(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 111508114 B
(45)授权公告日 2022.04.22

(21)申请号 202010303137.X

(22)申请日 2020.04.17

(65)同一申请的已公布的文献号
申请公布号 CN 111508114 A

(43)申请公布日 2020.08.07

(73)专利权人 上海钧正网络科技有限公司
地址 201199 上海市闵行区秀文路898号1幢501室

(72)发明人 杨磊 金威 曹学军

(74)专利代理机构 华进联合专利商标代理有限公司 44224
代理人 杨欢

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

(56)对比文件
CN 105069864 A,2015.11.18
CN 110047185 A,2019.07.23
CN 101504779 A,2009.08.12
CN 101276313 A,2008.10.01
CN 107211245 A,2017.09.26
CN 109150509 A,2019.01.04
CN 208393535 U,2019.01.18
US 2006214766 A1,2006.09.28
CN 110322600 A,2019.10.11

审查员 喻婷

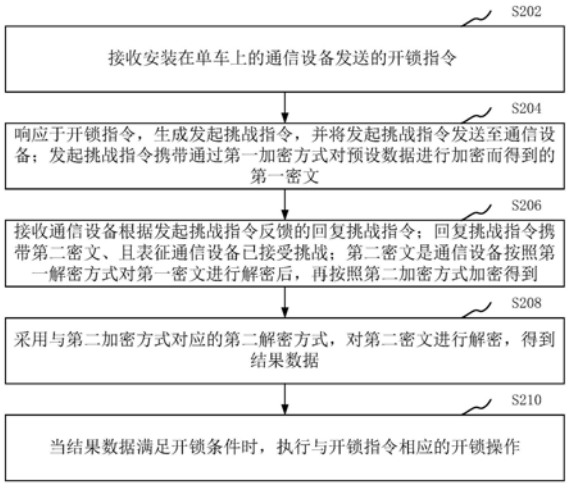
权利要求书2页 说明书14页 附图6页

(54)发明名称

单车开锁方法、装置、存储介质和轮毂锁

(57)摘要

本申请涉及一种单车开锁方法、装置、存储介质和轮毂锁。所述方法包括：接收安装在单车上的通信设备发送的开锁指令；响应于开锁指令，生成发起挑战指令，并将发起挑战指令发送至通信设备；发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；接收通信设备根据发起挑战指令反馈的回复挑战指令；回复挑战指令携带第二密文、且表征通信设备已接受挑战；第二密文是通信设备按照第一解密方式对第一密文进行解密后，再按照第二加密方式加密得到；采用与第二加密方式对应的第二解密方式，对第二密文进行解密，得到结果数据；当结果数据满足开锁条件时，执行与开锁指令相应的开锁操作。采用本方法能够提高单车的安全性。



CN 111508114 B

1.一种单车开锁方法,应用于安装在单车上的轮毂锁,其特征在于,所述方法包括:

接收安装在单车上的通信设备发送的开锁指令;

响应于所述开锁指令,生成发起挑战指令,并将所述发起挑战指令发送至所述通信设备;所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文;所述第一加密方式对应的预设密钥是诊断工具发送的与轮毂锁的配置信息对应的设置密钥,且所述预设密钥还上报至服务器以使得所述通信设备从所述服务器中获取与所述轮毂锁对应的预设密钥;

接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令;所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战;所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后,再按照第二加密方式加密得到;

采用与所述第二加密方式对应的第二解密方式,对所述第二密文进行解密,得到结果数据;

当所述结果数据满足开锁条件时,执行与所述开锁指令相应的开锁操作。

2.根据权利要求1所述的方法,其特征在于,所述接收安装在单车上的通信设备发送的开锁指令之前,所述方法还包括:

接收安装在单车上的通信设备发送的获取指令;

响应于所述获取指令,将所述轮毂锁的配置信息反馈至所述通信设备;反馈的所述配置信息用于指示所述通信设备从服务器处获取与所述配置信息相匹配的预设密钥;所述预设密钥用于辅助所述第一解密方式的实施。

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:

当诊断工具无法从服务器中查找到与所述轮毂锁的配置信息对应的预设密钥时,接收所述诊断工具设置的设置密钥,并进行相应的挑战操作;

当所述挑战操作成功时,将所述诊断工具设置的设置密钥作为与所述配置信息对应的预设密钥并存储,并触发所述诊断工具将所述预设密钥上报至所述服务器进行更新存储。

4.根据权利要求3所述的方法,其特征在于,所述当诊断工具无法从服务器中查找到与所述轮毂锁的配置信息对应的预设密钥时,接收所述诊断工具设置的设置密钥,包括:

当诊断工具无法从服务器中查找到与所述轮毂锁的配置信息对应的预设密钥时,接收所述诊断工具设置的设置密钥所对应的第三密文;所述第三密文通过默认密钥对所述设置密钥进行加密得到;

所述将所述诊断工具设置的设置密钥作为与所述配置信息对应的预设密钥并存储之前,所述方法还包括:

当所述挑战操作成功时,获取默认密钥,并通过所述默认密钥对所述第三密文进行解密,得到对应的设置密钥。

5.根据权利要求1所述的方法,其特征在于,所述第一密文的加密步骤包括:

获取所述轮毂锁本地存储的预设密钥;

通过所述预设密钥和加密函数,对预设数据进行加密处理得到对应的第一密文。

6.根据权利要求5所述的方法,其特征在于,所述第二密文的加密步骤包括:

所述通信设备获取与所述轮毂锁对应的预设密钥;

所述通信设备在获取到所述第一密文后,通过获取的预设密钥和解密函数对所述第一

密文进行解密，得到解密数据；

将所述解密数据同时作为明文和密钥，通过所述加密函数进行加密处理，得到对应的第二密文。

7.根据权利要求1至6中任一项所述的方法，其特征在于，所述当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作，包括：

当所述结果数据与所述预设数据为相同数据时，向所述通信设备反馈表示挑战成功的反馈数据；

按照所述开锁指令，在所述单车上执行开锁操作；

将与所述开锁操作对应的开锁结果反馈至所述通信设备。

8.一种单车开锁装置，应用于安装在单车上的轮毂锁，其特征在于，所述装置包括：

接收模块，用于接收安装在单车上的通信设备发送的开锁指令；

加密模块，用于响应于所述开锁指令，生成发起挑战指令，并将所述发起挑战指令发送至所述通信设备；所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；所述第一加密方式对应的预设密钥是诊断工具发送的与轮毂锁的配置信息对应的设置密钥，且所述预设密钥还上报至服务器以使得所述通信设备从所述服务器中获取与所述轮毂锁对应的预设密钥；

所述接收模块用于接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令；所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战；所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后，再按照第二加密方式加密得到；

解密模块，用于采用与所述第二加密方式对应的第二解密方式，对所述第二密文进行解密，得到结果数据；

执行模块，用于当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作。

9.一种轮毂锁，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至7中任一项所述的方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

单车开锁方法、装置、存储介质和轮毂锁

技术领域

[0001] 本申请涉及单车技术领域，特别是涉及一种单车开锁方法、装置、存储介质和轮毂锁。

背景技术

[0002] 随着单车技术的发展，出现了单车加密技术。其中，常见的单车包括私有单车、免费单车或者共享单车等类型的单车。由于单车技术解决了人们在短距离间的代步问题，因而受到了广泛的关注。现有的单车加密技术采用通信设备和锁体一体化的方式进行加密处理，并通过蜂窝网络或者蓝牙与一体化的通信设备和锁体进行通信，从而实现控制单车上的锁体的打开或关闭。

[0003] 然而，采用现有的一体化的通信设备和锁体的方式对单车进行加密处理时，由于单车上的锁体裸露在外，易于遭受自然或人为的损坏，因此无法避免非法用户暴力破坏锁体结构而免费骑行单车的情况，因而存在安全性低的问题。

发明内容

[0004] 基于此，有必要针对上述技术问题，提供一种能够提高安全性的单车开锁方法、装置、存储介质和轮毂锁。

[0005] 一种单车开锁方法，应用于安装在单车上的轮毂锁，所述方法包括：

[0006] 接收安装在单车上的通信设备发送的开锁指令；

[0007] 响应于所述开锁指令，生成发起挑战指令，并将所述发起挑战指令发送至所述通信设备；所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；

[0008] 接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令；所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战；所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后，再按照第二加密方式加密得到；

[0009] 采用与所述第二加密方式对应的第二解密方式，对所述第二密文进行解密，得到结果数据；

[0010] 当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作。

[0011] 一种单车开锁装置，应用于安装在单车上的轮毂锁，所述装置包括：

[0012] 接收模块，用于接收安装在单车上的通信设备发送的开锁指令；

[0013] 加密模块，用于响应于所述开锁指令，生成发起挑战指令，并将所述发起挑战指令发送至所述通信设备；所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；

[0014] 所述接收模块用于接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令；所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战；所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后，再按照第二加密方式加密得

到；

[0015] 解密模块，用于采用与所述第二加密方式对应的第二解密方式，对所述第二密文进行解密，得到结果数据；

[0016] 执行模块，用于当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作。

[0017] 一种轮毂锁，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

[0018] 接收安装在单车上的通信设备发送的开锁指令；

[0019] 响应于所述开锁指令，生成发起挑战指令，并将所述发起挑战指令发送至所述通信设备；所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；

[0020] 接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令；所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战；所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后，再按照第二加密方式加密得到；

[0021] 采用与所述第二加密方式对应的第二解密方式，对所述第二密文进行解密，得到结果数据；

[0022] 当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作。

[0023] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现以下步骤：

[0024] 接收安装在单车上的通信设备发送的开锁指令；

[0025] 响应于所述开锁指令，生成发起挑战指令，并将所述发起挑战指令发送至所述通信设备；所述发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文；

[0026] 接收所述通信设备根据所述发起挑战指令反馈的回复挑战指令；所述回复挑战指令携带第二密文、且表征所述通信设备已接受挑战；所述第二密文是所述通信设备按照第一解密方式对所述第一密文进行解密后，再按照第二加密方式加密得到；

[0027] 采用与所述第二加密方式对应的第二解密方式，对所述第二密文进行解密，得到结果数据；

[0028] 当所述结果数据满足开锁条件时，执行与所述开锁指令相应的开锁操作。

[0029] 上述单车开锁方法、装置、存储介质和轮毂锁，通过接收安装在单车上的通信设备发送的开锁指令，从而生成相应的发起挑战指令，并发送至单车上的通信设备。接收单车上的通信设备根据发起挑战指令反馈的回复挑战指令，并对回复挑战指令携带的第二密文进行解密处理，得到结果数据，当结果数据满足预设开锁条件时，执行与开锁指令相应的开锁操作。通过这样的方式，对单车进行加密，可避免因暴力行为破坏锁体而带来的安全问题，因而提高了单车的安全性。并且，由于减少了锁体被破坏的风险，也减少了因维修单车上的锁体和通信设备而产生的成本，因而降低了维修成本，大大提高了单车的使用效率。

附图说明

[0030] 图1为一个实施例中单车开锁方法的应用环境图；

[0031] 图2为一个实施例中单车开锁方法的流程示意图；

[0032] 图3为一个实施例中出厂设置的步骤的时序图；

[0033] 图4为一个实施例中单车开锁方法的时序图；

[0034] 图5为一个实施例中单车开锁方法的结构示意图；

[0035] 图6为一个实施例中单车开锁装置的结构框图；

[0036] 图7为另一个实施例中单车开锁装置的结构框图；.

[0037] 图8为一个实施例中轮毂锁的内部结构图。

具体实施方式

[0038] 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。

[0039] 本申请提供的单车开锁方法，可以应用于如图1所示的应用环境中。其中，服务器110通过网络与诊断工具120进行通信，诊断工具120通过接口与轮毂锁140进行通信，服务器110通过网络与通信设备130进行通信，通信设备130通过接口与轮毂锁140进行通信。其中，服务器110可以用独立的服务器或者是多个服务器组成的服务器集群来实现。诊断工具120具体可以是线下诊断仪，用于对轮毂锁的密钥设置情况进行诊断的仪器。通信设备130具体可以是安装在单车上的天线盒。轮毂锁140具体可以是安装在单车的轮毂位置的锁。

[0040] 可以理解，轮毂锁140接收诊断工具120设置的设置密钥，并将接收的设置密钥作为与轮毂锁140的配置信息对应的预设密钥并进行存储。轮毂锁140触发诊断工具120将预设密钥上报至服务器110进行更新存储，以使得通信设备130可从服务器110中获取与轮毂锁140对应的预设密钥。其中，设置密钥是诊断工具120设置的密钥，预设密钥是轮毂锁140更新后的密钥。

[0041] 轮毂锁140接收通信设备130发送的开锁指令，轮毂锁140响应于开锁指令，并生成发起挑战指令，并将发起挑战指令发送至通信设备，发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文。轮毂锁140接收通信设备130根据发起挑战指令反馈的回复挑战指令；回复挑战指令携带第二密文、且表征通信设备130已接受挑战，第二密文是通信设备130按照第一解密方式对第一密文进行解密后，再按照第二加密方式加密得到。轮毂锁140采用与第二加密方式对应的第二解密方式，对第二密文进行解密，得到结果数据。当结果数据满足开锁条件时，轮毂锁140执行与开锁指令相应的开锁操作。

[0042] 在一个实施例中，如图2所示，提供了一种单车开锁方法，以该方法应用于图1中的轮毂锁140为例进行说明，该单车开锁方法包括以下步骤：

[0043] S202，接收安装在单车上的通信设备发送的开锁指令。

[0044] 其中，通信设备是用于通信的设备，可分为有线通讯设备和无线通讯设备。其中，有线通讯设备是通过架空线缆、同轴线缆、光纤或音频线缆等传输介质传输信息的设备，具体可以是进行数据传输的小型电子设备。无线通讯设备是无需实体线缆作为传输介质的设备，具体可以是无线网桥、无线网卡、无线避雷器或天线盒等设备。

[0045] 指令是用于指示接收方执行相应操作的命令。开锁指令是安装在单车上的通信设备发送的、且用于指示轮毂锁进行开锁操作的指令。其中，轮毂锁是安装在单车的轮毂位置

的锁。

[0046] 具体地，通信设备和轮毂锁一同安装在单车上。通信设备生成开锁指令，并将开锁指令发送给轮毂锁，以使得轮毂锁可以接收到通信设备发送的开锁指令。

[0047] 在一个实施例中，通信设备主动向轮毂锁发送开锁请求，通信设备可以是无线通信设备，比如天线盒。安装在单车上的天线盒生成开锁请求，并将生成的开锁请求发送至轮毂锁，以使得轮毂锁可以接收到天线盒发送的开锁请求。其中，轮毂锁在接收到开锁请求之前处于休眠状态。

[0048] 在一个实施例中，轮毂锁与通信设备之间采用接口进行通信，具体可以是采用RS-485通信。其中，RS-485通信是一种半双工通信，也就是说轮毂锁与通信设备之间不能同时进行接收数据和发送数据。并且，通过一个RS-485转换器，就可将RS485的接口与轮毂锁内部集成的单片机的UART(Universal Asynchronous Receiver/Transmitter，通用异步收发传输器)串口或者I2C(Inter Integrated Circuit，多主控总线)进行连接，其中，轮毂锁的内部集成的可以是STM32M0系列的单片机。

[0049] 在一个实施例中，轮毂锁与通信设备之间由于采用RS-485通信方式进行通信时，可提高通信链路的抗干扰能力。并且，轮毂锁内部集成STM32M0系列的单片机作为主控芯片，既可以实现安全通信又可以降低功耗。

[0050] 在一个实施例中，轮毂锁与通信设备之间可以通过网络进行通信，比如通过互联网、4G(the 4th generation mobile communication technology，第四代移动通信技术)、或5G等网络进行通信，或者轮毂锁与通信设备之间可以通过数据线进行通信。本申请实施例对此不作限定。

[0051] 在一个实施例中，单车是二轮的小型陆上车辆，比如脚踏自行车、电动自行车或者电动摩托车等类型的车辆，还比如私有单车、免费单车或者共享单车等类型的车辆。

[0052] S204，响应于开锁指令，生成发起挑战指令，并将发起挑战指令发送至通信设备；发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文。

[0053] 其中，发起挑战指令是用于向接收方请求挑战的指令，比如轮毂锁向通信设备请求挑战。加密方式是对数据进行加密的方式，第一加密方式具体是轮毂锁上进行加密的方式。预设数据是预设的随机数，具体可以是轮毂锁生成的随机数。密文是加密后的数据，第一密文是通过第一加密方式对预设数据进行加密后得到的数据。

[0054] 具体地，单车上的轮毂锁响应于天线盒发送的开锁指令，生成随机数，并将随机数作为预设数据。轮毂锁采用第一加密方式对预设数据进行加密，从而生成对应的第一密文，且生成包括有第一密文的发起挑战指令并将发起挑战指令发送至天线盒，以使得天线盒接收到发起挑战指令以进行反馈。

[0055] 在一个实施例中，第一加密方式采用的加密算法可以是对称加密算法或者非对称加密算法。其中，对称加密算法比如AES算法(Advanced Encryption Standard，高级加密标准)和RC2算法(Rivest Code，一种传统的私钥块加密算法)等算法，非对称加密算法比如ECC算法(Elliptic Curves Cryptography，椭圆曲线密码编码学)或RSA算法(Rivest-Shamir-Adleman，一种加密和解密算法)等算法。本申请实施例对此不作限定。

[0056] 在一个实施例中，第一密文的加密步骤包括获取轮毂锁本地存储的预设密钥；通过预设密钥和加密函数，对预设数据进行加密处理得到对应的第一密文。

[0057] 在一个实施例中，轮毂锁采用AES算法对预设数据进行加密，具体可以是采用AES128加密算法。其中，AES128算法表示密钥长度为128位的AES算法。具体地，AES128加密算法可通过公式C＝E(K,P)来实现。其中，P表示明文，也就是待加密的数据；K表示密钥，也就是加密明文P的密码；E表示AES加密函数；C表示密文，也就是采用AES算法进行加密后所得到的加密数据。

[0058] 在一个实施例中，轮毂锁读取本地存储的预设密钥，将预设密钥作为进行加密数据的密码，也就是密钥K。轮毂锁生成随机数作为待加密的数据，也就是明文P。轮毂锁采用AES128加密函数C＝E(K,P)和密钥K对随机数进行加密处理，得到对应的第一密文。其中，加密函数具体可以是aes_encrypt_pkcs7。

[0059] 上述实施例中，轮毂锁通过预设密钥和加密函数，对预设数据进行加密处理从而得到对应的第一密文。通过这样的加密方式，轮毂锁可对预设数据进行加密，保证了预设数据的安全性，而保障了通信设备与轮毂锁之间的通信安全。

[0060] 在一个实施例中，轮毂锁将所得到的第一密文作为传输内容，从而生成对应的发起挑战指令，并将发起挑战指令发送至通信设备，如单车上的天线盒，以使得天线盒可以接收到轮毂锁生成的加密后的预设数据。

[0061] S206，接收通信设备根据发起挑战指令反馈的回复挑战指令；回复挑战指令携带第二密文、且表征通信设备已接受挑战；第二密文是通信设备按照第一解密方式对第一密文进行解密后，再按照第二加密方式加密得到。

[0062] 其中，回复挑战指令是用于回复发送方的挑战的指令，比如通信设备回应轮毂锁发起的挑战。加密方式是对数据进行加密的方式，第二加密方式具体是在通信设备上进行加密的方式。密文是加密后的数据，第二密文是通过第二加密方式对第一密文进行解密后的数据再进行加密所得到的数据。第一解密方式是对第一密文进行解密的方式，且第一解密方式与第一加密方式相互对应。

[0063] 具体地，单车上的通信设备接收轮毂锁发送的发起挑战指令，并采用第一解密方式对发起挑战指令中的第一密文进行解密，得到解密数据。通信设备采用第二加密方式对得到的解密数据进行加密，从而生成对应的第二密文，且生成包括有第二密文的回复挑战指令并将回复挑战指令发送至轮毂锁，以使得轮毂锁可以接收到回复挑战指令以表示通信设备接收了挑战。其中，解密数据是通信设备对第一密文进行解密后，所得到的数据。

[0064] 在一个实施例中，第一解密方式与第一加密方式相互对应。比如，当第一加密方式采用了AES加密算法，则第一解密方式采用对应的AES解密算法；当第一加密方式采用了RC2加密算法，则第一解密方式采用对应的RC2解密算法；当第一加密方式采用了ECC加密算法，则第一解密方式采用对应的ECC解密算法；当第一加密方式采用了RSA加密算法，则第一解密方式采用对应的RSA解密算法。

[0065] 在一个实施例中，第二密文的加密步骤包括：通信设备获取与轮毂锁对应的预设密钥；通信设备在获取到第一密文后，通过获取的预设密钥和解密函数对第一密文进行解密，得到解密数据；将解密数据同时作为明文和密钥，通过加密函数进行加密处理，得到对应的第二密文。

[0066] 在一个实施例中，轮毂锁采用AES解密算法对第一密文进行解密，具体可以是采用AES128解密算法。其中，AES128算法表示密钥长度为128位的AES算法。具体地，AES128解密

算法可通过公式P＝D(K,C)来实现。其中,C表示密文,也就是加密数据;K表示密钥,也就是解密密文C的密码;D表示AES解密函数;P表示明文,也就是采用AES算法进行解密后所得到的解密数据。

[0067] 在一个实施例中,通信设备将发起挑战指令中携带的第一密文作为密文C,将获取的与轮毂锁对应的预设密钥作为密钥K,通信设备采用AES128解密函数对密文C进行解密处理,也就是根据公式P＝D(K,C),从而得到解密数据。其中,解密函数具体可以是aes_decrypt_pkcs7。

[0068] 在一个实施例中,通信设备将解密数据同时作为明文P以及密钥K,通信设备采用AES128加密函数C＝E(K,P)对解密数据进行加密,从而得到对应的第二密文。加密函数具体可以是aes_encrypt_pkcs7。

[0069] 上述实施例中,通信设备通过预设密钥和解密函数对第一密文进行解密,得到解密数据,并采用加密函数对解密数据进行加密,从而到对应的第二密文。通过这样的方式,表示通信设备可对轮毂锁发送的第一密文进行解密,并对解密数据进行再次加密,保证了解密数据的安全性,从而保障了通信设备与轮毂锁之间的通信安全。

[0070] 在一个实施例中,通信设备将所得到的第二密文作为传输内容,从而生成对应的回复挑战指令,并将回复挑战指令发送至轮毂锁,以使得轮毂锁可以接收到通信设备生成的加密后的解密数据。

[0071] S208,采用与第二加密方式对应的第二解密方式,对第二密文进行解密,得到结果数据。

[0072] 其中,第二解密方式是对第二密文进行解密的方式,且第二解密方式与第二加密方式相互对应。结果数据是轮毂锁对第二密文进行解密后,所得到的数据。

[0073] 在一个实施例中,第二解密方式与第二加密方式相互对应。比如,当第二加密方式采用了AES加密算法,则第二解密方式采用对应的AES解密算法;当第二加密方式采用了RC2加密算法,则第二解密方式采用对应的RC2解密算法;当第二加密方式采用了ECC加密算法,则第二解密方式采用对应的ECC解密算法;当第二加密方式采用了RSA加密算法,则第二解密方式采用对应的RSA解密算法。

[0074] 在一个实施例中,轮毂锁采用AES解密算法对第二密文进行解密,具体可以是采用AES128解密算法。轮毂锁将回复挑战指令中携带的第二密文作为密文C,将预设数据作为密钥K,轮毂锁采用AES128解密函数对第二密文进行解密处理,也就是根据公式P＝D(K,C),从而得到对应的数据,轮毂锁将所得到的数据作为结果数据。其中,解密函数具体可以是aes_decrypt_pkcs7。

[0075] S210,当结果数据满足开锁条件时,执行与开锁指令相应的开锁操作。

[0076] 其中,开锁条件是轮毂锁执行开锁操作的前提,具体可以是轮毂锁得到的与第二次解密对应的结果数据与预设数据是相同的数据。具体地,当轮毂锁进行第二次解密得到的结果数据与本地生成的预设数据是相同的数据时,表示通信设备挑战成功,因而轮毂锁可执行开锁动作。

[0077] 在一个实施例中,步骤S210,也就是当结果数据满足开锁条件时,执行与开锁指令相应的开锁操作的步骤,具体包括:当结果数据与预设数据为相同数据时,向通信设备反馈表示挑战成功的反馈数据;按照开锁指令,在单车上执行开锁操作;将与开锁操作对应的开

锁结果反馈至通信设备。

[0078] 在一个实施例中，当轮毂锁进行第二次解密得到的结果数据与本地生成的预设数据是相同的数据时，表示通信设备挑战成功，因而轮毂锁可向通信设备发送用于表示挑战成功的反馈数据，以使得通信设备可通过查看反馈数据而得到挑战成功的挑战结果。

[0079] 在一个实施例中，当轮毂锁向通信设备发送用于表示挑战成功的反馈数据之后，轮毂锁在所在的单车上执行与开锁指令相应的开锁操作。当轮毂锁执行开锁操作之后，将对应的开锁结果发送至通信设备，以使得通信设备可通过查看开锁结果而得到单车处于已解锁状态。

[0080] 上述实施例中，当轮毂锁得到的结果数据与预设数据为相同数据时，将表示挑战成功的反馈数据发送至通信设备，同时轮毂锁执行开锁操作并将开锁结果发送至通信设备。通过这样的方式，通信设备可以得到单车上的轮毂锁已处于解锁状态，因而用户可以使用已解锁的单车。由于使用隐蔽的轮毂锁而避免了因暴力行为破坏锁体所带来的安全问题，因而提高了单车的安全性。

[0081] 在一个实施例中，当轮毂锁进行第二次解密得到的结果数据与本地生成的预设数据是不同的数据时，表示通信设备挑战失败，因而轮毂锁可向通信设备发送用于表示挑战失败的反馈数据，以使得通信设备可通过查看反馈数据而得到挑战失败的挑战结果。当通信设备挑战失败时，轮毂锁不执行开锁动作。在其中一个实施例中，当通信设备挑战失败时，轮毂锁可触发报警动作，比如震动或鸣叫等，以提示用户开锁失败，或对非正常开锁进行警告。

[0082] 上述单车开锁方法，通过接收安装在单车上的通信设备发送的开锁指令，从而生成相应的发起挑战指令，并发送至单车上的通信设备。接收单车上的通信设备根据发起挑战指令反馈的回复挑战指令，并对回复挑战指令携带的第二密文进行解密处理，得到结果数据，当结果数据满足预设开锁条件时，执行与开锁指令相应的开锁操作。通过这样的方式，对单车进行加密，可避免因暴力行为破坏锁体而带来的安全问题，因而提高了单车的安全性。并且，由于减少了锁体被破坏的风险，也减少了因维修单车上的锁体和通信设备而产生的成本，因而降低了维修成本，大大提高了单车的使用效率。

[0083] 在一个实施例中，步骤S202之前，也就是接收安装在单车上的通信设备发送的开锁指令的步骤之前，该单车开锁方法还包括发送配置信息的步骤，该发送配置信息的步骤具体包括：接收安装在单车上的通信设备发送的获取指令；响应于获取指令，将轮毂锁的配置信息反馈至通信设备；反馈的配置信息用于指示通信设备从服务器处获取与配置信息相匹配的预设密钥；预设密钥用于辅助第一解密方式的实施。

[0084] 其中，获取指令是通信设备用于获取轮毂锁中存储的预设密钥的指令。配置信息是与轮毂锁有关的锁信息，比如轮毂锁的版本号和ID(Identity，标识)号等。

[0085] 在一个实施例中，通信设备向轮毂锁发送获取指令，当轮毂锁接收到通信设备发送的获取指令后，轮毂锁响应于该获取指令，从而将自身的版本号和ID号反馈至通信设备。当通信设备接收到轮毂锁反馈的版本号和ID号后，将轮毂锁的版本号和ID号发送至服务器，以使得通信设备从服务器的数据库中获取与该版本号和ID号对应的轮毂锁的预设密钥。

[0086] 在一个实施例中，当通信设备从服务器的数据库中获取与该版本号和ID号对应的

轮毂锁的预设密钥后，通信设备将获取的预设密钥保存至非易失性存储器中，比如通信设备将预设密钥保存至本地的只读存储器中。

[0087] 上述实施例中，轮毂锁根据通信设备发送的获取指令，将配置信息反馈至通信设备，以使得通信设备可从服务器中获取与该配置信息相匹配的预设密钥。通过这样的方式，通信设备可以获取到与轮毂锁相对应的预设密钥，从而可对轮毂锁加密后的数据进行对应的解密处理，使得单车上的通信设备以及轮毂锁之间保持密钥的一致性，从而提高了对单车进行解锁的效率。

[0088] 在一个实施例中，该单车开锁方法还包括存储密钥的步骤，该存储密钥的步骤具体包括：当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥，并进行相应的挑战操作；当挑战操作成功时，将诊断工具设置的设置密钥作为与配置信息对应的预设密钥并存储，并触发诊断工具将预设密钥上报至服务器进行更新存储。

[0089] 其中，诊断工具是用于对轮毂锁的密钥设置情况进行诊断的仪器，具体可以是线下诊断仪。设置密钥是诊断工具设置的密钥。挑战操作是诊断工具和轮毂锁之间的相互操作，具体可以是轮毂锁向诊断工具发起挑战以及诊断工具进行回应挑战等。

[0090] 在一个实施例中，轮毂锁与诊断工具之间采用接口进行通信，具体可以是采用RS-485通信。通过一个RS-485转换器，就可将RS485的接口与轮毂锁内部集成的STM32M0系列单片机的UART串口进行连接。

[0091] 在一个实施例中，诊断工具向轮毂锁发送对应的指令，当轮毂锁接收到诊断工具发送的指令后，轮毂锁响应于接收到的指令，从而将自身的版本号和ID号反馈至诊断工具。当诊断工具接收到轮毂锁反馈的版本号和ID号后，将轮毂锁的版本号和ID号发送至服务器，以使得诊断工具从服务器的数据库中获取与该版本号和ID号对应的轮毂锁的密钥。

[0092] 在一个实施例中，当诊断工具无法从服务器的数据库中获取到与该版本号和ID号对应的轮毂锁的密钥时，也就是服务器返回的是轮毂锁的默认密钥时，表示该轮毂锁未进行出厂设置，也就是该轮毂锁未进行密钥的更新，因而此时，诊断工具将接收的服务器返回的默认密钥存储至本地存储器中。默认密钥比如0x0123456789ABCDEF。其中，出厂设置是将轮毂锁的默认密钥进行更新，使得每个轮毂锁都有对应的预设密钥。

[0093] 在一个实施例中，当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥的步骤，具体包括：当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥所对应的第三密文；第三密文通过默认密钥对设置密钥进行加密得到；将诊断工具设置的设置密钥作为与配置信息对应的预设密钥并存储之前，该单车开锁方法还包括获取设置密钥的步骤，该获取设置密钥的步骤具体包括：当挑战操作成功时，获取默认密钥，并通过默认密钥对第三密文进行解密，得到对应的设置密钥。

[0094] 在一个实施例中，当诊断工具无法从服务器的数据库中获取到与该版本号和ID号对应的轮毂锁的预设密钥时，诊断工具将服务器返回的默认密钥保存在本地存储器中。诊断工具设置一个设置密钥，并将该设置密钥作为待加密的数据，也就是明文P，以默认密钥作为密钥K，诊断工具采用AES128加密函数C＝E(K,P)和默认密钥对作为明文P的设置密钥进行加密处理，得到对应的第三密文。其中，第三密文是通过第三加密方式对设置密钥进行

加密后得到的数据。第三加密方式具体是对诊断工具上的设置密钥进行加密的方式。诊断工具根据加密后的设置密钥，也就是根据第三密文生成设置密钥指令，并将设置密钥指令发送至轮毂锁。

[0095] 在一个实施例中，轮毂锁接收到诊断工具发送的设置密钥指令后，轮毂锁生成随机数，轮毂锁对随机数进行加密，从而生成对应的密文，记为第一调试密文，且生成包括有该第一调试密文的指令，将该指令记为发起挑战调试指令。并将该发起挑战调试指令发送至诊断工具，以使得诊断工具接收到该发起挑战调试指令以进行反馈。

[0096] 在一个实施例中，诊断工具接收轮毂锁发送的发起挑战调试指令，对发起挑战调试指令中的第一调试密文进行解密，诊断工具对第一调试密文进行解密后得到的数据进行再次加密，从而生成对应的密文，记为第二调试密文。且生成包括有第二调试密文的指令，将该指令记为回复挑战调试指令。并将回复挑战调试指令发送至轮毂锁，以使得轮毂锁可以接收到回复挑战调试指令以表示诊断工具接收了挑战。

[0097] 在一个实施例中，当轮毂锁接收到诊断工具发送的回复挑战调试指令之后，对回复挑战调试指令中携带的第二调试密文进行解密，从而得到的数据，记为调试数据。当调试数据与本地生成的随机数是相同数据时，表示诊断工具挑战成功。

[0098] 在一个实施例中，当诊断工具挑战成功时，轮毂锁可向诊断工具发送用于表示挑战成功的数据，以使得通信设备可通过查看所接收的数据而得到挑战成功的挑战结果。

[0099] 在一个实施例中，轮毂锁采用预默认密钥，对接收到的设置密钥指令中携带的第三密文进行解密，从而得到诊断工具设置的设置密钥。轮毂锁将设置密钥作为预设密钥，并将本地存储器上存储的默认密钥更新为预设密钥。

[0100] 在一个实施例中，当轮毂锁将本地存储器上存储的默认密钥更新为预设密钥之后，轮毂锁将对应的密钥更新结果发送至诊断工具，以使得诊断工具可通过查看密钥更新结果而得到轮毂锁中的密钥情况。

[0101] 上述实施例中，当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥所对应的第三密文。以及当诊断工具挑战成功时，轮毂锁通过默认密钥对第三密文解密从而得到对应的设置密钥。通过这样的方式，诊断工具对设置密钥进行加密，从而保证了设置密钥的安全性，从而保障了诊断工具与轮毂锁之间的通信安全。

[0102] 在一个实施例中，诊断工具接收到密钥更新结果以后，将默认密钥更新为设置密钥，并保存至本地存储器中。并且，诊断工具通过网线或者4G网络联入互联网，并将预设密钥上报至服务器，以使得服务器将预设密钥以及对应的轮毂锁的版本号和ID号共同存储至数据库中。

[0103] 上述实施例中，当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥，并进行相应的挑战操作。当挑战操作成功时，诊断工具将设置密钥作为与配置信息对应的预设密钥并存储，并且，诊断工具将预设密钥上报至服务器进行更新存储。通过这样的方式，使得诊断工具对本地存储器中的存储的密钥进行更新，以及服务器中存储的密钥进行更新。这保证了对密钥更新的及时性，以及保证了轮毂锁中存储的密钥与服务器中存储的密钥的一致性，从而大大提高了轮毂锁所在单车的安全性。

[0104] 在一个实施例中，指令是用于指示接收方执行相应操作的命令，具体可以通过通信协议来进行传输。通信协议具体包括六个部分：属性域、命令字段、长度、内容、序列码和CRC32(Cyclic Redundancy Check 32，循环冗余校验)。其中，属性域可以由数字分别表示不同的操作，比如0表示读操作、1表示写操作、2表示控制操以及4表示挑战操作；参考表1，命令字段表示所执行的命令，命令字段的不同ID分别表示不同的含义和属性。比如命令字段ID为0表示读取锁信息；长度域表示传输内容长度，其中，传输内容的长度不包括头尾和长度域本身的长度；内容域表示传输内容，具体可以是以长度域中的数值为长度的实际传输内容；序列码是由数字表示的序列编码，具体可从数字0开始，比如0表示第1条消息序列，数字1表示第2条消息序列，以此类推；CRC32域表示数据的CRC32值，具体可按照算法对数据进行计算而得到CRC32值。

[0105] 表1命令字段及对应的含义和属性表

[0106]

命令字段ID	含义	属性
0	锁信息(版本号，ID等)	只读
1	车速	只读
2	车锁状态	只读
3	读取故障码	只读
4	清除故障码	只写
5	请求开锁	控制
6	请求关锁	控制
7	设置AES密钥	只写
8	升级固件	控制
9	升级包写入	只写
10	挑战请求	挑战
11	挑战回应	挑战
12	挑战结果	挑战

[0107] 参考图3，在一个具体的实施例中，该单车开锁方法还包括出厂设置的步骤，该出厂设置的步骤的时序图包括：线下诊断仪可通过发送指令向轮毂锁获取轮毂锁的版本号和ID号，轮毂锁将对应的版本号和ID号反馈至线下诊断仪。比如，线下诊断发送命令字段为0的指令开获取轮毂锁的版本号和ID号，并且，轮毂锁通过反馈命令字段为0的指令来回复相应的版本号和ID号。线下诊断仪按照接收到的轮毂锁的版本号和ID号发送至服务器，以从服务器中获取对应的轮毂锁的密钥。当线下诊断仪从服务器获取的是轮毂锁的默认密钥时，表示该轮毂锁未进行密钥的更新，此时，线下诊断仪将接收的服务器返回的默认密钥存储至本地存储器中。

[0108] 线下诊断仪设置一个AES密钥，并对该AES密钥进行加密处理，线下诊断仪将加密后的AES密钥发送至轮毂锁。轮毂锁响应接收到的加密的AES密钥，采用默认密钥对生成的随机数进行加密，并将加密的随机数作为传输内容，生成相应指令，比如轮毂锁生成04 0xA的指令发送至线下诊断仪，表示轮毂锁向线下诊断仪发起挑战。线下诊断仪接收到挑战后，采用默认密钥对接收到的指令中所携带的密文进行解密，还原轮毂锁生成的随机数。线下诊断仪将随机数作为密钥，加密自身后得到对应的密文，并生成包含该密文的指令，且将该

指令反馈至轮毂锁。比如线下诊断仪生成04 0xB的指令反馈至轮毂锁。当轮毂锁接收到线下诊断仪发送的指令后，对指令中携带的密文进行解密，从而得到相应的数据。当得到的数据与本地生成的随机数是相同数据时，表示线下诊断仪挑战成功。比如轮毂锁生成04 0xC的指令反馈至线下诊断仪以表示线下诊断仪挑战成功。

[0109] 此时，轮毂锁可向线下诊断仪发送用于表示挑战成功的挑战结果。比如轮毂锁生成命令字段为12、且传输内容为数字1的指令，将该指令反馈至线下诊断仪以表示线下诊断仪挑战成功。并且，轮毂锁采用默认密钥对先前接收到的加密的AES密钥进行解密，从而得到线下诊断仪设置的AES密钥。轮毂锁将AES密钥在本地存储器上进行更新存储。此外，轮毂锁将AES密钥更新成功的结果发送至线下诊断仪，使得线下诊断仪将默认密钥更新为AES密钥，并保存至本地存储器中。并且，线下诊断仪通过网线或者4G网络通信将更新后的AES密钥上报至服务器，以使得服务器对AES密钥实现同步更新。

[0110] 参考图4，在一个具体的实施例中，该单车开锁方法的时序图具体包括：安装在单车上的天线盒向轮毂锁发送开锁请求，比如天线盒向轮毂锁发送命令字段为05的开锁请求指令。轮毂锁响应接收到的开锁请求，采用预设密钥对生成的随机数进行加密，并将加密的随机数作为传输内容，生成相应指令发送至天线盒，表示轮毂锁向天线盒发起挑战。比如轮毂锁生成04 0xA的指令发送至天线盒，表示轮毂锁向天线盒发起挑战。天线盒接收到挑战后，采用预设密钥对接收到的指令中所携带的密文进行解密，还原轮毂锁生成的随机数。天线盒将随机数作为密钥，加密自身后得到对应的密文，并生成包含该密文的指令，且将该指令反馈至轮毂锁。比如天线盒生成04 0xB的指令反馈至轮毂锁。

[0111] 当轮毂锁接收到天线盒发送的指令后，对指令中携带的密文进行解密，从而得到相应的数据。当得到的数据与本地生成的随机数是相同数据时，表示天线盒挑战成功。比如轮毂锁生成04 0xC的指令反馈至天线盒以表示天线盒挑战成功。轮毂锁可向天线盒发送用于表示挑战成功的挑战结果。比如轮毂锁生成命令字段为12、且传输内容为数字1的指令，将该指令反馈至天线盒以表示天线盒挑战成功。轮毂锁执行与开锁请求相应的开锁操作。并且，轮毂锁将开锁成功的开锁结果发送至天线盒，比如轮毂锁向轮毂锁反馈命令字段为05的开锁结果，以使得天线盒接收对应的开锁结果。

[0112] 此外，当轮毂锁对指令中携带的密文进行解密所得到的数据与本地生成的随机数是不同数据时，表示天线盒挑战失败。比如轮毂锁生成命令字段为12、且传输内容为数字0的指令，将该指令反馈至天线盒以表示天线盒挑战失败。此时，轮毂锁可向天线盒发送用于表示挑战失败的挑战结果。

[0113] 参考图5，在一个实施例中，提供了一种单车开锁方法的结构示意图，具体是天线盒和轮毂锁进行接口通信。其中，天线盒包括调制解调器(Modem)、主控芯片和外扩存储器。其中，Modem主要用于把接收到的数字信号转换成可传送的脉冲信号。主控芯片内置的内存储器中或者外扩存储器中可用于存储密钥。轮毂锁的MCU(Microcontroller Unit，微控制单元或者单片机)包括非易失性存储介质，比如FLASH闪存(Flash Memory)。其中，MCU内置的FLASH可用于存储密钥。天线盒与轮毂锁通过串行通信接口相连接，比如通过UART或者I2C实现密钥的传输。

[0114] 应该理解的是，虽然图2-5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2-5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。

[0115] 在一个实施例中，如图6所示，提供了一种单车开锁600装置，包括：接收模块601、加密模块602、解密模块603和执行模块604，其中：

[0116] 接收模块601，用于接收安装在单车上的通信设备发送的开锁指令。

[0117] 加密模块602，用于响应于开锁指令，生成发起挑战指令，并将发起挑战指令发送至通信设备；发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文。

[0118] 接收模块601还用于接收通信设备根据发起挑战指令反馈的回复挑战指令；回复挑战指令携带第二密文、且表征通信设备已接受挑战；第二密文是通信设备按照第一解密方式对第一密文进行解密后，再按照第二加密方式加密得到。

[0119] 解密模块603，用于采用与第二加密方式对应的第二解密方式，对第二密文进行解密，得到结果数据。

[0120] 执行模块604，用于当结果数据满足开锁条件时，执行与开锁指令相应的开锁操作。

[0121] 参考图7，在一个实施例中，该单车开锁600装置还包括获取模块605，用于接收安装在单车上的通信设备发送的获取指令；响应于获取指令，将轮毂锁的配置信息反馈至通信设备；反馈的配置信息用于指示通信设备从服务器处获取与配置信息相匹配的预设密钥；预设密钥用于辅助第一解密方式的实施。

[0122] 在一个实施例中，该单车开锁600装置还包括存储模块606，用于当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥，并进行相应的挑战操作；当挑战操作成功时，将诊断工具设置的设置密钥作为与配置信息对应的预设密钥并存储，并触发诊断工具将预设密钥上报至服务器进行更新存储。

[0123] 在一个实施例中，加密模块602还用于当诊断工具无法从服务器中查找到与轮毂锁的配置信息对应的预设密钥时，接收诊断工具设置的设置密钥所对应的第三密文；第三密文通过默认密钥对设置密钥进行加密得到；解密模块603还用于当挑战操作成功时，获取默认密钥，并通过默认密钥对第三密文进行解密，得到对应的设置密钥。

[0124] 在一个实施例中，加密模块602还用于获取轮毂锁本地存储的预设密钥；通过预设密钥和加密函数，对预设数据进行加密处理得到对应的第一密文。

[0125] 在一个实施例中，加密模块602还用于通信设备获取与轮毂锁对应的预设密钥；通信设备在获取到第一密文后，通过获取的预设密钥和解密函数对第一密文进行解密，得到解密数据；将解密数据同时作为明文和密钥，通过加密函数进行加密处理，得到对应的第二密文。

[0126] 在一个实施例中，执行模块604还用于当结果数据与预设数据为相同数据时，向通信设备反馈表示挑战成功的反馈数据；按照开锁指令，在单车上执行开锁操作；将与开锁操作对应的开锁结果反馈至通信设备。

[0127] 上述单车开锁装置，通过接收安装在单车上的通信设备发送的开锁指令，从而生

成相应的发起挑战指令，并发送至单车上的通信设备。接收单车上的通信设备根据发起挑战指令反馈的回复挑战指令，并对回复挑战指令携带的第二密文进行解密处理，得到结果数据，当结果数据满足预设开锁条件时，执行与开锁指令相应的开锁操作。通过这样的方式，对单车进行加密，可避免因暴力行为破坏锁体而带来的安全问题，因而提高了单车的安全性。并且，由于减少了锁体被破坏的风险，也减少了因维修单车上的锁体和通信设备而产生的成本，因而降低了维修成本，大大提高了单车的使用效率。

[0128] 关于单车开锁装置的具体限定可以参见上文中对于单车开锁方法的限定，在此不再赘述。上述单车开锁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轮毂锁中的处理器中，也可以以软件形式存储于轮毂锁中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0129] 在一个实施例中，提供了一种轮毂锁，该轮毂锁的内部结构图可以如图8所示。该轮毂锁包括单片机、锁头和通信接口。其中，该轮毂锁的单片机用于提供计算和控制能力。该轮毂锁的单片机上包括非易失性存储介质，比如FALSH闪存。该单片机上存储计算机程序。该轮毂锁的通信接口用于与外部的终端进行有线或无线方式的通信，无线方式可通过WIFI(Wireless Fidelity，无线局域网)、运营商网络、NFC(Near Field Communication，近场通信)或其他技术实现。该计算机程序被处理器执行时以实现一种单车开锁方法。

[0130] 本领域技术人员可以理解，图8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轮毂锁的限定，具体的轮毂锁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。

[0131] 在一个实施例中，提供了一种轮毂锁，包括存储器和处理器，存储器存储有计算机程序，计算机程序被处理器执行时，使得处理器执行上述单车开锁方法的步骤。此处单车开锁方法的步骤可以是上述各个实施例的单车开锁方法中的步骤。

[0132] 在一个实施例中，提供了一种计算机可读存储介质，存储有计算机程序，计算机程序被处理器执行时，使得处理器执行上述单车开锁方法的步骤。此处单车开锁方法的步骤可以是上述各个实施例的单车开锁方法中的步骤。

[0133] 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，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，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。

[0134] 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。

[0135] 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。

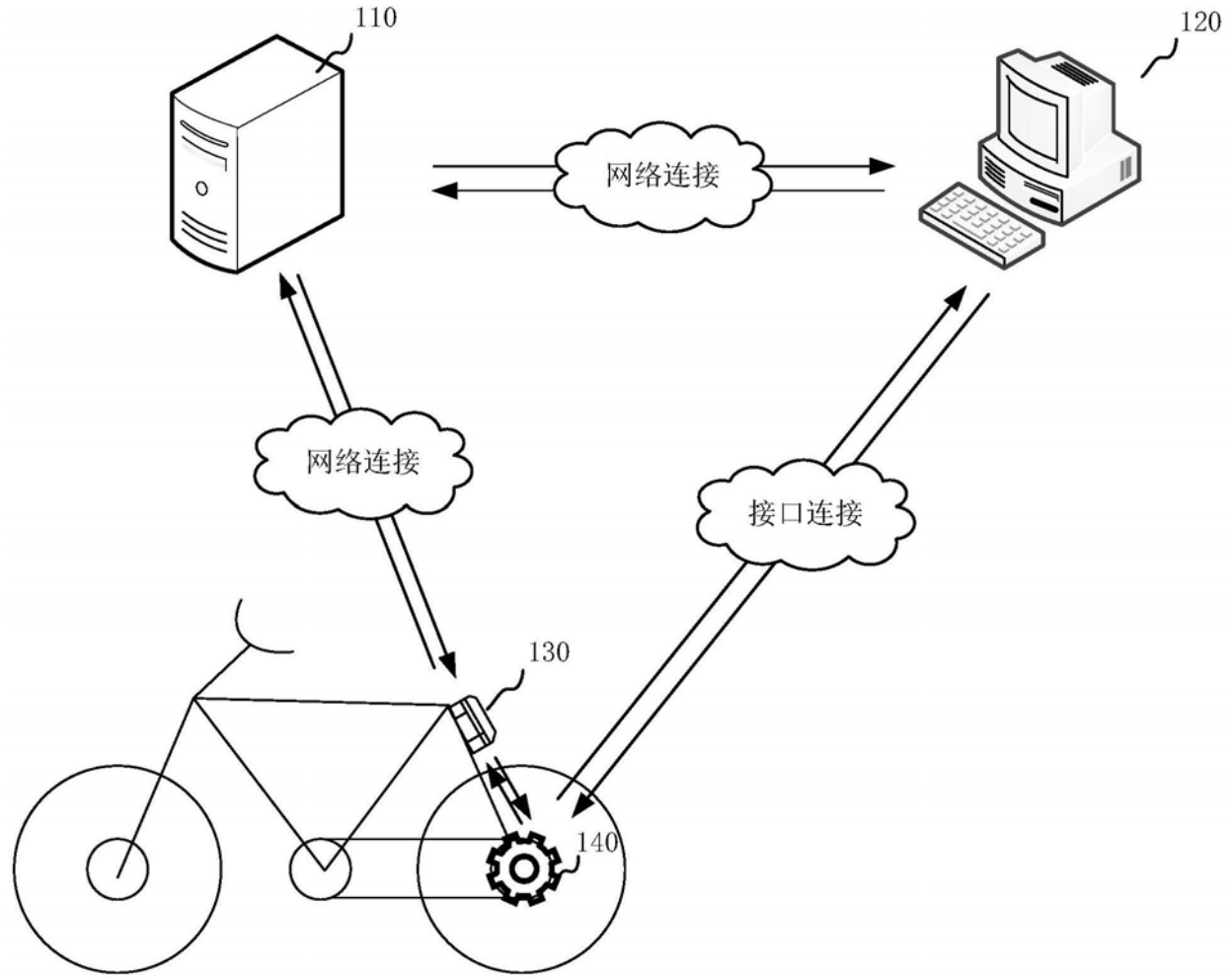


图1

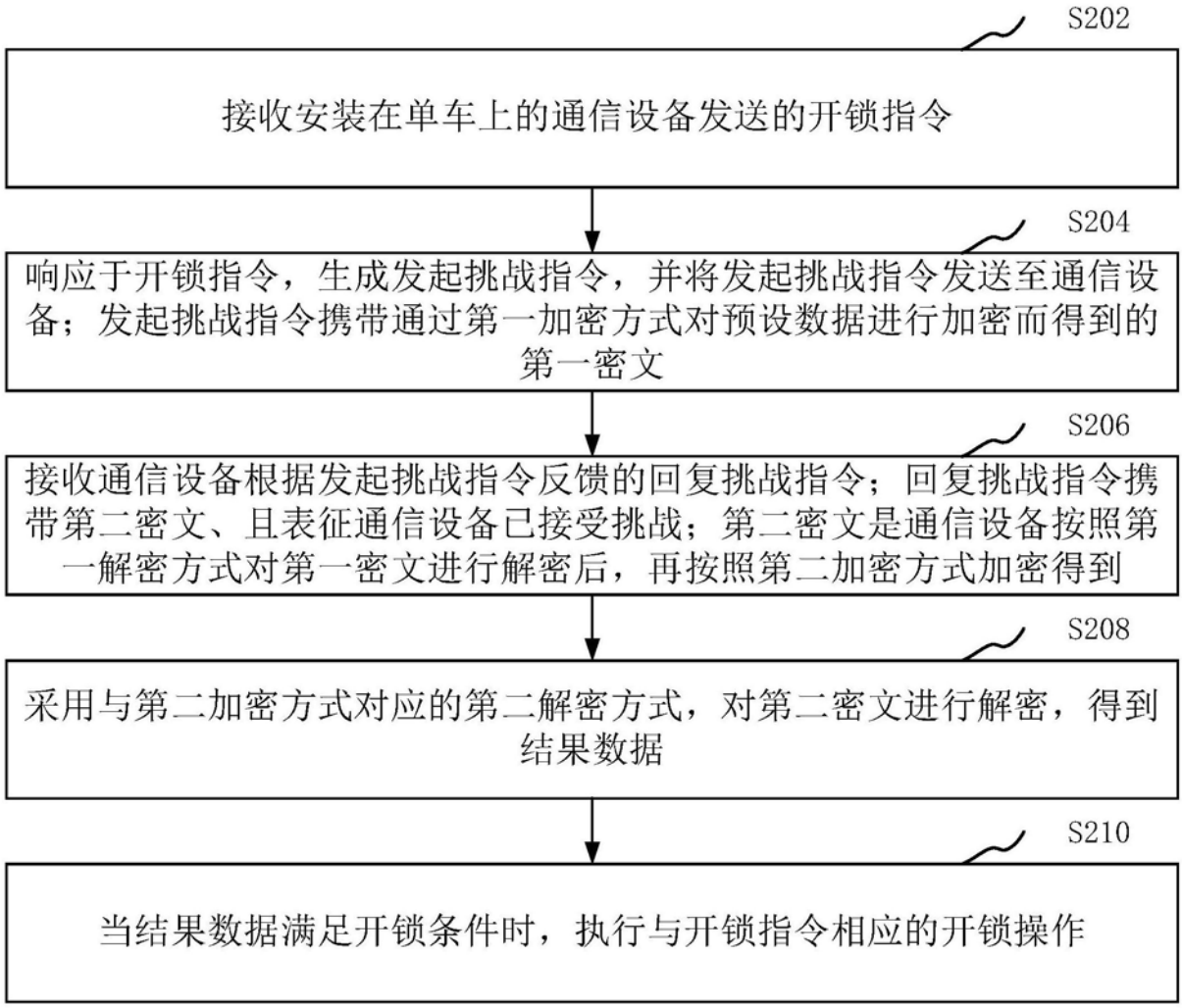

S202
接收安装在单车上的通信设备发送的开锁指令
S204
响应于开锁指令，生成发起挑战指令，并将发起挑战指令发送至通信设备；发起挑战指令携带通过第一加密方式对预设数据进行加密而得到的第一密文
S206
接收通信设备根据发起挑战指令反馈的回复挑战指令；回复挑战指令携带第二密文、且表征通信设备已接受挑战；第二密文是通信设备按照第一解密方式对第一密文进行解密后，再按照第二加密方式加密得到
S208
采用与第二加密方式对应的第二解密方式，对第二密文进行解密，得到结果数据
S210
当结果数据满足开锁条件时，执行与开锁指令相应的开锁操作

图2

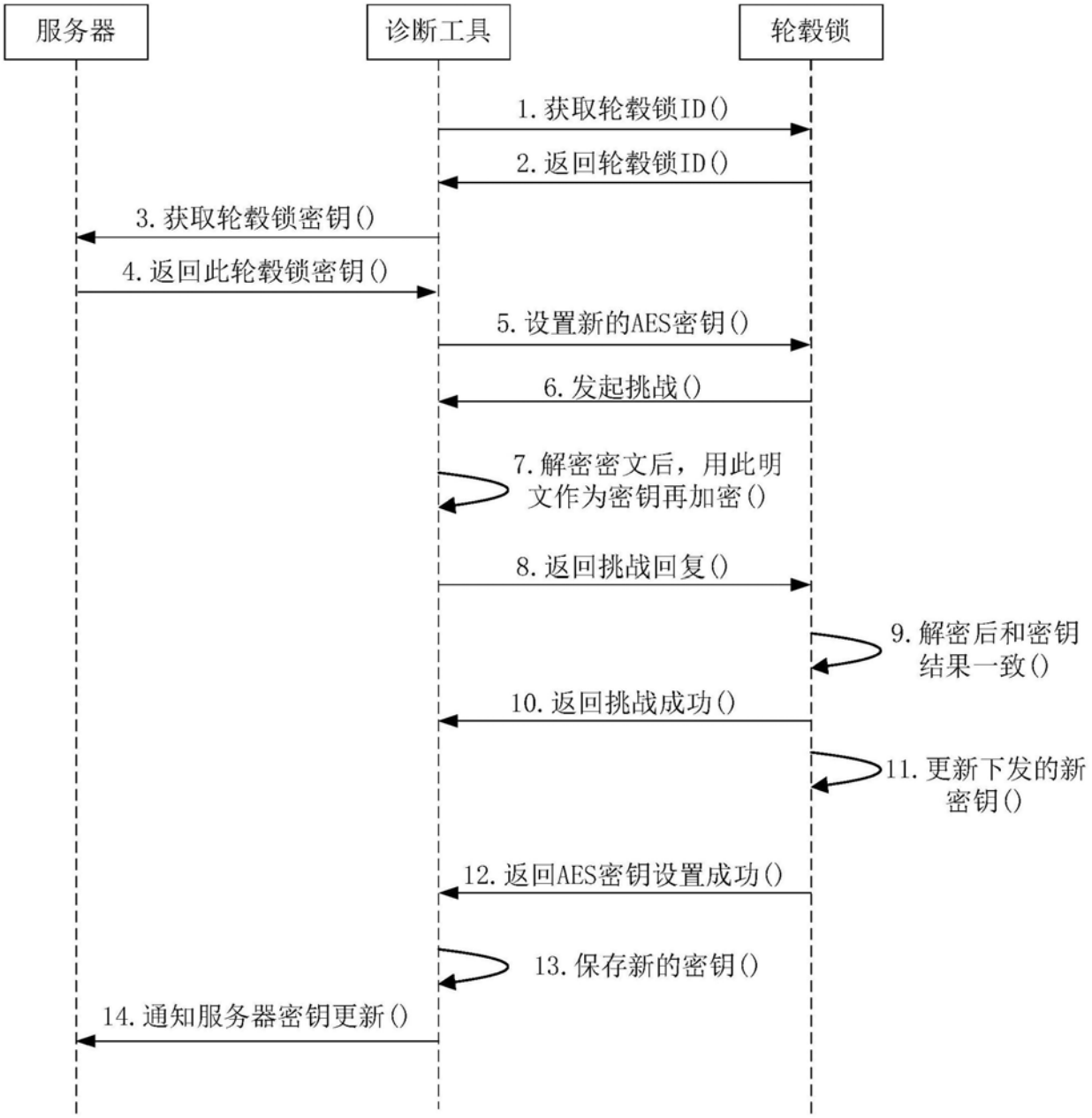

服务器
诊断工具
轮毂锁
1.获取轮毂锁ID()
2.返回轮毂锁ID()
3.获取轮毂锁密钥()
4.返回此轮毂锁密钥()
5.设置新的AES密钥()
6.发起挑战()
7.解密密文后，用此明文作为密钥再加密()
8.返回挑战回复()
9.解密后和密钥结果一致()
10.返回挑战成功()
11.更新下发的新密钥()
12.返回AES密钥设置成功()
13.保存新的密钥()
14.通知服务器密钥更新()

图3

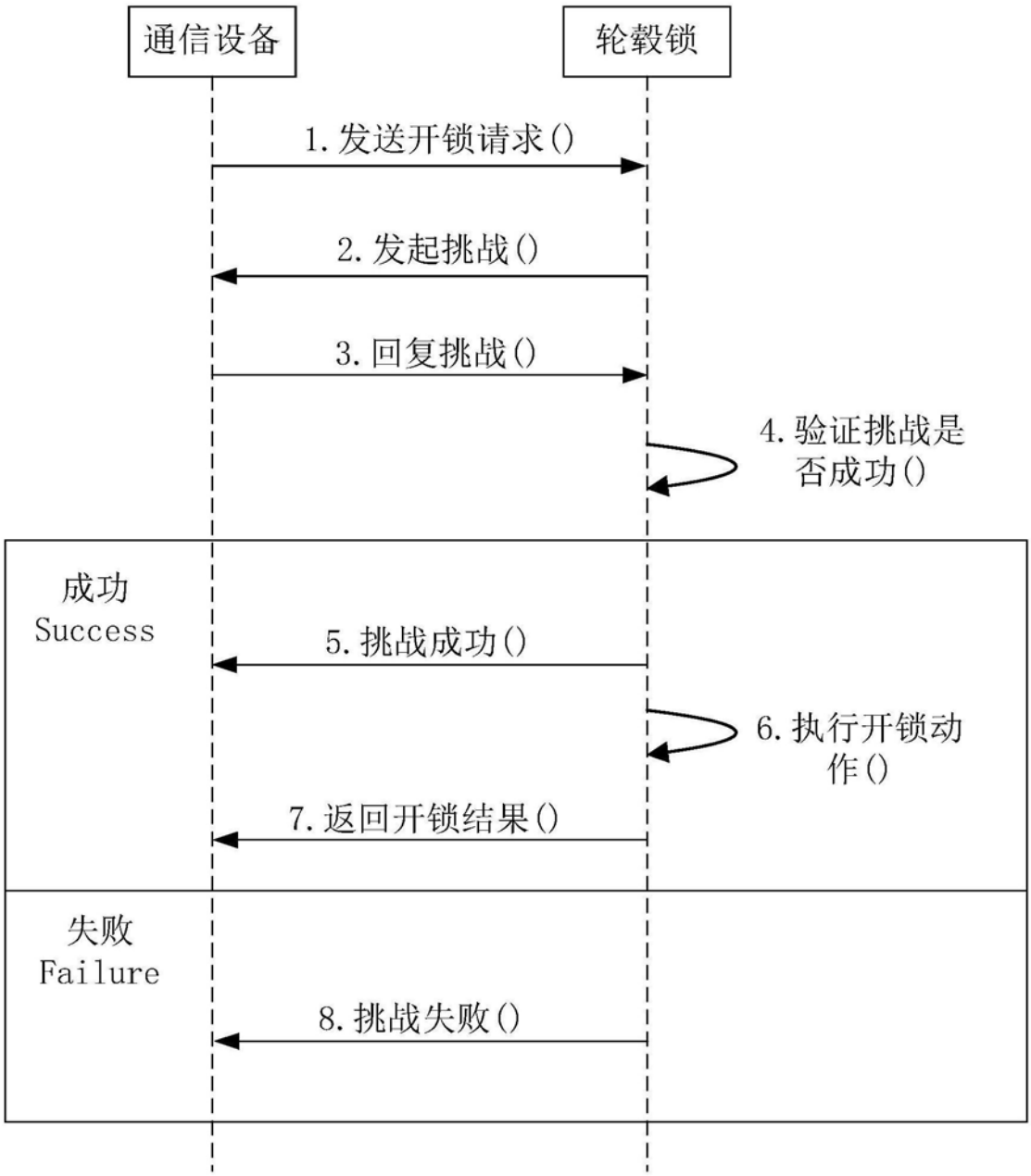

通信设备
轮毂锁
1. 发送开锁请求()
2. 发起挑战()
3. 回复挑战()
4. 验证挑战是否成功()
成功
Success
5. 挑战成功()
6. 执行开锁动作()
7. 返回开锁结果()
失败
Failure
8. 挑战失败()

图4

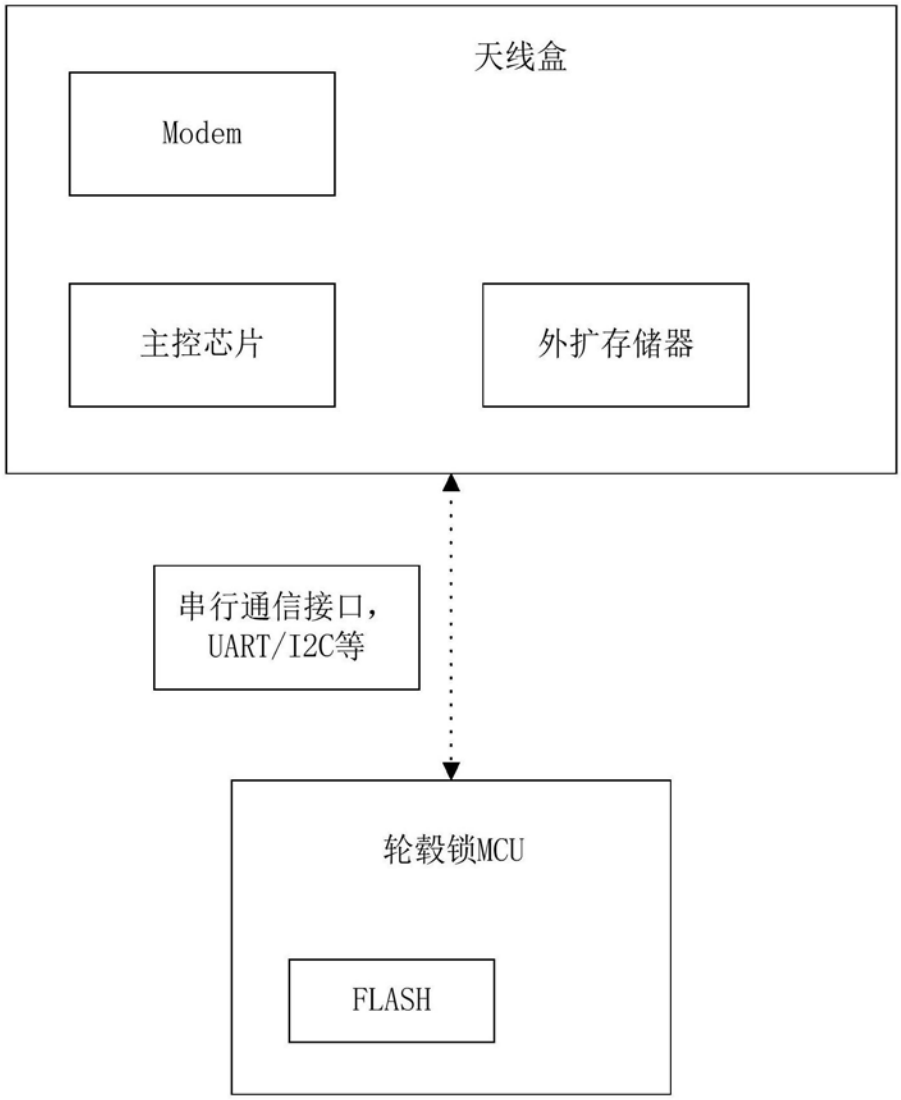

天线盒
Modem
主控芯片
外扩存储器
串行通信接口，
UART/I2C等
轮毂锁MCU
FLASH

图5

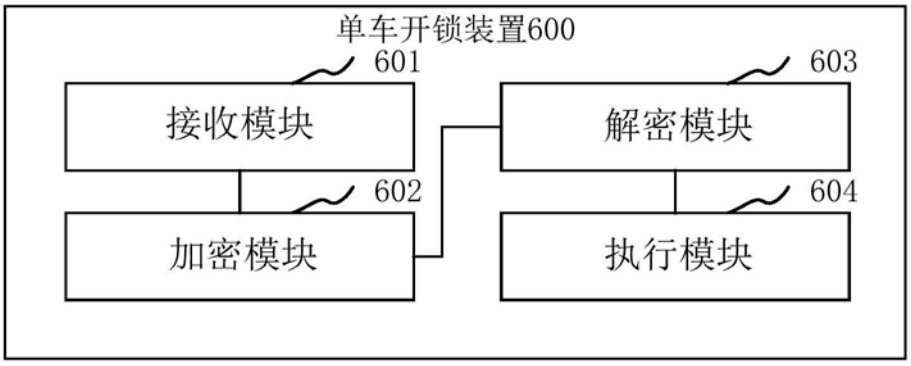

单车开锁装置600
601
接收模块
603
解密模块
602
加密模块
604
执行模块

图6

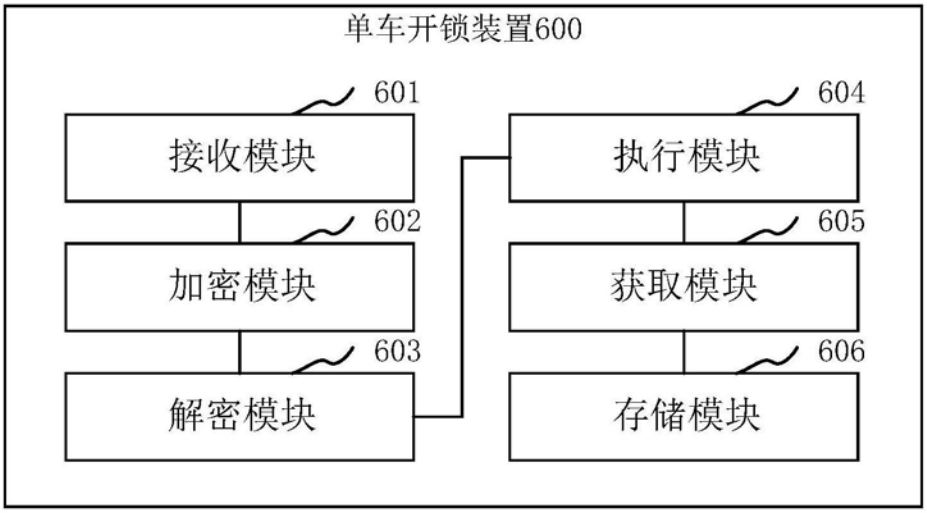

单车开锁装置600
601
接收模块
602
加密模块
603
解密模块
604
执行模块
605
获取模块
606
存储模块

图7

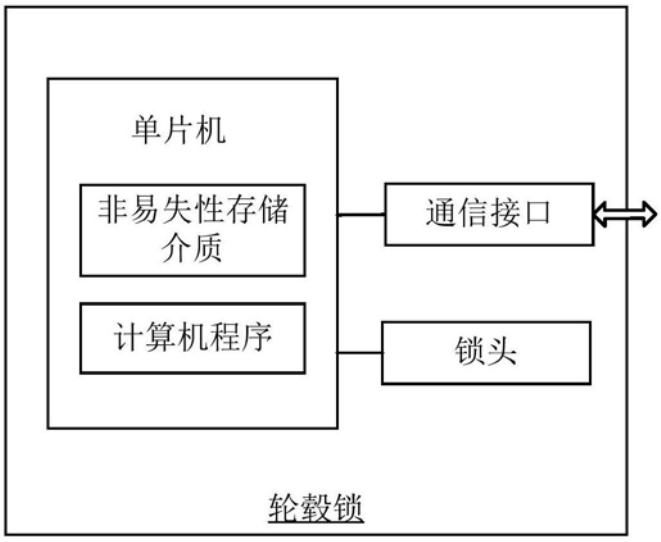

单片机
非易失性存储介质
计算机程序
通信接口
锁头
轮毂锁

图8