锁身份标识对应的公钥；基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，所述锁对应私钥为所述智能锁从所述云平台获取的与所述锁身份标识对应的私钥；向所述开锁设备发送验证通过信息；从所述开锁设备接收开锁指令，基于所述开锁指令执行开锁动作，所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

[0005] 在上述实现方式中，智能锁向开锁设备发送智能锁信息，以使开锁设备获取锁对应公钥生成第一加密信息，再通过智能锁基于非对称加密方式对第一加密信息进行密钥验证，通过验证后开锁设备从云平台获取开锁指令控制智能锁开锁，从而通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，每次开锁前都进行节点与节点之间的身份认证，只有认证通过，才会逐级发送开锁指令，安全等级更高，且能够通过云平台直接地管理账户的开锁权限，无需用户绑定钥匙和锁，降低了操作难度。

[0006] 可选地，所述基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，包括：采用所述锁对应私钥对所述第一加密信息进行解密，获得所述第一校验码；基于所述智能锁本地存储的所述第一加密算法对所述第一随机数加密获得第二校验码；在所述第一校验码和所述第二校验码相同时，确定所述第一加密信息通过密钥验证。

[0007] 在上述实现方式中，基于非对称加密方式对第一加密信息进行验证，能够迅速、准确地验证开锁设备的身份，从而提高了开锁验证的安全性。

[0008] 可选地，在所述向开锁设备发送智能锁信息之前，所述方法还包括：在所述云平台进行注册，以生成所述锁对应公钥和所述锁对应私钥；从所述云平台获取所述锁对应私钥。

[0009] 在上述实现方式中，通过云平台进行注册以下发非对称加密的公钥和私钥，从而能够在云平台进行公私钥管理，避免开锁设备和智能锁的繁琐绑定流程，提高了操作便捷度。

[0010] 本申请实施例提供了一种智能锁开启方法，应用于开锁设备，所述方法包括：从智能锁接收智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；基于所述锁身份标识从云平台接收与所述锁身份标识对应的锁对应公钥；基于所述锁对应公钥、第一加密算法和所述第一随机数获得第一加密信息，所述第一加密算法为与所述第一加密算法标识对应的加密算法；发送所述第一加密信息至所述智能锁，以使所述智能锁基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，向所述开锁设备发送验证通过信息；基于所述验证通过信息从所述云平台获取开锁指令，并将所述开锁指令发送至所述智能锁，所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

[0011] 在上述实现方式中，智能锁向开锁设备发送智能锁信息，以使开锁设备获取锁对应公钥生成第一加密信息，再通过智能锁基于非对称加密方式对第一加密信息进行密钥验证，通过验证后开锁设备从云平台获取开锁指令控制智能锁开锁，从而通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，只有认证通过，才会发送开锁指令，安全等级更高，且能够通过云平台直接地管理账户的开锁权限，无需用户绑定钥匙和锁，降低了操作难度。

[0012] 可选地，所述开锁设备包括开锁终端和智能钥匙，所述从智能锁接收智能锁信息，包括：通过所述智能钥匙向所述开锁终端发送智能钥匙信息，所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数；通过所述开锁终端向所述智能钥匙发送第三加密信息，所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得，所述第三加密算法为与所述第三加密算法标识对应的加密算法，所述钥匙对应公钥为所述开锁终端从所述云平台接收的与所述钥匙身份标识对应的公钥；通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证，所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥；通过所述智能钥匙获取所述智能锁发送的智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数。

[0013] 在上述实现方式中，在使用智能钥匙时，通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，每次开锁前都进行节点与节点之间的身份认证，只有逐级验证通过才能完整整个开锁验证流程完成开锁动作，因此单独泄露的开锁指令无法完成开锁验证，提高了开锁验证的安全性。

[0014] 可选地，所述智能钥匙和所述开锁终端之间的通信采用所述钥匙对应公钥和所述钥匙对应私钥进行通信加密，所述智能钥匙和所述智能锁之间的通信采用所述锁对应公钥和所述锁对应私钥进行通信加密。

[0015] 在上述实现方式中，对智能钥匙、开锁终端和智能锁之间的通信进行非对称加密，进一步提高了开锁验证的安全性。

[0016] 可选地，所述基于所述验证通过信息从所述云平台获取开锁指令，包括：在获取到验证通过信息时，从所述云平台请求所述开锁指令，以使所述云平台确定所述开锁终端具有所述智能锁的开锁权限后，向所述开锁终端发送所述开锁指令；接收所述云平台发送的所述开锁指令。

[0017] 在上述实现方式中，通过云平台进行开锁权限的判定，不用提前绑定开锁终端和智能锁，在每次具有开锁需求时在云平台进行开锁权限的判定即可，减少了用户进行开锁验证的操作步骤。

[0018] 可选地，在所述从智能锁接收智能锁信息之前，所述方法还包括：在所述云平台进行注册，以生成所述钥匙对应公钥和所述钥匙对应私钥；从所述云平台获取所述钥匙对应私钥。

[0019] 在上述实现方式中，通过云平台进行注册以下发非对称加密的公钥和私钥，从而能够在云平台进行公私钥管理，避免开锁设备和智能锁的繁琐绑定流程，提高了操作便捷度。

[0020] 可选地，所述智能锁和所述开锁设备中均存储有加密算法标识和加密算法的映射关系。

[0021] 在上述实现方式中，在智能锁、开锁设备中存储加密算法标识和加密算法的映射关系，以在接收到其他设备的身份验证需求时进行对应的加密信息处理，从而不需要后台进行统一的加密认证，且只有本系统内能够通过加密算法标识和加密算法的对应关系进行解密，提高了安全性。

[0022] 本申请实施例还提供了一种智能锁开启装置，应用于智能锁，所述装置包括：智能锁信息发送模块，用于向开锁设备发送智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；加密信息接收模块，用于从所述开锁设备接收第一加密信息，所述第一加密信息为所述开锁设备基于锁对应公钥、第一加密算法和所述第一随机数获得，所述第一加密算法为与所述第一加密算法标识对应的加密算法，所述锁对应公钥为所述开锁设备从云平台接收的与所述锁身份标识对应的公钥；验证模块，用于基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，所述锁对应私钥为所述智能锁从所述云平台获取的与所述锁身份标识对应的私钥；验证信息发送模块，用于向所述开锁设备发送验证通过信息；开锁执行模块，用于从所述开锁设备接收开锁指令，基于所述开锁指令执行开锁动作，所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

[0023] 在上述实现方式中，智能锁向开锁设备发送智能锁信息，以使开锁设备获取锁对应公钥生成第一加密信息，再通过智能锁基于非对称加密方式对第一加密信息进行密钥验证，通过验证后开锁设备从云平台获取开锁指令控制智能锁开锁，从而通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，每次开锁前都进行节点与节点之间的身份认证，只有认证通过，才会逐级发送开锁指令，安全等级更高，且能够通过云平台直接地管理账户的开锁权限，无需用户绑定钥匙和锁，降低了操作难度。

[0024] 可选地，所述验证模块具体用于：采用所述锁对应私钥对所述第一加密信息进行解密，获得所述第一校验码；基于所述智能锁本地存储的所述第一加密算法对所述第一随机数加密获得第二校验码；在所述第一校验码和所述第二校验码相同时，确定所述第一加

密信息通过密钥验证。

[0025] 在上述实现方式中，基于非对称加密方式对第一加密信息进行验证，能够迅速、准确地验证开锁设备的身份，从而提高了开锁验证的安全性。

[0026] 可选地，所述智能锁开启装置还包括：注册模块，用于在所述云平台进行注册，以生成所述锁对应公钥和所述锁对应私钥；从所述云平台获取所述锁对应私钥。

[0027] 在上述实现方式中，通过云平台进行注册以下发非对称加密的公钥和私钥，从而能够在云平台进行公私钥管理，避免开锁设备和智能锁的繁琐绑定流程，提高了操作便捷度。

[0028] 本申请实施例还提供了一种智能锁开启装置，应用于开锁设备，所述装置包括：智能锁信息接收模块，用于从智能锁接收智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；公钥接收模块，用于基于所述锁身份标识从云平台接收与所述锁身份标识对应的锁对应公钥；加密信息确定模块，用于基于所述锁对应公钥、第一加密算法和所述第一随机数获得第一加密信息，所述第一加密算法为与所述第一加密算法标识对应的加密算法；加密信息发送模块，用于发送所述第一加密信息至所述智能锁，以使所述智能锁基于锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证，向所述开锁设备发送验证通过信息；开锁指令转发模块，用于基于所述验证通过信息从所述云平台获取开锁指令，并将所述开锁指令发送至所述智能锁，所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

[0029] 在上述实现方式中，智能锁向开锁设备发送智能锁信息，以使开锁设备获取锁对应公钥生成第一加密信息，再通过智能锁基于非对称加密方式对第一加密信息进行密钥验证，通过验证后开锁设备从云平台获取开锁指令控制智能锁开锁，从而通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，只有认证通过，才会发送开锁指令，安全等级更高，且能够通过云平台直接地管理账户的开锁权限，无需用户绑定钥匙和锁，降低了操作难度。

[0030] 可选地，所述开锁设备包括开锁终端和智能钥匙，所述智能锁信息接收模块具体用于：通过所述智能钥匙向所述开锁终端发送智能钥匙信息，所述智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数；通过所述开锁终端向所述智能钥匙发送第三加密信息，所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得，所述第三加密算法为与所述第三加密算法标识对应的加密算法，所述钥匙对应公钥为所述开锁终端从所述云平台接收的与所述钥匙身份标识对应的公钥；通过所述智能钥匙基于钥匙对应私钥、所述第三加密算法和所述第三随机数确定所述第三加密信息通过密钥验证，所述钥匙对应私钥为所述智能钥匙从所述云平台获取的与所述钥匙身份标识对应的私钥；通过所述智能钥匙获取所述智能锁发送的智能锁信息，所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数。

[0031] 在上述实现方式中，在使用智能钥匙时，通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，每次开锁前都进行节点与节点之间的身份认证，只有逐级验证通过才能完整整个开锁验证流程完成开锁动作，因此单独泄露的开锁指令无法完成开锁验证，提高了开锁验证的安全性。

[0032] 可选地，所述智能钥匙和所述开锁终端之间的通信采用所述钥匙对应公钥和所述

钥匙对应私钥进行通信加密，所述智能钥匙和所述智能锁之间的通信采用所述锁对应公钥和所述锁对应私钥进行通信加密。

[0033] 在上述实现方式中，对智能钥匙、开锁终端和智能锁之间的通信进行非对称加密，进一步提高了开锁验证的安全性。

[0034] 可选地，所述开锁指令转发模块具体用于：在获取到验证通过信息时，从所述云平台请求所述开锁指令，以使所述云平台确定所述开锁终端具有所述智能锁的开锁权限后，向所述开锁终端发送所述开锁指令；接收所述云平台发送的所述开锁指令。

[0035] 在上述实现方式中，通过云平台进行开锁权限的判定，不用提前绑定开锁终端和智能锁，在每次具有开锁需求时在云平台进行开锁权限的判定即可，减少了用户进行开锁验证的操作步骤。

[0036] 可选地，所述智能锁开启装置还包括：注册模块，用于在所述云平台进行注册，以生成所述钥匙对应公钥和所述钥匙对应私钥；从所述云平台获取所述钥匙对应私钥。

[0037] 在上述实现方式中，通过云平台进行注册以下发非对称加密的公钥和私钥，从而能够在云平台进行公私钥管理，避免开锁设备和智能锁的繁琐绑定流程，提高了操作便捷度。

[0038] 可选地，所述智能锁和所述开锁设备中均存储有加密算法标识和加密算法的映射关系。

[0039] 在上述实现方式中，在智能锁、开锁设备中存储加密算法标识和加密算法的映射关系，以在接收到其他设备的身份验证需求时进行对应的加密信息处理，从而不需要后台进行统一的加密认证，且相对于暗号类型的开锁口令，只有本系统内能够通过加密算法标识和加密算法的对应关系进行解密，提高了安全性。

[0040] 本申请实施例还提供了一种电子设备，所述电子设备包括存储器和处理器，所述存储器中存储有程序指令，所述处理器读取并运行所述程序指令时，执行上述任一实现方式中的步骤。

[0041] 本申请实施例还提供了一种可读取存储介质，所述可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器读取并运行时，执行上述任一实现方式中的步骤。

## 附图说明

[0042] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

[0043] 图1为本申请实施例提供的一种智能锁开启方法的流程示意图。

[0044] 图2为本申请实施例提供的又一种智能锁开启方法的流程示意图。

[0045] 图3为本申请实施例提供的一种应用于智能锁的智能锁开启装置的模块示意图。

[0046] 图4为本申请实施例提供的一种应用于开锁设备的智能锁开启装置的模块示意图。

[0047] 图标：30-智能锁开启装置；31-智能锁信息发送模块；32-加密信息接收模块；33-

验证模块;34-验证信息发送模块;35-开锁执行模块;40-智能锁开启装置;41-智能锁信息接收模块;42-公钥接收模块;43-加密信息确定模块;44-加密信息发送模块;45-开锁指令转发模块。

## 具体实施方式

[0048] 下面将结合本申请实施例中附图,对本申请实施例中的技术方案进行描述。

[0049] 为了解决现有技术中采用开锁指令作为权限的具体体现形式进行云端下发导致的开锁验证流程安全性较低的问题,本申请实施例提供了一种智能锁开启方法,应用于智能锁、开锁设备以及云平台。

[0050] 首先对云平台、开锁设备和智能锁进行说明:

[0051] 开锁设备可以包括安装有开锁应用程序的开锁终端,还可以包括安装有开锁应用程序的开锁终端以及智能钥匙,该开锁应用程序需要在云平台进行注册。

[0052] 上述开锁终端可以是手机、平板电脑和智能手表等电子设备。

[0053] 开锁应用程序的账户需要在云平台进行注册,该开锁应用程序中还包括与智能钥匙和/或智能锁进行加密的加密算法以及算法标识,其中加密算法可以为一种或多种,且存储有加密算法和算法标识的映射关系,例如采用映射表的形式存储加密算法和算法标识的映射关系,算法标识0x01对应加密算法1,0x02对应加密算法2等。

[0054] 同理,智能钥匙和智能锁中也存储有进行加密的加密算法、算法标识,以及加密算法与算法标识的映射关系,开锁应用程序、智能钥匙和智能锁中存储的映射关系相同。

[0055] 智能钥匙可以是能够与开锁设备配合完成开锁验证的电子设备,智能钥匙需要在云平台注册,智能钥匙的钥匙对应私钥保存在智能钥匙本地,钥匙对应公钥保存至云平台。

[0056] 可选地,智能钥匙还可以内置有加密芯片、硬件加密模块或加密软件,以支持开锁设备的开锁应用程序的通信固定加密。该通信固定加密可以是单密钥加密,例如DES(Data Encryption Standard,数据加密标准)算法、3DES(Triple DES)算法和AES(Advanced Encryption Standard,高级加密标准)算法等。

[0057] 此外,本实施中的智能钥匙还可以产生随机数以配合进行非对称加密,本实施例中的随机数生成可以采用线性同余算法和平方截取法等随机数生成算法。

[0058] 上述非对称加密算法可以是RSA算法、Elgamal加密算法、Rabin算法和ECC(Elliptic Curves Cryptography,椭圆曲线密码编码)算法等。

[0059] 智能锁可以是具有通信和计算处理功能的锁具,智能锁需要在云平台注册,智能锁的锁对应私钥保存在智能锁本地,锁对应公钥保存至云平台。

[0060] 可选地,智能锁内置有加密芯片、硬件加密模块或加密软件,以支持开锁设备的开锁应用程序和/或智能钥匙的通信固定加密。该通信固定加密可以是单密钥加密,例如DES(Data Encryption Standard,数据加密标准)算法、3DES(Triple DES)算法和AES(Advanced Encryption Standard,高级加密标准)算法等。

[0061] 可选地,智能锁还可以产生随机数,以进行非对称加密步骤。

[0062] 云平台是开锁设备、智能锁等整个系统的管理平台,用于用户管理、设备管理和权限管理等。云平台可以保存有一个或多个智能钥匙的钥匙对应公钥,以及一个或多个智能锁的锁对应公钥。

[0063] 本实施例中的智能锁对应的开锁指令在云平台和智能锁本地均有保存，用于进行开锁验证。

[0064] 云平台可以通过管理软件对开锁应用程序账户分配开锁权限，开锁设备每次通过开锁应用程序向云平台请求开锁指令时，云平台判断开锁应用程序账户是否具有对应智能锁的开锁权限，有权限的开锁应用程序账户才可以从云平台获取具有对应智能锁的开锁指令。

[0065] 上述云平台和开锁设备可以通过移动通信技术通信连接；开锁终端和智能钥匙可以通过WiFi、蓝牙等无线通信方式通信连接，也可以采用USB(Universal Serial Bus，通用串行总线)等有线连接方式通信连接；智能钥匙和智能锁可以通过总线或其他有线连接方式通信连接。

[0066] 由于开锁设备可以只包括开锁终端，也可以包括开锁终端和智能钥匙，本实施例首先对只采用开锁终端的智能锁开启方法进行说明。

[0067] 接下来请参考图1，图1为本申请实施例提供的一种智能锁开启方法的流程示意图，其中锁ID表示锁身份标识，本次算法标识1对应第一加密算法标识，加密算法1对应第一加密算法，随机数1为第一随机数，MAC1对应第一校验码，MAC2对应第二校验码，私钥1对应锁对应私钥，公钥1对应锁对应公钥，该智能锁开启方法的具体步骤可以如下：

[0068] 首先智能锁和开锁终端在云平台完成注册，智能锁将锁对应公钥存储至云平台，将锁对应私钥存储在本地。

[0069] 用户在开锁终端通过开锁应用程序发起开锁请求，开锁应用程序基于开锁请求向智能锁发送锁信息获取指令。

[0070] 智能锁接收到锁信息获取指令后，将智能锁自身的锁身份标识、第一加密算法标识和第一随机数作为智能锁信息发送至开锁终端。

[0071] 可选地，本实施例中的锁身份标识可以为数字、字母或其他字符组成的字符串，每个锁身份标识具有唯一性。

[0072] 上述第一加密算法标识可以是智能锁基于随机算法或其他方式在本地存储的所有加密算法中选取本次通信采用的加密算法对应的加密算法标识。

[0073] 可选地，本实施例中开锁终端和智能锁之间进行智能锁信息的请求和获取的通信过程可以采用固定加密方式进行加密。

[0074] 本实施例通过固定加密方式，在非对称加密的基础上进一步提高了开锁验证流程的整体安全性。

[0075] 开锁终端接收智能锁信息，并向云平台发送包含锁身份标识的锁对应公钥请求信息，以使云平台基于锁对应公钥请求信息向开锁终端发送与锁身份标识对应的锁对应公钥。

[0076] 开锁终端接收到锁对应公钥后，在算法标识和加密算法的映射关系中确定第一加密算法标识对应的第一加密算法，并确定从智能锁接收的第一随机数，然后基于锁对应公钥、第一加密算法、第一随机数生成第一加密信息，将第一加密信息发送至智能锁。

[0077] 具体地，开锁终端可以使用第一加密算法对第一随机数加密获得第一校验码，采用锁对应公钥对第一校验码进行公钥加密，从而获得第一加密信息。

[0078] 智能锁接收到第一加密信息后，采用锁对应私钥对第一加密信息进行解密获得第

一校验码，并基于智能锁本地的第一加密算法对第一随机数进行加密获得第二校验码，然后将第一校验码和第二校验码进行对比，在第一校验码和第二校验码相同时确定开锁终端通过身份认证，反之开锁终端未通过身份认证。

[0079] 可见，锁对应私钥并不进行对外发送，泄密风险极小，在锁对应私钥未泄密的情况下，采用锁对应私钥对开锁终端进行身份验证，非法获得锁对应公钥以及开锁指令均无法通过该身份验证以及整个开锁验证流程，提高了智能锁开启的安全性。

[0080] 在开锁终端通过身份认证后，智能锁向开锁终端发送验证通过信息，以使开锁终端的开锁应用程序向云平台发送开锁指令请求信息。

[0081] 云平台基于开锁指令请求信息中的锁对应标识和开锁终端的账户判定开锁应用程序是否具有该智能锁的开锁权限，在其具有开锁权限时确定该智能锁对应的开锁指令，将开锁指令发送至开锁终端。

[0082] 开锁终端通过开锁应用程序向智能锁发送开锁指令。

[0083] 智能锁从开锁终端接收到开锁指令后与智能锁本地存储的开锁指令进行对比，在两者相同时执行开锁动作，或者智能锁在接收到开锁指令时直接执行开锁动作。

[0084] 可选地，智能锁在执行开锁动作后还可以向开锁终端发送开锁响应确认信息，以使开锁终端通过开锁应用程序向云平台上报开锁状态。

[0085] 应当理解的是，本实施例中开锁终端和智能锁进行第一加密信息、验证通过信息、开锁指令和开锁响应确认信息的传输时，可以采用锁对应公钥和锁对应私钥进行通信加解密。

[0086] 本实施例通过对智能锁和开锁终端的通信进行非对称加密，进一步提高了智能锁开启流程的安全性，且在进行开锁权限验证的流程前并不需要提前在云平台绑定开锁终端的开锁应用程序与智能锁，简化了用户进行开锁验证的操作步骤。

[0087] 接下来对采用智能钥匙和开锁终端的方式进行说明，请参考图2，图2为本申请实施例提供的又一种智能锁开启方法的流程示意图，其中key ID对应钥匙身份标识，锁ID对应锁身份标识，本次算法标识1对应第一加密算法标识，算法标识3对应第三加密算法，加密算法1对应第一加密算法，加密算法3对应第三加密算法，随机数1对应第一随机数，随机数3对应第三随机数，公钥1对应锁对应公钥，私钥1对应锁对应私钥，公钥3对应钥匙对应公钥，私钥3对应钥匙对应私钥，MAC1对应第一校验码，MAC2对应第二校验码，MAC3对应第三校验码，MAC4对应第四校验码，该智能锁开启方法的具体步骤可以如下：

[0088] 首先智能锁、智能钥匙和开锁终端在云平台完成注册，智能锁将锁对应公钥存储至云平台，将锁对应私钥存储在本地，智能钥匙将钥匙对应公钥存储至云平台，将钥匙对应私钥存储在本地。

[0089] 用户在开锁终端通过开锁应用程序发起开锁请求，开锁应用程序基于开锁请求向智能钥匙发送钥匙信息获取指令。

[0090] 智能钥匙接收到钥匙信息获取指令后，将智能钥匙自身的钥匙身份标识、第三加密算法标识和第三随机数作为智能钥匙信息发送至开锁终端。

[0091] 可选地，本实施例中的钥匙身份标识可以为数字、字母或其他字符组成的字符串，每个钥匙身份标识具有唯一性。

[0092] 上述第三加密算法标识可以是智能钥匙基于随机算法或其他方式在本地存储的

所有加密算法中选取本次通信采用的加密算法对应的加密算法标识。

[0093] 可选地，本实施例中开锁终端和智能钥匙之间进行智能钥匙信息的请求和获取的通信过程可以采用固定加密方式进行加密。

[0094] 开锁终端接收智能钥匙信息，并向云平台发送包含钥匙身份标识的钥匙对应公钥请求信息，以使云平台基于钥匙对应公钥请求信息向开锁终端发送与钥匙身份标识对应的钥匙对应公钥。

[0095] 开锁终端接收到钥匙对应公钥后，在算法标识和加密算法的映射关系中确定第三加密算法标识对应的第三加密算法，并确定从智能钥匙接收的第三随机数，然后基于钥匙对应公钥、第三加密算法、第三随机数生成第三加密信息，将第三加密信息发送至智能钥匙。

[0096] 具体地，开锁终端可以使用第三加密算法对第三随机数加密获得第三校验码，采用钥匙对应公钥对第三校验码进行公钥加密，从而获得第三加密信息。

[0097] 智能钥匙接收到第三加密信息后，采用钥匙对应私钥对第三加密信息进行解密获得第三校验码，并基于智能锁本地的第三加密算法对第三随机数进行加密获得第四校验码，然后将第三校验码和第四校验码进行对比，在第三校验码和第四校验码相同时确定开锁终端通过身份认证，反之开锁终端未通过身份认证。

[0098] 在开锁终端通过智能钥匙的身份认证后，智能钥匙向智能锁发送锁信息获取指令。

[0099] 智能锁接收到锁信息获取指令后，将智能锁自身的锁身份标识、第一加密算法标识和第一随机数作为智能锁信息发送至智能钥匙。

[0100] 可选地，本实施例中智能锁和智能钥匙之间进行智能锁信息的请求和获取的通信过程可以采用固定加密方式进行加密。

[0101] 智能钥匙接收智能锁信息，并向开锁终端发送包含锁身份标识的锁对应公钥请求信息，以使开锁终端向云平台发送包含锁身份标识的锁对应公钥请求信息，然后云平台基于锁对应公钥请求信息向开锁终端发送与锁身份标识对应的锁对应公钥。

[0102] 开锁终端将锁对应公钥发送至智能钥匙后，智能钥匙在算法标识和加密算法的映射关系中确定第一加密算法标识对应的第一加密算法，并确定智能锁发送的第一随机数，然后使用第一加密算法对第一随机数进行加密获得第一校验码，采用锁对应公钥对第一校验码进行公钥加密，从而获得第一加密信息，将第一加密信息发送至智能锁。

[0103] 智能锁接收到第一加密信息后，采用锁对应私钥对第一加密信息进行解密获得第一校验码，并基于智能锁本地的第一加密算法对第一随机数进行加密获得第二校验码，然后将第一校验码和第二校验码进行对比，在第一校验码和第二校验码相同时确定智能钥匙通过身份认证，反之智能钥匙未通过身份认证。

[0104] 在智能钥匙通过身份认证后，智能锁向智能钥匙发送验证通过信息，以使智能钥匙将验证通过信息发送至开锁终端，通过开锁终端的开锁应用程序向云平台发送开锁指令请求信息。

[0105] 云平台基于开锁指令请求信息中的锁对应标识和开锁终端的账户判定开锁应用程序是否具有该智能锁的开锁权限，在其具有开锁权限时确定该智能锁对应的开锁指令，将开锁指令发送至开锁终端，以使开锁终端将开锁指令通过智能钥匙发送至智能锁。

[0106] 智能锁从智能钥匙接收到开锁指令后与智能锁本地存储的开锁指令进行对比，在两者相同时执行开锁动作，或者智能锁在接收到开锁指令时直接执行开锁动作。

[0107] 应当理解的是，本实施例中智能钥匙与开锁终端之间的通信过程，除了上述固定加密的步骤外，其他通信数据可以采用钥匙对应公钥和钥匙对应密钥进行非对称加解密，智能钥匙与智能锁之间的通信过程，除了上述固定加密的步骤外，其他通信数据可以采用锁对应公钥和锁对应密钥进行非对称加解密。

[0108] 为了配合本申请实施例提供的上述的智能锁开启方法，分别针对其中应用于智能锁和开锁设备的部分提供了一种智能锁开启装置。

[0109] 请参考图3，图3为本申请实施例提供的一种应用于智能锁的智能锁开启装置的模块示意图。

[0110] 智能锁开启装置30包括：

[0111] 智能锁信息发送模块31，用于向开锁设备发送智能锁信息，智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；

[0112] 加密信息接收模块32，用于从开锁设备接收第一加密信息，第一加密信息为开锁设备基于锁对应公钥、第一加密算法和第一随机数获得，第一加密算法为与第一加密算法标识对应的加密算法，锁对应公钥为开锁设备从云平台接收的与锁身份标识对应的公钥；

[0113] 验证模块33，用于基于锁对应私钥、第一加密算法和第一随机数确定第一加密信息通过密钥验证，锁对应私钥为智能锁从云平台获取的与锁身份标识对应的私钥；

[0114] 验证信息发送模块34，用于向开锁设备发送验证通过信息；

[0115] 开锁执行模块35，用于从开锁设备接收开锁指令，基于开锁指令执行开锁动作，开锁指令为开锁设备从云平台接收的与锁身份标识对应的指令。

[0116] 可选地，验证模块33具体用于：采用所述锁对应私钥对所述第一加密信息进行解密，获得所述第一校验码；基于所述智能锁本地存储的所述第一加密算法对所述第一随机数加密获得第二校验码；在所述第一校验码和所述第二校验码相同时，确定所述第一加密信息通过密钥验证。

[0117] 可选地，智能锁开启装置30还包括：注册模块，用于在云平台进行注册，以生成锁对应公钥和锁对应私钥，从云平台获取锁对应私钥。

[0118] 请参考图4，图4为本申请实施例提供的一种应用于开锁设备的智能锁开启装置的模块示意图。

[0119] 智能锁开启装置40包括：

[0120] 智能锁信息接收模块41，用于从智能锁接收智能锁信息，智能锁信息包括锁身份标识、第一加密算法标识和第一随机数；

[0121] 公钥接收模块42，用于基于锁身份标识从云平台接收与锁身份标识对应的锁对应公钥；

[0122] 加密信息确定模块43，用于基于锁对应公钥、第一加密算法和第一随机数获得第一加密信息，第一加密算法为与第一加密算法标识对应的加密算法；

[0123] 加密信息发送模块44，用于发送第一加密信息至智能锁，以使智能锁基于锁对应私钥、第一加密算法和第一随机数确定第一加密信息通过密钥验证，向开锁设备发送验证通过信息；

[0124] 开锁指令转发模块45,用于基于验证通过信息从云平台获取开锁指令,并将开锁指令发送至智能锁,开锁指令为开锁设备从云平台接收的与锁身份标识对应的指令。

[0125] 可选地,开锁设备包括开锁终端和智能钥匙,智能锁信息接收模块41具体用于:通过智能钥匙向开锁终端发送智能钥匙信息,智能钥匙信息包括钥匙身份标识、第三加密算法标识和第三随机数;通过开锁终端向智能钥匙发送第三加密信息,所述第三加密信息为所述开锁终端基于钥匙对应公钥、第三加密算法和所述第三随机数获得,第三加密算法为与第三加密算法标识对应的加密算法,钥匙对应公钥为开锁终端从云平台接收的与钥匙身份标识对应的公钥;通过智能钥匙基于钥匙对应私钥、第三加密算法和第三随机数确定第三加密信息通过密钥验证,钥匙对应私钥为智能钥匙从云平台获取的与钥匙身份标识对应的私钥;通过智能钥匙获取智能锁发送的智能锁信息,智能锁信息包括锁身份标识、第一加密算法标识和第一随机数。

[0126] 可选地,所述智能钥匙和所述开锁终端之间的通信采用所述钥匙对应公钥和所述钥匙对应私钥进行通信加密,所述智能钥匙和所述智能锁之间的通信采用所述锁对应公钥和所述锁对应私钥进行通信加密。

[0127] 可选地,所述开锁指令转发模块45具体用于:在获取到验证通过信息时,从所述云平台请求所述开锁指令,以使所述云平台确定所述开锁终端具有所述智能锁的开锁权限后,向所述开锁终端发送所述开锁指令;接收所述云平台发送的所述开锁指令。

[0128] 可选地,智能锁和开锁设备中均存储有加密算法标识和加密算法的映射关系。

[0129] 可选地,所述智能锁开启装置40还包括:注册模块,用于在所述云平台进行注册,以生成所述钥匙对应公钥和所述钥匙对应私钥;从所述云平台获取所述钥匙对应私钥。

[0130] 本申请实施例还提供了一种电子设备,该电子设备包括存储器和处理器,所述存储器中存储有程序指令,所述处理器读取并运行所述程序指令时,执行本实施例提供的智能锁开启方法中任一项所述方法中的步骤。

[0131] 应当理解是,该电子设备可以是个人电脑(Personal Computer,PC)、平板电脑、智能手机、个人数字助理(Personal Digital Assistant,PDA)等具有逻辑计算功能的电子设备。

[0132] 本申请实施例还提供了一种可读取存储介质,所述可读取存储介质中存储有计算机程序指令,所述计算机程序指令被一处理器读取并运行时,执行智能锁开启方法中的步骤。

[0133] 综上所述,本申请实施例提供了一种智能锁开启方法、装置、电子设备及存储介质,应用于智能锁,所述方法包括:向开锁设备发送智能锁信息,所述智能锁信息包括锁身份标识、第一加密算法标识和第一随机数;从所述开锁设备接收第一加密信息,所述第一加密信息为所述开锁设备基于锁对应公钥、第一加密算法和所述第一随机数获得,所述第一加密算法为与所述第一加密算法标识对应的加密算法,所述锁对应公钥为所述开锁设备从云平台接收的与所述锁身份标识对应的公钥;基于所述锁对应私钥、所述第一加密算法和所述第一随机数确定所述第一加密信息通过密钥验证,所述锁对应私钥为所述智能锁从所述云平台获取的与所述锁身份标识对应的私钥;向所述开锁设备发送验证通过信息;从所述开锁设备接收开锁指令,基于所述开锁指令执行开锁动作,所述开锁指令为所述开锁设备从所述云平台接收的与所述锁身份标识对应的指令。

[0134] 在上述实现方式中，智能锁向开锁设备发送智能锁信息，以使开锁设备获取锁对应公钥生成第一加密信息，再通过智能锁基于非对称加密方式对第一加密信息进行密钥验证，通过验证后开锁设备从云平台获取开锁指令控制智能锁开锁，从而通过智能锁、云平台和开锁设备之间基于非对称加密方式的通信流程进行开锁验证，每次开锁前都进行节点与节点之间的身份认证，只有认证通过，才会逐级发送开锁指令，安全等级更高，且能够通过云平台直接地管理账户的开锁权限，无需用户绑定钥匙和锁，降低了操作难度。

[0135] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的框图显示了根据本申请的多个实施例的设备的可能实现的体系架构、功能和操作。在这点上，框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现方式中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图中的每个方框、以及框图的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0136] 另外，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0137] 所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。因此本实施例还提供了一种可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器读取并运行时，执行区块数据存储方法中任一项所述方法中的步骤。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(ROM，Read-Only Memory)、随机存取存储器(RAM，RanDom Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0138] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0139] 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。

[0140] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备

所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

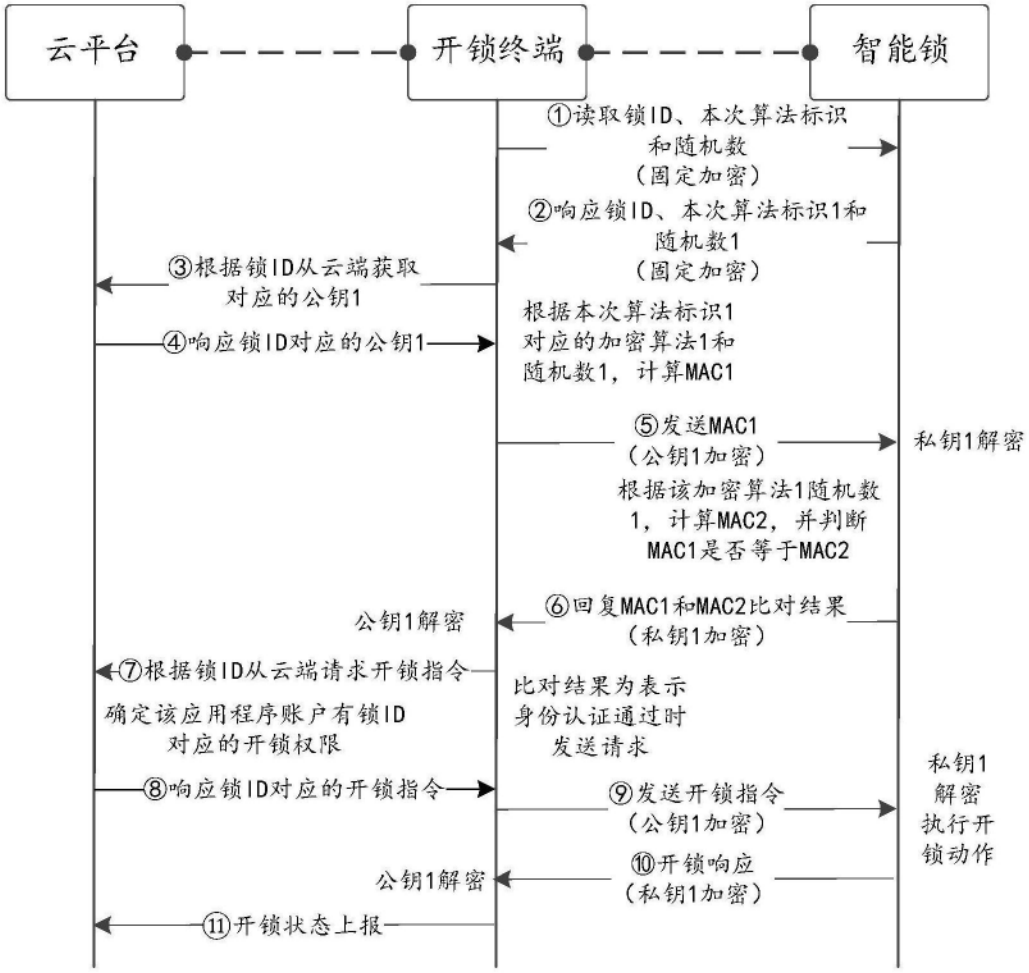

云平台
开锁终端
智能锁
①读取锁ID、本次算法标识和随机数（固定加密）
②响应锁ID、本次算法标识1和随机数1（固定加密）
③根据锁ID从云端获取对应的公钥1
④响应锁ID对应的公钥1
根据本次算法标识1对应的加密算法1和随机数1，计算MAC1
⑤发送MAC1（公钥1加密）
私钥1解密
根据该加密算法1随机数1，计算MAC2，并判断MAC1是否等于MAC2
⑥回复MAC1和MAC2比对结果（私钥1加密）
公钥1解密
⑦根据锁ID从云端请求开锁指令
比对结果为表示身份认证通过时发送请求
确定该应用程序账户有锁ID对应的开锁权限
⑧响应锁ID对应的开锁指令
⑨发送开锁指令（公钥1加密）
私钥1解密执行开锁动作
⑩开锁响应（私钥1加密）
公钥1解密
⑪开锁状态上报

图1

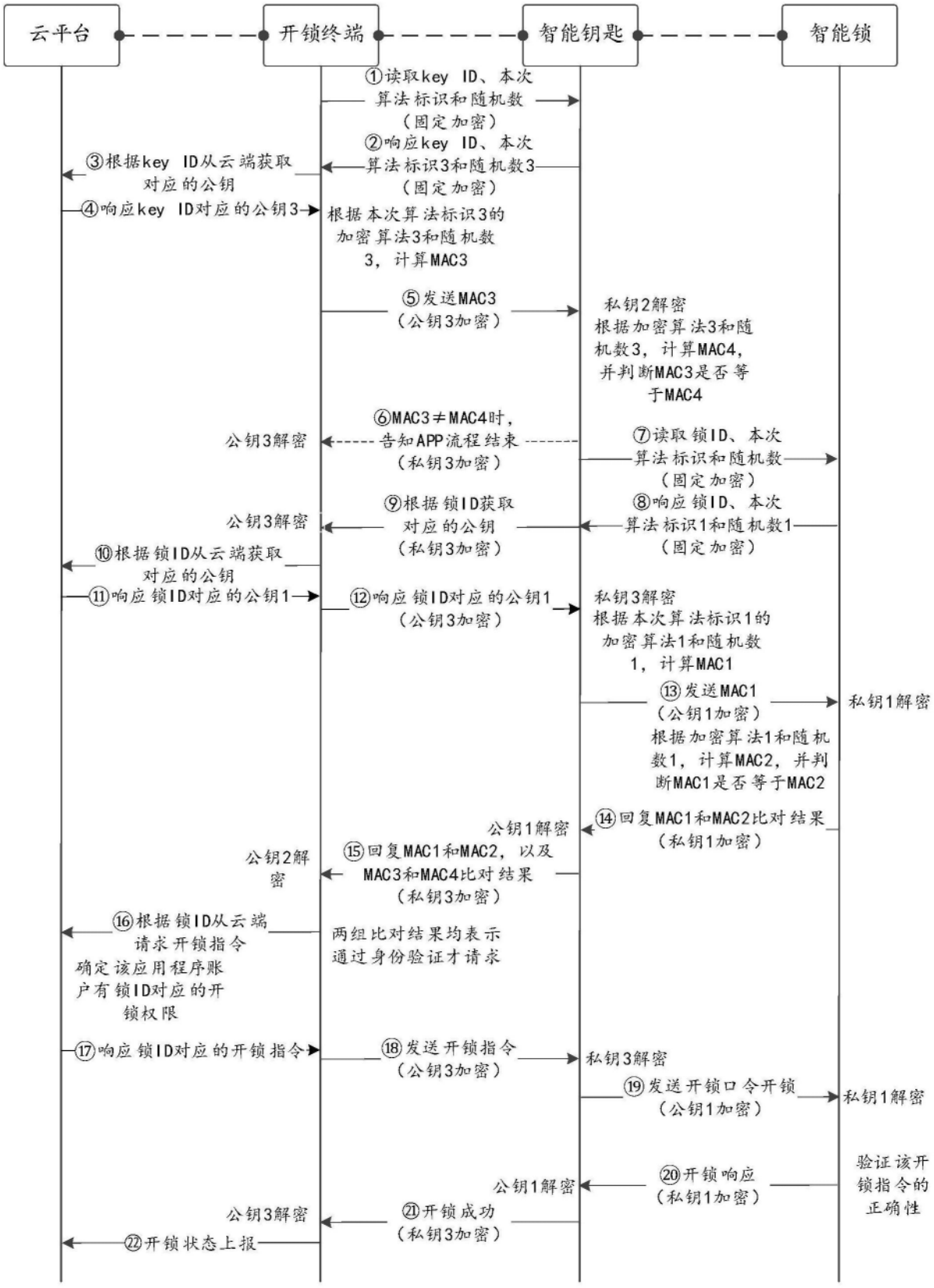

云平台
开锁终端
智能钥匙
智能锁
①读取key ID、本次算法标识和随机数（固定加密）
②响应key ID、本次算法标识3和随机数3（固定加密）
③根据key ID从云端获取对应的公钥
④响应key ID对应的公钥3
根据本次算法标识3的加密算法3和随机数3，计算MAC3
⑤发送MAC3（公钥3加密）
私钥2解密
根据加密算法3和随机数3，计算MAC4，并判断MAC3是否等于MAC4
⑥MAC3≠MAC4时，告知APP流程结束（私钥3加密）
公钥3解密
⑦读取锁ID、本次算法标识和随机数（固定加密）
⑧响应锁ID、本次算法标识1和随机数1（固定加密）
⑨根据锁ID获取对应的公钥（私钥3加密）
公钥3解密
⑩根据锁ID从云端获取对应的公钥
⑪响应锁ID对应的公钥1
⑫响应锁ID对应的公钥1（公钥3加密）
私钥3解密
根据本次算法标识1的加密算法1和随机数1，计算MAC1
⑬发送MAC1（公钥1加密）
私钥1解密
根据加密算法1和随机数1，计算MAC2，并判断MAC1是否等于MAC2
⑭回复MAC1和MAC2比对结果（私钥1加密）
公钥1解密
⑮回复MAC1和MAC2，以及MAC3和MAC4比对结果（私钥3加密）
公钥2解密
⑯根据锁ID从云端请求开锁指令
确定该应用程序账户有锁ID对应的开锁权限
两组比对结果均表示通过身份验证才请求
⑰响应锁ID对应的开锁指令
⑱发送开锁指令（公钥3加密）
私钥3解密
⑲发送开锁口令开锁（公钥1加密）
私钥1解密
⑳开锁响应（私钥1加密）
公钥1解密
验证该开锁指令的正确性
㉑开锁成功（私钥3加密）
公钥3解密
㉒开锁状态上报

图2

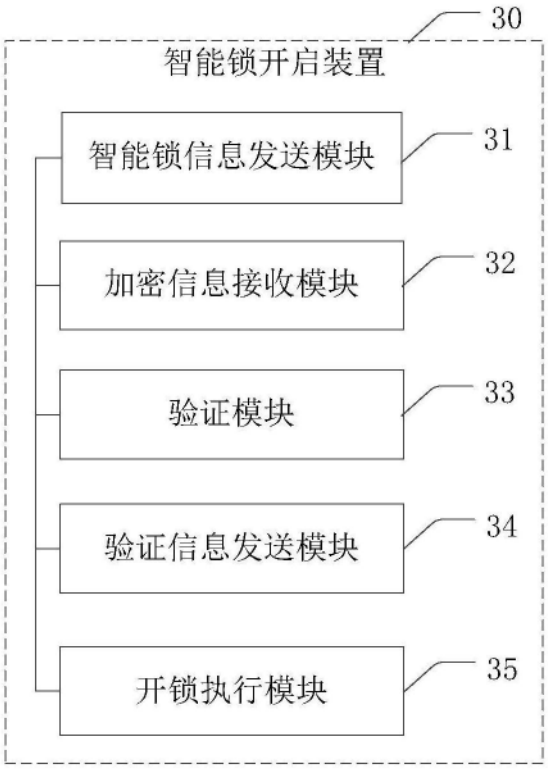

30
智能锁开启装置
智能锁信息发送模块
31
加密信息接收模块
32
验证模块
33
验证信息发送模块
34
开锁执行模块
35

图3

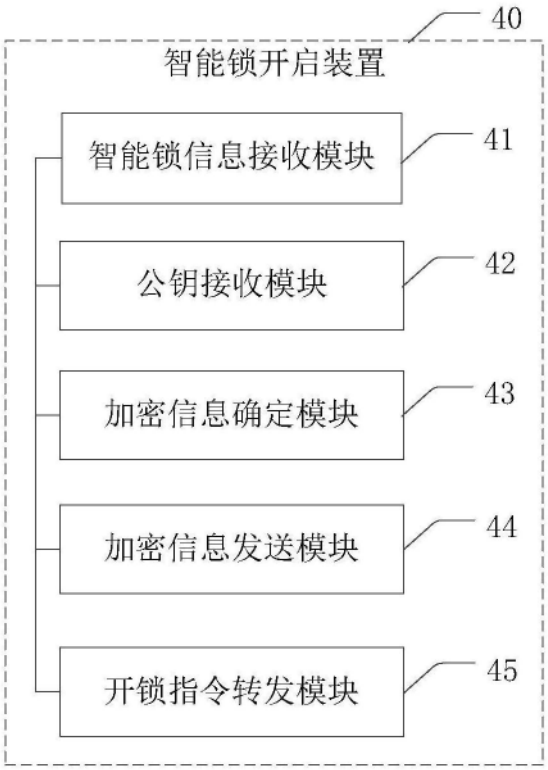

40
智能锁开启装置
智能锁信息接收模块
41
公钥接收模块
42
加密信息确定模块
43
加密信息发送模块
44
开锁指令转发模块
45

图4