(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113554783 B
(45)授权公告日 2023.03.28

(21)申请号 202010270911.1
(22)申请日 2020.04.08
(65)同一申请的已公布的文献号
申请公布号 CN 113554783 A
(43)申请公布日 2021.10.26
(73)专利权人 中国移动通信有限公司研究院
地址 100053 北京市西城区宣武门西大街32号
专利权人 中国移动通信集团有限公司
(72)发明人 谢进柳 黄静
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 王花丽 张颖玲
(51)Int.Cl.
G07C 9/00(2020.01)

(56)对比文件
CN 110610569 A,2019.12.24
CN 110192228 A,2019.08.30
CN 105813069 A,2016.07.27
CN 110766524 A,2020.02.07
CN 109712278 A,2019.05.03
DE 10354517 A1,2005.06.16
US 2005060555 A1,2005.03.17

审查员 蔡瑞

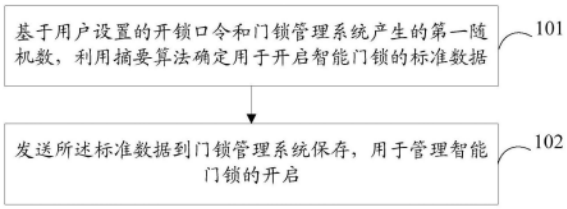
权利要求书3页 说明书14页 附图5页

(54)发明名称

一种认证数据的存储方法、装置和计算机可读存储介质

(57)摘要

本发明实施例提供了一种认证数据的存储方法、装置和计算机可读存储介质，所述方法包括：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。



CN 113554783 B

1.一种认证数据的存储方法,其特征在于,该方法应用于智能门锁,包括:

基于用户设置的开锁口令和门锁管理系统产生的第一随机数,利用摘要算法确定用于开启智能门锁的标准数据;

发送所述标准数据到门锁管理系统保存,用于管理智能门锁的开启;

在开锁过程中,该方法还包括:

将用户输入的开锁口令和第一随机数进行摘要计算,得到第三摘要值;

向门锁管理系统请求所述标准数据;

接收门锁管理系统下发的第二随机数、门锁管理系统的签名,以及第二随机数与标准数据的摘要计算结果;

利用所述第二随机数对所述第三摘要值进行摘要计算,并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较,如果两者相同,则开启门锁。

2.根据权利要求1所述的方法,其特征在于,所述确定用于开启智能门锁的标准数据之前,该方法还包括:

基于智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数,与所述门锁管理系统进行相互身份验证。

3.根据权利要求2所述的方法,其特征在于,所述与所述门锁管理系统进行相互身份验证之前,该方法还包括:

接收用户通过输入设备输入的开锁口令和所述第一随机数;其中,所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

4.根据权利要求1所述的方法,其特征在于,所述基于用户设置的开锁口令和门锁管理系统产生的第一随机数,利用摘要算法确定用于开启智能门锁的标准数据,包括:

将用户设置的开锁口令进行摘要计算,得到第一摘要值;

再将所述第一摘要值和所述第一随机数进行摘要计算,得到第二摘要值;其中,所述第二摘要值为所述用于开启智能门锁的标准数据。

5.根据权利要求4所述的方法,其特征在于,所述发送所述标准数据到门锁管理系统保存时,该方法还包括:

将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统,用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

6.根据权利要求2所述的方法,其特征在于,所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数,与所述门锁管理系统进行相互身份验证,包括:

将所述智能门锁标识和所述第一随机数进行摘要计算,并将计算结果和所述智能门锁标识发送到门锁管理系统;

在门锁管理系统确定所述智能门锁身份验证通过后,接收门锁管理系统发送的签名;

将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较,如果两者相同,则确认所述门锁管理系统身份验证通过。

7.一种认证数据的存储方法,其特征在于,该方法应用于门锁管理系统,包括:

接收智能门锁发送的标准数据;其中,所述标准数据为:智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的;

保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启；

在开锁过程中，该方法还包括：

接收智能门锁发送的对标准数据的请求；

将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

8.根据权利要求7所述的方法，其特征在于，所述接收智能门锁发送的标准数据之前，该方法还包括：

基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

9.根据权利要求8所述的方法，其特征在于，所述与所述智能门锁进行相互身份验证之前，该方法还包括：

产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；

将所述第一随机数通过短信或网页的通信方式传递给用户。

10.根据权利要求7所述的方法，其特征在于，所述接收智能门锁发送的标准数据时，该方法还包括：

接收第一摘要值以及智能门锁标识；其中，

所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

11.根据权利要求10所述的方法，其特征在于，所述保存所述标准数据与智能门锁标识的对应关系，包括：

对所述第一摘要值和所述第一随机数进行摘要计算；

将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

删除已保存的所述第一随机数。

12.根据权利要求8所述的方法，其特征在于，所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证，包括：

接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

13.一种认证数据的存储装置，其特征在于，该装置应用于智能门锁，包括：

确定模块，用于基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

发送模块，用于发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启；

在开锁过程中，所述确定模块，还用于将用户输入的开锁口令和第一随机数进行摘要计算，得到第三摘要值；

所述发送模块，还用于向门锁管理系统请求所述标准数据；

所述确定模块，还用于接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

14.一种认证数据的存储装置，其特征在于，该装置应用于门锁管理系统，包括：

接收模块，用于接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

存储模块，用于保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启；

在开锁过程中，所述接收模块，还用于接收智能门锁发送的对标准数据的请求；

所述存储模块，还用于将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

15.一种认证数据的存储装置，其特征在于，该装置包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

其中，所述处理器用于运行所述计算机程序时，执行权利要求1-6中任一项所述方法的步骤、或执行权利要求7-12中任一项所述方法的步骤。

16.一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，该计算机程序被处理器执行时实现权利要求1-6中任一项所述方法的步骤、或实现权利要求7-12中任一项所述方法的步骤。

一种认证数据的存储方法、装置和计算机可读存储介质

技术领域

[0001] 本发明涉及移动通信技术领域，尤其涉及一种认证数据的存储方法、装置和计算机可读存储介质。

背景技术

[0002] 目前市面上大部分智能门锁的敏感数据，如用户密码、用户生物数据等都直接存储在智能门锁中，一旦被泄露，极易导致人身、设备、财产受到损害。相关敏感数据安全存储方式主要有以下几种方式：一、将敏感数据存储在安全模块(SE)中，提高了敏感数据存储的安全性；二、在操作系统层面构建访问控制模块，通过访问控制模块设计文件访问控制权限，保证存储的敏感数据不能被任意读取。

[0003] 但以上几种方式存在需要改造硬件导致成本高或在门锁内存储密码根导致安全性不高的问题，无法保证敏感数据(用户设置的开锁口令)的安全。

发明内容

[0004] 有鉴于此，本发明实施例期望提供一种认证数据的存储方法、装置和计算机可读存储介质。

[0005] 为达到上述目的，本发明实施例的技术方案是这样实现的：

[0006] 本发明实施例提供了一种认证数据的存储方法，该方法应用于智能门锁，包括：

[0007] 基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

[0008] 发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。

[0009] 可选的，所述确定用于开启智能门锁的标准数据之前，该方法还包括：

[0010] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证。

[0011] 可选的，所述与所述门锁管理系统进行相互身份验证之前，该方法还包括：

[0012] 接收用户通过输入设备输入的开锁口令和所述第一随机数；其中，所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

[0013] 其中，所述基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据，包括：

[0014] 将用户设置的开锁口令进行摘要计算，得到第一摘要值；

[0015] 再将所述第一摘要值和所述第一随机数进行摘要计算，得到第二摘要值；其中，所述第二摘要值为所述用于开启智能门锁的标准数据。

[0016] 可选的，所述发送所述标准数据到门锁管理系统保存时，该方法还包括：

[0017] 将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统，用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

[0018] 其中，所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生

的第一随机数，与所述门锁管理系统进行相互身份验证，包括：

[0019] 将所述智能门锁标识和所述第一随机数进行摘要计算，并将计算结果和所述智能门锁标识发送到门锁管理系统；

[0020] 在门锁管理系统确定所述智能门锁身份验证通过后，接收门锁管理系统发送的签名；

[0021] 将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较，如果两者相同，则确认所述门锁管理系统身份验证通过。

[0022] 可选的，在开锁过程中，该方法还包括：

[0023] 将用户输入的开锁口令和第一随机数进行摘要计算，得到第三摘要值；

[0024] 向门锁管理系统请求所述标准数据；

[0025] 接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；

[0026] 利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

[0027] 本发明实施例还提供了一种认证数据的存储方法，该方法应用于门锁管理系统，包括：

[0028] 接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0029] 保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0030] 可选的，所述接收智能门锁发送的标准数据之前，该方法还包括：

[0031] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

[0032] 可选的，所述与所述智能门锁进行相互身份验证之前，该方法还包括：

[0033] 产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；

[0034] 将所述第一随机数通过短信或网页的通信方式传递给用户。

[0035] 可选的，所述接收智能门锁发送的标准数据时，该方法还包括：

[0036] 接收第一摘要值以及智能门锁标识；其中，

[0037] 所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

[0038] 其中，所述保存所述标准数据与智能门锁标识的对应关系，包括：

[0039] 对所述第一摘要值和所述第一随机数进行摘要计算；

[0040] 将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

[0041] 删除已保存的所述第一随机数。

[0042] 其中，所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证，包括：

[0043] 接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

[0044] 将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

[0045] 如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

[0046] 可选的，在开锁过程中，该方法还包括：

[0047] 接收智能门锁发送的对标准数据的请求；

[0048] 将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

[0049] 所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

[0050] 所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

[0051] 本发明实施例还提供了一种认证数据的存储装置，该装置应用于智能门锁，包括：

[0052] 确定模块，用于基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

[0053] 发送模块，用于发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。

[0054] 本发明实施例还提供了一种认证数据的存储装置，该装置应用于门锁管理系统，包括：

[0055] 接收模块，用于接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0056] 存储模块，用于保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0057] 本发明实施例还提供了一种认证数据的存储装置，该装置包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

[0058] 其中，所述处理器用于运行所述计算机程序时，执行上述方法的步骤。

[0059] 本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述方法的步骤。

[0060] 本发明实施例提供的认证数据的存储方法、装置和计算机可读存储介质，智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。本发明实施例在用户设置开锁口令后，基于第一随机数和摘要算法实现数据传递的防篡改、防重放，保证了标准数据的安全性。此外，用户口令以摘要值的形式存储在门锁管理系统，确保开锁口令不被门锁管理系统识别，避免用户的开锁口令暴露在网络上，有效提高了验证的安全性，且不需要对硬件进行改造。

[0061] 此外，本发明实施例还在存储标准数据前进行智能门锁与门锁管理系统的相互身份验证，保证标准数据保存在正确的门锁管理系统中。

附图说明

[0062] 图1为本发明实施例所述认证数据的存储方法流程示意图一；

[0063] 图2为本发明实施例所述认证数据的存储方法流程示意图二；

[0064] 图3为本发明实施例所述认证数据的存储装置结构示意图一；

[0065] 图4为本发明实施例所述认证数据的存储装置结构示意图二；

[0066] 图5为本发明实施例所述认证数据的存储装置结构示意图三；

[0067] 图6为本发明实施例所述认证数据的存储装置结构示意图四；

[0068] 图7为本发明实施例所述开锁认证模型示意图；

[0069] 图8为本发明实施例所述开锁场景示意图；

[0070] 图9为本发明实施例所述用户设置的开锁口令的存储流程示意图；

[0071] 图10为本发明实施例所述用户开锁流程示意图。

具体实施方式

[0072] 下面结合附图和实施例对本发明进行描述。

[0073] 本发明实施例提供了一种认证数据的存储方法，如图1所示，该方法应用于智能门锁，包括：

[0074] 步骤101：基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

[0075] 步骤102：发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。

[0076] 本发明实施例在用户设置开锁口令后，基于第一随机数和摘要算法实现数据传递的防篡改、防重放，保证了标准数据的安全性。此外，用户口令以摘要值的形式存储在门锁管理系统，确保开锁口令不被门锁管理系统识别，避免用户的开锁口令暴露在网络上，有效提高了验证的安全性，且不需要对硬件进行改造。

[0077] 一个实施例中，所述确定用于开启智能门锁的标准数据之前，该方法还包括：

[0078] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证。

[0079] 这样，可保证标准数据保存在正确的门锁管理系统中，进一步提高安全性。

[0080] 一个实施例中，所述与所述门锁管理系统进行相互身份验证之前，该方法还包括：

[0081] 接收用户通过输入设备输入的开锁口令和所述第一随机数；其中，所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

[0082] 这样，所述第一随机数不通过智能门锁与门锁管理系统的通信通道进行传递，可保证随机数的传输安全。

[0083] 本发明实施例中，所述基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据，包括：

[0084] 将用户设置的开锁口令进行摘要计算，得到第一摘要值；

[0085] 再将所述第一摘要值和所述第一随机数进行摘要计算，得到第二摘要值；其中，所述第二摘要值为所述用于开启智能门锁的标准数据。

[0086] 这里，利用摘要算法的单向特性，用户设置的开锁口令经随机数加扰再进行摘要运算，实现数据传递的机密性和防篡改、防重放。

[0087] 一个实施例中，所述发送所述标准数据到门锁管理系统保存时，该方法还包括：

[0088] 将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统，用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

[0089] 本发明实施例中，所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证，包括：

[0090] 将所述智能门锁标识和所述第一随机数进行摘要计算，并将计算结果和所述智能门锁标识发送到门锁管理系统；

[0091] 在门锁管理系统确定所述智能门锁身份验证通过后，接收门锁管理系统发送的签名；

[0092] 将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较，如果两者相同，则确认所述门锁管理系统身份验证通过。

[0093] 一个实施例中，在开锁过程中，该方法还包括：

[0094] 将用户输入的开锁口令和第一随机数进行摘要计算，得到第三摘要值；

[0095] 向门锁管理系统请求所述标准数据；

[0096] 接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；

[0097] 利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

[0098] 这里，在开锁过程中对比校准数据经第二随机数加扰后的摘要值，如此，每次开锁的钥匙一次一变(每次产生的第二随机数都不同)，即使门锁管理系统的私钥被泄露，也可以保障开锁的安全。

[0099] 本发明实施例中，用户输入(开锁时)或设置(存储时)用户开锁口令后，快速在内存中进行摘要运算，此后全部操作中都没有明文暴露过用户开锁口令，安全性高。

[0100] 本发明实施例还提供了一种认证数据的存储方法，如图2所示，该方法应用于门锁管理系统，包括：

[0101] 步骤201：接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0102] 步骤202：保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0103] 一个实施例中，所述接收智能门锁发送的标准数据之前，该方法还包括：

[0104] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

[0105] 一个实施例中，所述与所述智能门锁进行相互身份验证之前，该方法还包括：

[0106] 产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；

[0107] 将所述第一随机数通过短信或网页的通信方式传递给用户。

[0108] 一个实施例中，所述接收智能门锁发送的标准数据时，该方法还包括：

[0109] 接收第一摘要值以及智能门锁标识；其中，

[0110] 所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

[0111] 本发明实施例中，所述保存所述标准数据与智能门锁标识的对应关系，包括：

[0112] 对所述第一摘要值和所述第一随机数进行摘要计算；

[0113] 将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

[0114] 删除已保存的所述第一随机数。

[0115] 这里，用户设置的开锁口令与第一随机数的摘要值存储在门锁管理系统中，由于所述标准数据存储结束后，不再保存所述第一随机数，确保攻击者即使可控制门锁管理系统，也无法伪造标准数据，无法达到伪造开锁数据的目的。

[0116] 本发明实施例中，所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证，包括：

[0117] 接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

[0118] 将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

[0119] 如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

[0120] 一个实施例中，在开锁过程中，该方法还包括：

[0121] 接收智能门锁发送的对标准数据的请求；

[0122] 将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

[0123] 所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

[0124] 所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

[0125] 这里，在开锁过程中对比校准数据经第二随机数加扰后的摘要值，如此，每次开锁的钥匙一次一变(每次产生的第二随机数都不同)，即使门锁管理系统的私钥被泄露，也可以保障开锁的安全。

[0126] 本发明实施例还提供了一种认证数据的存储装置，如图3所示，该装置应用于智能门锁，包括：

[0127] 确定模块301，用于基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

[0128] 发送模块302，用于发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。

[0129] 一个实施例中，如图4所示，该装置还包括：第一验证模块303；

[0130] 所述确定模块301确定用于开启智能门锁的标准数据之前，所述第一验证模块303，用于基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证。

[0131] 一个实施例中，所述确定模块301与所述门锁管理系统进行相互身份验证之前，

[0132] 所述确定模块301，还用于接收用户通过输入设备输入的开锁口令和所述第一随机数；其中，所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

[0133] 这样，所述第一随机数不通过智能门锁与门锁管理系统的通信通道进行传递，可保证随机数的传输安全。

[0134] 本发明实施例中，所述确定模块301基于用户设置的开锁口令和门锁管理系统产

生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据，包括：

[0135] 将用户设置的开锁口令进行摘要计算，得到第一摘要值；

[0136] 再将所述第一摘要值和所述第一随机数进行摘要计算，得到第二摘要值；其中，所述第二摘要值为所述用于开启智能门锁的标准数据。

[0137] 这里，利用摘要算法的单向特性，用户设置的开锁口令经随机数加扰再进行摘要运算，实现数据传递的机密性和防篡改、防重放。

[0138] 一个实施例中，所述发送模块302发送所述标准数据到门锁管理系统保存时，还用于将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统，用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

[0139] 本发明实施例中，所述第一验证模块303基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证，包括：

[0140] 将所述智能门锁标识和所述第一随机数进行摘要计算，并将计算结果和所述智能门锁标识发送到门锁管理系统；

[0141] 在门锁管理系统确定所述智能门锁身份验证通过后，接收门锁管理系统发送的签名；

[0142] 将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较，如果两者相同，则确认所述门锁管理系统身份验证通过。

[0143] 一个实施例中，在开锁过程中，

[0144] 所述确定模块301，还用于将用户输入的开锁口令和第一随机数进行摘要计算，得到第三摘要值；

[0145] 所述发送模块302，还用于向门锁管理系统请求所述标准数据；

[0146] 所述确定模块301，还用于接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

[0147] 这里，在开锁过程中对比校准数据经第二随机数加扰后的摘要值，如此，每次开锁的钥匙一次一变(每次产生的第二随机数都不同)，即使门锁管理系统的私钥被泄露，也可以保障开锁的安全。

[0148] 本发明实施例还提供了一种认证数据的存储装置，如图5所示，该装置应用于门锁管理系统，包括：

[0149] 接收模块501，用于接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0150] 存储模块502，用于保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0151] 一个实施例中，如图6所示，该装置还包括：第二验证模块503；

[0152] 所述接收模块501接收智能门锁发送的标准数据之前，

[0153] 所述第二验证模块503，用于基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

[0154] 一个实施例中，所述第二验证模块503与所述智能门锁进行相互身份验证之前，

[0155] 所述存储模块502，还用于产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；将所述第一随机数通过短信或网页的通信方式传递给用户。

[0156] 一个实施例中，所述接收模块501接收智能门锁发送的标准数据时，还用于接收第一摘要值以及智能门锁标识；其中，

[0157] 所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

[0158] 本发明实施例中，所述存储模块502保存所述标准数据与智能门锁标识的对应关系，包括：

[0159] 对所述第一摘要值和所述第一随机数进行摘要计算；

[0160] 将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

[0161] 删除已保存的所述第一随机数。

[0162] 这里，用户设置的开锁口令与第一随机数的摘要值存储在门锁管理系统中，由于所述标准数据存储结束后，不再保存所述第一随机数，确保攻击者即使可控制门锁管理系统，也无法伪造标准数据，无法达到伪造开锁数据的目的。

[0163] 本发明实施例中，所述第二验证模块503基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证，包括：

[0164] 接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

[0165] 将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

[0166] 如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

[0167] 一个实施例中，在开锁过程中，

[0168] 所述接收模块501，还用于接收智能门锁发送的对标准数据的请求；

[0169] 所述存储模块502，还用于将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

[0170] 所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

[0171] 所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

[0172] 这里，在开锁过程中对比校准数据经第二随机数加扰后的摘要值，如此，每次开锁的钥匙一次一变(每次产生的第二随机数都不同)，即使门锁管理系统的私钥被泄露，也可以保障开锁的安全。

[0173] 本发明实施例还提供了一种认证数据的存储装置，该装置包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

[0174] 其中，所述处理器用于运行所述计算机程序时，执行：

[0175] 基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据；

[0176] 发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启。

[0177] 所述确定用于开启智能门锁的标准数据之前，所述处理器还用于运行所述计算机程序时，执行：

[0178] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证。

[0179] 所述与所述门锁管理系统进行相互身份验证之前，所述处理器还用于运行所述计算机程序时，执行：

[0180] 接收用户通过输入设备输入的开锁口令和所述第一随机数；其中，所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

[0181] 所述基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据时，所述处理器还用于运行所述计算机程序时，执行：

[0182] 将用户设置的开锁口令进行摘要计算，得到第一摘要值；

[0183] 再将所述第一摘要值和所述第一随机数进行摘要计算，得到第二摘要值；其中，所述第二摘要值为所述用于开启智能门锁的标准数据。

[0184] 所述发送所述标准数据到门锁管理系统保存时，所述处理器还用于运行所述计算机程序时，执行：

[0185] 将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统，用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

[0186] 所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述门锁管理系统进行相互身份验证时，所述处理器还用于运行所述计算机程序时，执行：

[0187] 将所述智能门锁标识和所述第一随机数进行摘要计算，并将计算结果和所述智能门锁标识发送到门锁管理系统；

[0188] 在门锁管理系统确定所述智能门锁身份验证通过后，接收门锁管理系统发送的签名；

[0189] 将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较，如果两者相同，则确认所述门锁管理系统身份验证通过。

[0190] 在开锁过程中，所述处理器还用于运行所述计算机程序时，执行：

[0191] 将用户输入的开锁口令和第一随机数进行摘要计算，得到第三摘要值；

[0192] 向门锁管理系统请求所述标准数据；

[0193] 接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；

[0194] 利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

[0195] 本发明实施例还提供了一种认证数据的存储装置，该装置包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

[0196] 其中，所述处理器用于运行所述计算机程序时，执行：

[0197] 接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0198] 保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0199] 所述接收智能门锁发送的标准数据之前，所述处理器还用于运行所述计算机程序时，执行：

[0200] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

[0201] 所述与所述智能门锁进行相互身份验证之前，所述处理器还用于运行所述计算机程序时，执行：

[0202] 产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；

[0203] 将所述第一随机数通过短信或网页的通信方式传递给用户。

[0204] 所述接收智能门锁发送的标准数据时，所述处理器还用于运行所述计算机程序时，执行：

[0205] 接收第一摘要值以及智能门锁标识；其中，

[0206] 所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

[0207] 所述保存所述标准数据与智能门锁标识的对应关系，所述处理器还用于运行所述计算机程序时，执行：

[0208] 对所述第一摘要值和所述第一随机数进行摘要计算；

[0209] 将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

[0210] 删除已保存的所述第一随机数。

[0211] 所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证时，所述处理器还用于运行所述计算机程序时，执行：

[0212] 接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

[0213] 将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

[0214] 如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

[0215] 在开锁过程中，所述处理器还用于运行所述计算机程序时，执行：

[0216] 接收智能门锁发送的对标准数据的请求；

[0217] 将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

[0218] 所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第三摘要值进行摘要计算的结果进行比较来确定是否开启门锁；其中，

[0219] 所述第三摘要值为：智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

[0220] 需要说明的是：上述实施例提供的装置在进行认证数据的存储时，仅以上述各程序模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的程序模块完成，即将设备的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的装置与相应方法实施例属于同一构思，其具体实现过程详见

方法实施例,这里不再赘述。

[0221] 在示例性实施例中,本发明实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质可以是FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器;也可以是包括上述存储器之一或任意组合的各种设备,如移动电话、计算机、平板设备、个人数字助理等。

[0222] 本发明实施例还提供了一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时,执行:

[0223] 基于用户设置的开锁口令和门锁管理系统产生的第一随机数,利用摘要算法确定用于开启智能门锁的标准数据;

[0224] 发送所述标准数据到门锁管理系统保存,用于管理智能门锁的开启。

[0225] 所述确定用于开启智能门锁的标准数据之前,所述计算机程序被处理器运行时,还执行:

[0226] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数,与所述门锁管理系统进行相互身份验证。

[0227] 所述与所述门锁管理系统进行相互身份验证之前,所述计算机程序被处理器运行时,还执行:

[0228] 接收用户通过输入设备输入的开锁口令和所述第一随机数;其中,所述第一随机数为门锁管理系统通过短信或网页的通信方式传递给用户。

[0229] 所述基于用户设置的开锁口令和门锁管理系统产生的第一随机数,利用摘要算法确定用于开启智能门锁的标准数据时,所述计算机程序被处理器运行时,还执行:

[0230] 将用户设置的开锁口令进行摘要计算,得到第一摘要值;

[0231] 再将所述第一摘要值和所述第一随机数进行摘要计算,得到第二摘要值;其中,所述第二摘要值为所述用于开启智能门锁的标准数据。

[0232] 所述发送所述标准数据到门锁管理系统保存时,所述计算机程序被处理器运行时,还执行:

[0233] 将所述第一摘要值以及智能门锁标识发送到所述门锁管理系统,用于所述门锁管理系统确定智能门锁发送的标准数据是否有效。

[0234] 所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数,与所述门锁管理系统进行相互身份验证时,所述计算机程序被处理器运行时,还执行:

[0235] 将所述智能门锁标识和所述第一随机数进行摘要计算,并将计算结果和所述智能门锁标识发送到门锁管理系统;

[0236] 在门锁管理系统确定所述智能门锁身份验证通过后,接收门锁管理系统发送的签名;

[0237] 将所述签名与智能门锁已保存的门锁管理系统的证书中的签名比较,如果两者相同,则确认所述门锁管理系统身份验证通过。

[0238] 在开锁过程中,所述计算机程序被处理器运行时,还执行:

[0239] 将用户输入的开锁口令和第一随机数进行摘要计算,得到第三摘要值;

[0240] 向门锁管理系统请求所述标准数据;

[0241] 接收门锁管理系统下发的第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果；

[0242] 利用所述第二随机数对所述第三摘要值进行摘要计算，并将得到的计算结果与所述第二随机数与标准数据的摘要计算结果进行比较，如果两者相同，则开启门锁。

[0243] 本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时，执行：

[0244] 接收智能门锁发送的标准数据；其中，所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的；

[0245] 保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启。

[0246] 所述接收智能门锁发送的标准数据之前，所述计算机程序被处理器运行时，还执行：

[0247] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证。

[0248] 所述与所述智能门锁进行相互身份验证之前，所述计算机程序被处理器运行时，还执行：

[0249] 产生第一随机数，并保存所述第一随机数与智能门锁标识的对应关系；

[0250] 将所述第一随机数通过短信或网页的通信方式传递给用户。

[0251] 所述接收智能门锁发送的标准数据时，所述计算机程序被处理器运行时，还执行：

[0252] 接收第一摘要值以及智能门锁标识；其中，

[0253] 所述第一摘要值为：将用户设置的开锁口令进行摘要计算得到的结果。

[0254] 所述保存所述标准数据与智能门锁标识的对应关系，所述计算机程序被处理器运行时，还执行：

[0255] 对所述第一摘要值和所述第一随机数进行摘要计算；

[0256] 将摘要计算结果与所述标准数据进行比较，如果两者相同，则保存所述标准数据与智能门锁标识的对应关系；其中，所述第一随机数与所述智能门锁标识对应；

[0257] 删除已保存的所述第一随机数。

[0258] 所述基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数，与所述智能门锁进行相互身份验证时，所述计算机程序被处理器运行时，还执行：

[0259] 接收智能门锁发送的智能门锁标识、以及所述智能门锁标识和第一随机数进行摘要计算的结果；

[0260] 将收到的智能门锁标识与对应的第一随机数进行摘要计算，将计算结果与智能门锁发送的智能门锁标识和第一随机数摘要计算的结果进行比较；

[0261] 如果两者相同，则表明对智能门锁的身份验证通过，并将门锁管理系统的签名发送到智能门锁，用于智能门锁对门锁管理系统进行身份验证。

[0262] 在开锁过程中，所述计算机程序被处理器运行时，还执行：

[0263] 接收智能门锁发送的对标准数据的请求；

[0264] 将第二随机数、门锁管理系统的签名，以及第二随机数与标准数据的摘要计算结果发送到智能门锁；其中，

[0265] 所述第二随机数与标准数据的摘要计算结果，用于与智能门锁将第二随机数和第

三摘要值进行摘要计算的结果进行比较来确定是否开启门锁;其中,

[0266] 所述第三摘要值为:智能门锁将用户输入的开锁口令和第一随机数进行摘要计算的结果。

[0267] 下面结合场景实施例对本发明进行描述。

[0268] 本实施例提出一种无需改造硬件,无需存储密码根的智能门锁敏感信息(用户设置的开锁口令)远端存储方法。

[0269] 开锁认证模型如图7所示,所述标准数据为用户设置的开锁口令(如指纹、密码)的HASH值,标准数据存储于门锁管理系统中。开锁时,用户的输入数据与存储的标准数据进行比较,如果比较结果一致,则执行动作1(开锁),否则执行动作2(不开锁)。

[0270] 本实施例将标准数据存储于安全接入网关或云端服务器(门锁管理系统)中,即可用于智能门锁的用户开锁场景,场景示意图如图8所示。场景中用户开锁口令的采集及暂存于内存中的安全不在本文研究范围。下面以门锁管理系统为适用面广的云端服务器为例说明标准数据的存储流程,安全接入网关存储类似。

[0271] 预先准备工作

[0272] 云端服务器的证书(含签名)存储于智能门锁中。门锁管理系统中预先存储智能门锁标识ID,并分配给用户初始用户名和登陆密码。

[0273] 本实施例基于随机数挑战的方式,实现门锁管理系统对智能门锁的身份认证。随机数不通过门锁与门锁管理系统的通信通道进行传递,而是以短信或https网页等通信通道下发给用户。用户设置开锁口令后,经随机数加扰再进行摘要运算,实现数据传递的机密性和防篡改、防重放。用户开锁口令以摘要值存储在服务器中,确保口令不被门锁管理系统识别获取。通过证书验签方式对门锁管理系统进行认证,确保开锁口令摘要值存储在正确的门锁管理系统中。

[0274] 如图9所示,用户设置的开锁口令的存储流程包括如下流程:

[0275] 步骤901:用户(通过初始用户名和登陆密码)登录门锁管理界面,进行开锁密码设置。门锁管理系统随机产生的一串数RAND1(第一随机数)给用户,数据RAND1以短信或https网页等通信方式传递给用户。RAND1、ID的对应关系被存储于门锁管理系统中。可设置RAND1在一定的时间内有效,超时无效。

[0276] 步骤902:用户通过键盘或指纹装置设置开启智能门锁的口令(密码或用户指纹数据),并输入获得的随机数串RAND1。

[0277] 步骤903:智能门锁计算value0=hash(RAND1||ID),并将ID、value0一同发送至门锁管理系统。

[0278] 步骤904:门锁管理系统检查ID对应RAND1的时效性,并根据ID和ID对应的随机数串RAND1计算value0。如果计算所得的value0与智能门锁发送的value0相同,则发送value0及门锁管理系统的签名给智能门锁。

[0279] 步骤905:智能门锁确定门锁管理系统发送的签名与已存储的签名相同,则门锁管理系统验签通过,智能门锁保存RAND1,并对设置的开锁口令计算hash值value1(第一摘要值),然后将value1与随机数串RAND1连接后做hash计算得value2(第二摘要值,即标准数据),最后将ID、value1和value2一同发送至门锁管理系统。其中,

[0280] value1=hash(开锁口令);

[0281] value2＝hash(RAND1||value1)。

[0282] 步骤906:门锁管理系统检查智能门锁ID对应的RAND1的时效性,并根据value1和ID对应的随机数串RAND1计算value2。如果正确,则保存ID与value2的对应关系,并将之前保存的RAND1删除。

[0283] 步骤907:门锁管理系统发送口令设置流程成功消息,智能门锁转发成功消息给用户。

[0284] 本实施例门锁管理系统不需要对智能门锁的身份进行认证,即可接受用户标准数据查询。为防止恶意获取标准数据,标准数据经第二随机数加扰后签名运算返回给智能门锁。用户开锁流程如图10所示,包括:

[0285] 步骤1001:用户通过键盘或指纹装置输入开启智能门锁的口令;

[0286] 步骤1002:智能门锁对用户输入的开锁口令、已保存的RAND1计算hash值value2’(第三摘要值),同时向门锁管理系统发起请求,获取保存着的智能门锁的value2(标准数据)。

[0287] value2’＝hash(RAND1||hash(开锁口令))。

[0288] 步骤1003:门锁管理系统将RAND2(第二随机数,每次开锁时不同)、HASH(RAND2||value2)和签名值发送给智能门锁。

[0289] 步骤1004:智能门锁验证门锁管理系统发送的签名验证通过后,计算HASH(RAND2||value2’),并与门锁管理系统发送的HASH(RAND2||value2)进行比较,如果两者一致,门锁开启。

[0290] 本发明实施例在用户设置开锁口令后,基于第一随机数和摘要算法实现数据传递的防篡改、防重放,保证了标准数据的安全性。此外,用户口令以摘要值的形式存储在门锁管理系统,确保开锁口令不被门锁管理系统识别,避免用户的开锁口令暴露在网络上,有效提高了验证的安全性,且不需要对硬件进行改造。

[0291] 此外,本发明实施例还在存储标准数据前进行智能门锁与门锁管理系统的相互身份验证,保证标准数据保存在正确的门锁管理系统中。

[0292] 基于所述智能门锁标识、门锁管理系统的证书以及门锁管理系统产生的第一随机数,与所述门锁管理系统进行相互身份验证。这样,可保证标准数据保存在正确的门锁管理系统中,进一步提高安全性。

[0293] 所述第一随机数不通过智能门锁与门锁管理系统的通信通道进行传递,而是通过短信或网页的通信方式传递给用户,可保证随机数的传输安全。

[0294] 本发明实施例利用摘要算法的单向特性,用户设置的开锁口令经随机数加扰再进行摘要运算,实现数据传递的机密性和防篡改、防重放。

[0295] 在开锁过程中对比校准数据经第二随机数加扰后的摘要值,如此,每次开锁的钥匙一次一变(每次产生的第二随机数都不同),即使门锁管理系统的私钥被泄露,也可以保障开锁的安全。

[0296] 以上所述,仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。

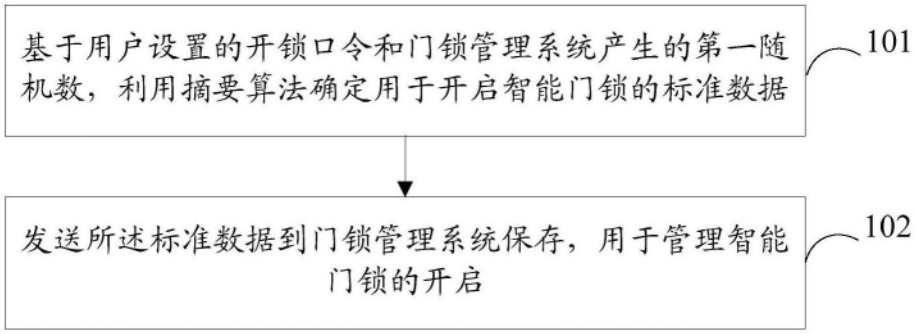

基于用户设置的开锁口令和门锁管理系统产生的第一随机数，利用摘要算法确定用于开启智能门锁的标准数据
101
发送所述标准数据到门锁管理系统保存，用于管理智能门锁的开启
102

图1

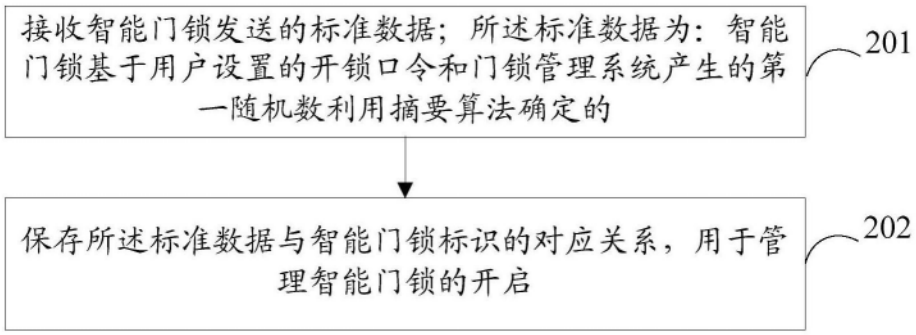

接收智能门锁发送的标准数据；所述标准数据为：智能门锁基于用户设置的开锁口令和门锁管理系统产生的第一随机数利用摘要算法确定的
201
保存所述标准数据与智能门锁标识的对应关系，用于管理智能门锁的开启
202

图2


确定模块301
发送模块302
认证数据的存储装置

图3


第一验证模块303
确定模块301
发送模块302
认证数据的存储装置

图4


接收模块501
存储模块502
认证数据的存储装置

图5


第二验证模块503
接收模块501
存储模块502
认证数据的存储装置

图6

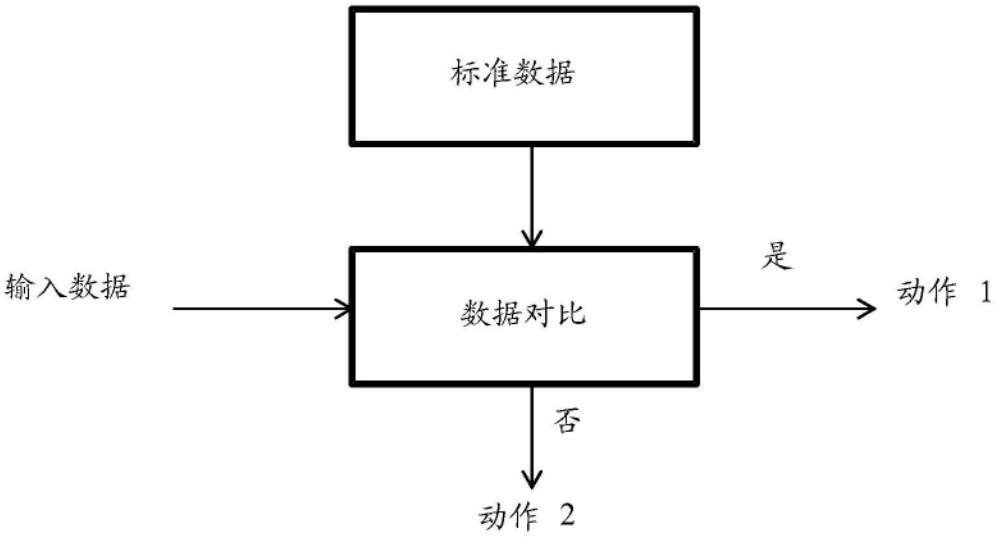

标准数据
输入数据
数据对比
是
动作 1
否
动作 2

图7

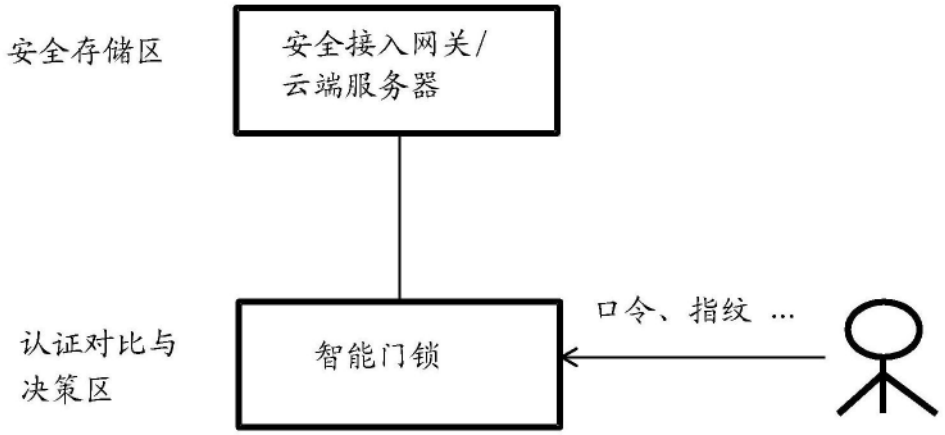

安全存储区
安全接入网关/
云端服务器
认证对比与
决策区
智能门锁
口令、指纹 ...

图8

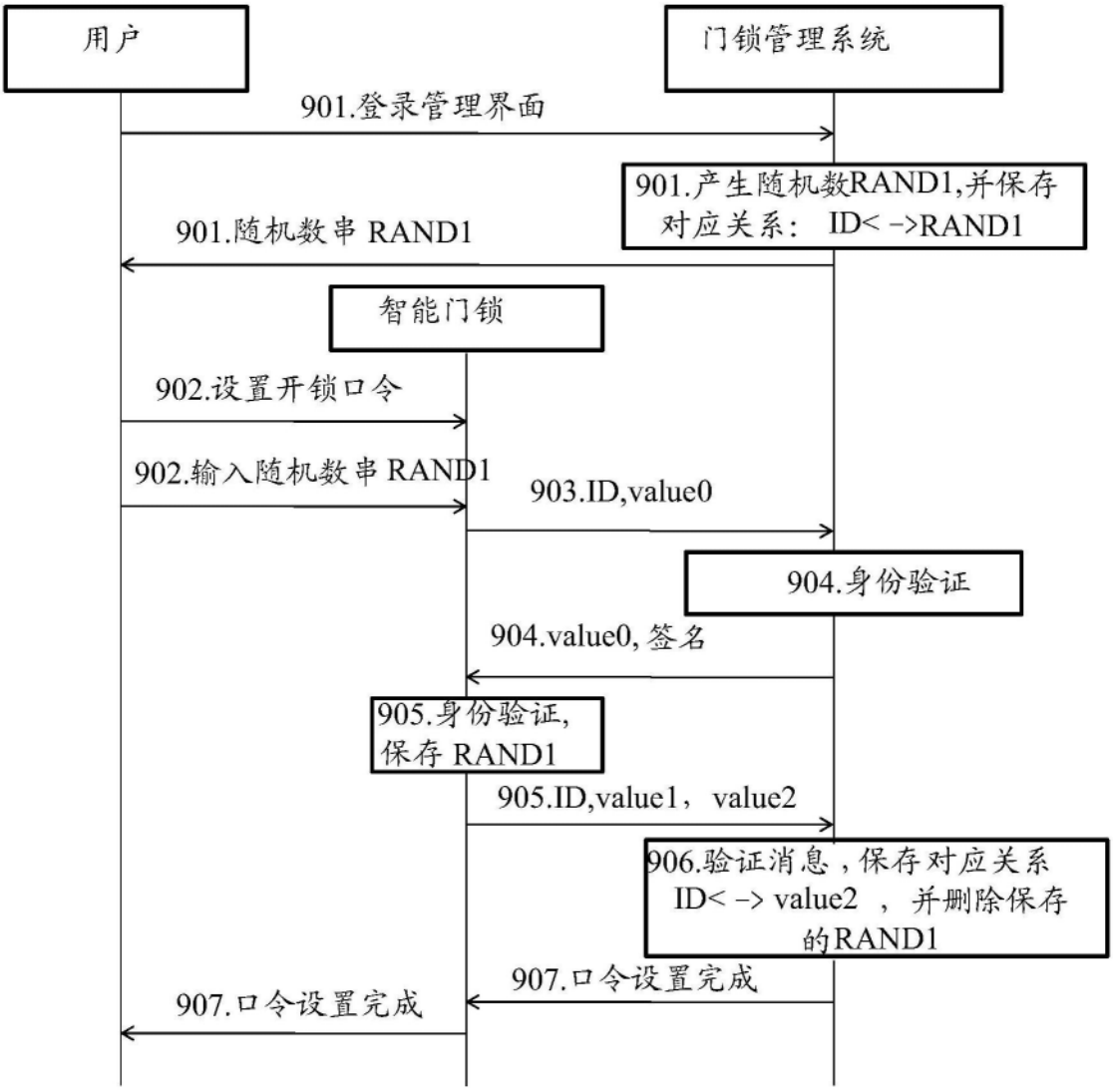

用户
门锁管理系统
901.登录管理界面
901.产生随机数RAND1,并保存
对应关系： ID< ->RAND1
901.随机数串 RAND1
智能门锁
902.设置开锁口令
902.输入随机数串 RAND1
903.ID,value0
904.身份验证
904.value0, 签名
905.身份验证,
保存 RAND1
905.ID,value1， value2
906.验证消息，保存对应关系
ID< -> value2 ， 并删除保存
的RAND1
907.口令设置完成
907.口令设置完成

图9

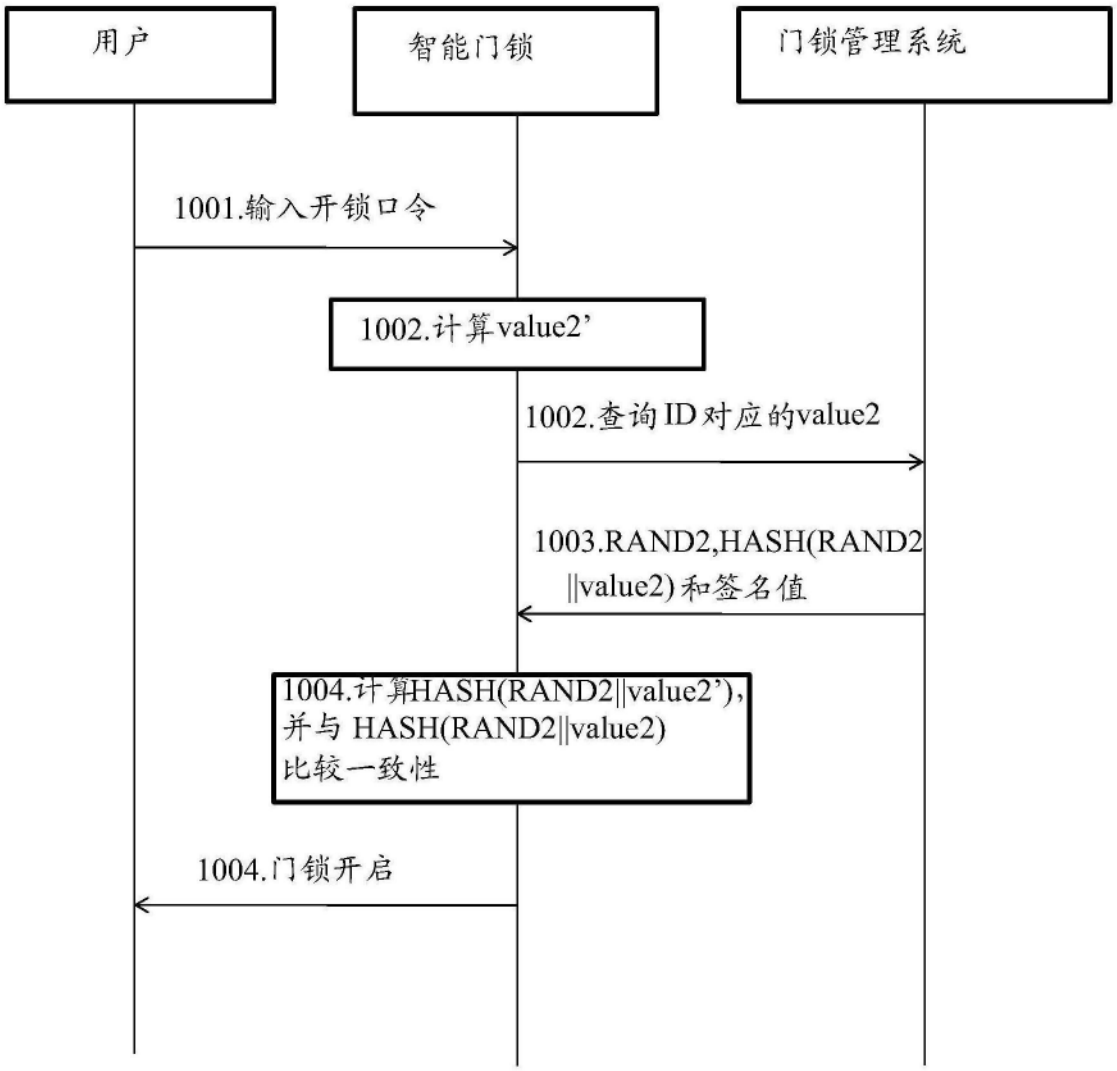

用户
智能门锁
门锁管理系统
1001.输入开锁口令
1002.计算value2'
1002.查询ID对应的value2
1003.RAND2,HASH(RAND2||value2)和签名值
1004.计算HASH(RAND2||value2'),并与 HASH(RAND2||value2)比较一致性
1004.门锁开启

图10