(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105844744 A
(43)申请公布日 2016.08.10

(21)申请号 201610164306.X

(22)申请日 2016.03.21

(71)申请人 成都艾德沃传感技术有限公司
地址 610000 四川省成都市天府大道天府软件园D7-303

(72)发明人 胡家安

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

(51)Int.Cl.
G07C 9/00(2006.01)

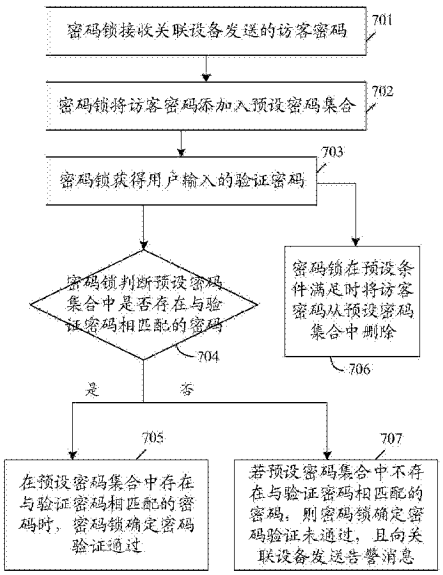
权利要求书2页 说明书8页 附图1页

(54)发明名称

一种验证密码的方法及密码锁

(57)摘要

一种密码验证方法及密码锁，用于解决因给他人打开密码锁的权限导致密码锁密码不安全的问题。该密码验证方法包括如下步骤：密码锁接收关联设备发送的访客密码；所述密码锁将所述访客密码添加入预设密码集合，且在预设条件满足时将所述访客密码从所述预设密码集合中删除；所述密码锁获得用户输入的验证密码；并判断所述预设密码集合中是否存在与所述验证密码相匹配的密码；若存在，则所述密码锁确定密码验证通过。



CN 105844744 A

1.一种密码验证方法,其特征在于,包括:

密码锁接收关联设备发送的访客密码;

所述密码锁将所述访客密码添加入预设密码集合,且在预设条件满足时将所述访客密码从所述预设密码集合中删除;

所述密码锁获得用户输入的验证密码;并

判断所述预设密码集合中是否存在与所述验证密码相匹配的密码;

若存在,则所述密码锁确定密码验证通过。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

所述密码锁接收所述关联设备发送的删除所述访客密码的请求;

所述密码锁响应所述请求,确定所述预设条件满足。

3.如权利要求1所述的方法,其特征在于,所述方法还包括:

所述密码锁接收所述关联设备发送的所述访客密码的有效次数;

所述密码锁对通过所述访客密码完成密码验证的次数进行计数;

在所述次数达到所述有效次数时,所述密码锁确定所述预设条件满足。

4.如权利要求1所述的方法,其特征在于,所述方法还包括:

所述密码锁接收所述关联设备发送的所述访客密码的失效时间;

在所述失效时间到达时,所述密码锁确定所述预设条件满足。

5.如权利要求1-4中任一项所述的方法,其特征在于,所述密码锁判断所述预设密码集合中是否存在与所述验证密码相匹配的密码,包括:

所述密码锁判断所述验证密码中是否存在与所述预设密码集合中任一密码相同的字符串,所述字符串的字符数小于所述验证密码的字符数;

若所述验证密码中存在与所述预设密码集合中的第一预设密码相同的字符串,则所述密码锁确定所述第一预设密码与所述验证密码相匹配。

6.如权利要求1-4中任一项所述的方法,其特征在于,所述方法还包括:

在用户输入访客密码的过程中,所述密码锁提示用户输入随机字符。

7.如权利要求1-4任一项所述的方法,其特征在于,在所述密码锁判断所述预设密码集合中是否存在与所述验证密码相匹配的密码之后,所述方法还包括:

若所述预设密码集合中不存在与所述验证密码相匹配的密码,则所述密码锁确定密码验证未通过,且向所述关联设备发送告警消息。

8.一种密码锁,其特征在于,包括:

接收单元,用于收关联设备发送的访客密码;

存储单元,用于存储所述访客密码以及预设密码集合;

输入单元,用于获得用户输入的字符;

处理单元,与所述接收单元、所述存储单元以及所述输入单元耦合,用于将所述访客密码添加入所述预设密码集合,且在预设条件满足时将所述访客密码从所述预设密码集合中删除;以及在所述输入单元获得用户输入的验证密码后,判断所述预设密码集合中是否存在与所述验证密码相匹配的密码;若存在,则确定密码验证通过。

9.如权利要求8所述的密码锁,其特征在于,所述接收单元还用于:接收所述关联设备发送的删除所述访客密码的请求;

所述处理单元还用于:响应所述请求,确定所述预设条件满足。

10.如权利要求8所述的密码锁,其特征在于,所述接收单元还用于:接收所述关联设备发送的所述访客密码的有效次数;

所述处理单元还用于:对通过所述访客密码完成密码验证的次数进行计数;并在所述次数达到所述有效次数时,确定所述预设条件满足。

11.如权利要求8所述的密码锁,其特征在于,所述接收单元还用于:接收所述关联设备发送的所述访客密码的失效时间;

所述处理单元还用于:在所述失效时间到达时,确定所述预设条件满足。

12.如权利要求8-11中任一项所述的密码锁,其特征在于,所述处理单元用于:判断所述预设密码集合中是否存在与所述验证密码相匹配的密码,包括:

判断所述验证密码中是否存在与所述预设密码集合中任一密码相同的字符串,所述字符串的字符数小于所述验证密码的字符数;

若所述验证密码中存在与所述预设密码集合中的第一预设密码相同的字符串,则确定所述第一预设密码与所述验证密码相匹配。

13.如权利要求8-11中任一项所述的密码锁,其特征在于,所述密码锁还包括:

提示单元,用于向用户输出提示信息;

所述处理单元还用于:在用户输入访客密码的过程中,通过所述提示单元提示用户输入随机字符。

14.如权利要求8-10任一项所述的密码锁,其特征在于,所述密码锁还包括:

发送单元,用于向所述关联设备发送消息;

所述处理单元还用于:在判断出所述预设密码集合中不存在与所述验证密码相匹配的密码后,确定密码验证未通过,且通过所述发送单元向所述关联设备发送告警消息。

一种验证密码的方法及密码锁

技术领域

[0001] 本发明涉及信息安全领域，特别涉及一种验证密码的方法及密码锁。

背景技术

[0002] 目前，很多地方设置有密码锁，如门禁、防盗门、行李箱、保险柜等等。在使用密码锁时，保证密码的安全至关重要。

[0003] 但是，很多情况时，用户需要让别人打开密码锁，如有朋友到家访问而自己尚未到家的时候，可以想让朋友先进家等候。但是，如果告知朋友密码锁的密码，将导致密码锁的密码不安全。

发明内容

[0004] 本申请提供一种验证密码的方法及密码锁，用于解决因给他人打开密码锁的权限导致密码锁密码不安全的问题。

[0005] 第一方面，本发明实施例提供一种密码验证方法，包括：密码锁接收关联设备发送的访客密码；所述密码锁将所述访客密码添加入预设密码集合，且在预设条件满足时将所述访客密码从所述预设密码集合中删除；所述密码锁获得用户输入的验证密码；并判断所述预设密码集合中是否存在与所述验证密码相匹配的密码；若存在，则所述密码锁确定密码验证通过。

[0006] 上述实现方式中，用户可以通过关联设备在密码锁中添加访客密码，使得他人可以通过访客密码通过密码验证，而不会泄露自己的核心密码。而且访客密码会在预设条件满足时被无效，保证密码锁的安全，进而实现在保护密码锁安全的情况下，给其他用户短期的通过密码锁验证的权限。

[0007] 在一些可能的实现方式中，所述方法还包括：所述密码锁接收所述关联设备发送的删除所述访客密码的请求；所述密码锁响应所述请求，确定所述预设条件满足。本实现方式中，用户能够手动无效访客密码，保证在访客离开后密码锁的安全。

[0008] 在一些可能的实现方式中，所述方法还包括：所述密码锁接收所述关联设备发送的所述访客密码的有效次数；所述密码锁对通过所述访客密码完成密码验证的次数进行计数；在所述次数达到所述有效次数时，所述密码锁确定所述预设条件满足。本实现方式中，密码锁将基于用户通过关联设备设定的失效机制无效访客密码，保证在访客离开后密码锁的安全。

[0009] 在一些可能的实现方式中，所述方法还包括：所述密码锁接收所述关联设备发送的所述访客密码的失效时间；在所述失效时间到达时，所述密码锁确定所述预设条件满足。本实现方式中，密码锁将基于用户通过关联设备设定的失效机制无效访客密码，保证在访客离开后密码锁的安全。

[0010] 在一些可能的实现方式中，所述密码锁判断所述预设密码集合中是否存在与所述验证密码相匹配的密码，包括：所述密码锁判断所述验证密码中是否存在与所述预设密码

集合中任一密码相同的字符串，所述字符串的字符数小于所述验证密码的字符数；若所述验证密码中存在与所述预设密码集合中的第一预设密码相同的字符串，则所述密码锁确定所述第一预设密码与所述验证密码相匹配。通过本实现方式，用户可以输入包含预设密码以及冗余字符的验证密码，使用户在通过密码验证时他人难以偷窥记录有效密码，保护密码安全。

[0011] 在一些可能的实现方式中，所述方法还包括：在用户输入访客密码的过程中，所述密码锁提示用户输入随机字符。

[0012] 在一些可能的实现方式中，在所述密码锁判断所述预设密码集合中是否存在与所述验证密码相匹配的密码之后，所述方法还包括：若所述预设密码集合中不存在与所述验证密码相匹配的密码，则所述密码锁确定密码验证未通过，且向所述关联设备发送告警消息。通过本实现方式，密码锁在密码验证未通过后，向关联设备发送告警消息，对用户进行安全提示，进而使其能够及时保护财产安全。

[0013] 第二方面，本发明实施例提供一种密码锁，包括：接收单元，用于收关联设备发送的访客密码；存储单元，用于存储所述访客密码以及预设密码集合；输入单元，用于获得用户输入的字符；处理单元，与所述接收单元、所述存储单元以及所述输入单元耦合，用于将所述访客密码添加入所述预设密码集合，且在预设条件满足时将所述访客密码从所述预设密码集合中删除；以及在所述输入单元获得用户输入的验证密码后，判断所述预设密码集合中是否存在与所述验证密码相匹配的密码；若存在，则确定密码验证通过。

[0014] 在一些可能的实现方式中，所述接收单元还用于：接收所述关联设备发送的删除所述访客密码的请求；所述处理单元还用于：响应所述请求，确定所述预设条件满足。

[0015] 在一些可能的实现方式中，所述接收单元还用于：接收所述关联设备发送的所述访客密码的有效次数；所述处理单元还用于：对通过所述访客密码完成密码验证的次数进行计数；并在所述次数达到所述有效次数时，确定所述预设条件满足。

[0016] 在一些可能的实现方式中，所述接收单元还用于：接收所述关联设备发送的所述访客密码的失效时间；所述处理单元还用于：在所述失效时间到达时，确定所述预设条件满足。

[0017] 在一些可能的实现方式中，所述处理单元用于：判断所述预设密码集合中是否存在与所述验证密码相匹配的密码，包括：判断所述验证密码中是否存在与所述预设密码集合中任一密码相同的字符串，所述字符串的字符数小于所述验证密码的字符数；若所述验证密码中存在与所述预设密码集合中的第一预设密码相同的字符串，则确定所述第一预设密码与所述验证密码相匹配。

[0018] 在一些可能的实现方式中，所述密码锁还包括：提示单元，用于向用户输出提示信息；所述处理单元还用于：在用户输入访客密码的过程中，通过所述提示单元提示用户输入随机字符。

[0019] 在一些可能的实现方式中，所述密码锁还包括：发送单元，用于向所述关联设备发送消息；所述处理单元还用于：在判断出所述预设密码集合中不存在与所述验证密码相匹配的密码后，确定密码验证未通过，且通过所述发送单元向所述关联设备发送告警消息。

附图说明

[0020] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0021] 图1为本发明实施例中密码锁的结构示意框图；

[0022] 图2为本发明实施例中密码验证方法的流程示意图。

具体实施方式

[0023] 下面通过附图以及具体实施例对本发明技术方案做详细的说明，应当理解本发明实施例以及实施例中的具体特征是对本发明技术方案的详细的说明，而不是对本发明技术方案的限定，在不冲突的情况下，本发明实施例以及实施例中的技术特征可以相互组合。

[0024] 本发明实施例中的密码锁可以设置在防盗门、保险柜、行李箱之上。参照图1，密码锁包括处理单元10、存储单元20、输入单元30以及接收单元40。

[0025] 其中，处理单元10是密码锁的控制中心，利用各种接口和线路连接整个密码锁的各个部分，通过运行自身固化的指令或存储在存储单元20内的指令以及调用存储在存储单元20内的数据，执行密码锁的各种功能和处理数据，从而实现密码验证。可选的，处理单元10可包括一个或多个处理元件，具体的，处理单元10可以是中央处理器(Central Processing Unit;简称:CPU)，也可以是特定集成电路(Application Specific Intergrated Circuit;简称:ASIC)，或者是被配置成实施本发明实施例的一个或多个集成电路，例如:一个或多个微处理器(digital singnal processor;简称:DSP)，或，一个或者多个现场可编程门阵列(Field Programmable Gate Array;简称:FPGA)。优选的，处理单元10可集成有调制解调处理器，其中，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理单元10中。在一些实施例中，处理单元10、存储单元20可以在单一芯片上实现，在一些实施例中，他们也可以在独立的芯片上分别实现。

[0026] 所述存储单元20可用于存储指令和数据，可包括一个或多个存储元件。存储单元20可主要包括存储指令区和存储数据区，存储数据区可存储预设密码集合中的密码、用户输入的验证密码或密码锁接收的请求或数据等;存储指令区可存储密码锁的操作系统、至少一个功能所需的指令等。

[0027] 输入单元30的实现方式包括:其一，输入单元30为设置有实体按键的输入面板，每个实体按键与字符对应，用户通过触压输入面板上的按键，可以输入用于密码验证的验证密码。其二，输入单元30为触摸屏，具体可以为矢量压力传感技术触摸屏、电阻技术触摸屏、电容技术触摸屏、红外线技术触摸屏、表面声波技术触摸屏，等等。作为输入单元30的触摸屏可以显示虚拟按键，用户通过触摸虚拟按键可以输入用于密码验证的验证密码。可选的，输入单元30还可以获取用户在触摸屏上输入的以虚拟按键为节点的轨迹图案，该轨迹图案可以单独作为验证密码或者与字符串结合作为验证密码。

[0028] 接收单元40用于接收外部网元发送的信息。本发明实施例中，密码锁可以与一个或多个通信设备(如平板电脑、智能手机、智能手表等)进行关联，并接收关联的通信设备发送的请求或数据，例如，接收单元40可以从关联设备处接收添加或删除访客密码的请求，或者接收关联设备发送的对密码锁进行配置的参数，等等。通常，接收单元包括但不限于天

线、至少一个放大器、收信机、耦合器、低噪声放大器(Low Noise Amplifier,LNA)等。接收单元40可以使用任一通信标准或协议,包括但不限于:全球移动通讯系统(Global System of Mobile communication;简称:GSM)、通用分组无线服务(General Packet Radio Service;简称:GPRS)、码分多址(Code Division Multiple Access;简称:CDMA)、宽带码分多址(Wideband Code Division Multiple Access;简称:WCDMA)、长期演进(Long Term Evolution;简称:LTE)、、第五代移动通信系统(The fifth generation mobile communication system;简称:5G)、Wi-Fi通信、蓝牙(Bluetooth)通信、红外(Infrared)通信、紫蜂(Zigbee)通信、近场通信(Near Field Communication;简称:NFC)。

[0029] 在一些可能的实现方式中,密码锁还包括发送单元50,用于向其他网络发送信息,例如,发送单元50可以向关联设备发送密码验证的日志,或者在密码验证多次失败后向关联设备发送告警消息。本发明实施例中,发送单元50与接收单元40可以集成在一起,也可以分别为两个元件。发送单元50包括但不限于天线、至少一个放大器、发信机、耦合器、低噪声放大器(Low Noise Amplifier,LNA)等。发送单元50使用的通信标准或协议请参照接收单元40。

[0030] 在一些可能的实现方式中,密码锁还包括提示单元60,用于向用户输出信息。例如,在输入单元30为设置有实体按键的输入面板时,提示单元60可以为设置在该实体按键上的提示灯,通过点亮提示灯,提示用于按压该提示灯对应的实体按键。又例如,在输入单元30为显示虚拟按键的触摸屏时,用于对用户进行提示的提示单元60可以为输入单元30本身,输入单元30可以通过改变虚拟按键的显示方式(如改变虚拟按键的亮度、颜色,或者使虚拟按键闪烁、移动,等等),提示用于按压该显示方式改变的虚拟按键。

[0031] 尽管未示出,密码锁还可以包括摄像头、提示灯、音频输出装置、电源、无线充电器等。

[0032] 另外,本发明实施例中,密码锁与关联设备进行关联的方式包括:其一,密码锁通过账号登录与远程管理服务器建立连接,而关联设备登录同一账号与远程管理服务器建立连接,进而,远程管理服务器能够作为密码锁与关联设备之间数据传输以及信令传输的中转,密码锁与关联设备完成关联。其二,密码锁与关联设备之间通过机器与机器(Machine to Machine;简称:M2M)通信网络建立连接并配对关联,或者,密码锁与关联设备通过紫蜂(Zigbee)网络连接并配对关联,或者,码锁与关联设备通过NFC方式连接并配对,或者,码锁与关联设备通过蓝牙方式连接并配对。

[0033] 图2为本发明实施例提供的密码验证方法的流程示意图,该方法包括如下步骤:

[0034] 步骤701:密码锁接收关联设备发送的访客密码;

[0035] 步骤702:密码锁将访客密码添加入预设密码集合;

[0036] 步骤703:密码锁获得用户输入的验证密码;

[0037] 步骤704:密码锁判断预设密码集合中是否存在与验证密码相匹配的密码;若是,则执行步骤705;

[0038] 步骤705:在预设密码集合中存在与验证密码相匹配的密码时,密码锁确定密码验证通过;

[0039] 步骤706:密码锁在预设条件满足时将访客密码从预设密码集合中删除。

[0040] 具体的,本发明实施例中,预设密码集合中的密码为预设的使用户能够通过密码

验证的密码，换言之，如果用户输入的密码与预设密码集合中任一密码相匹配，则密码验证通过。

[0041] 通常情况下，预设密码集合中包括用户本人使用的核心密码，当用户需要让他人打开密码锁时，如果告知别人核心密码，则会造成核心密码泄露，用户不得不事后更改核心密码，非常不便。

[0042] 为了解决该问题，本发明实施例中，用户可以通过关联设备设置访客密码，并通过关联设备将访客密码发送至密码锁，密码锁将该访客密码添加进预设密码集合之中。这时，如果有用户输入的验证密码与该访客密码匹配，则用户能够通过密码验证，打开密码锁。

[0043] 并且，在预设条件满足时，密码锁可以从预设密码集合中删除该访客密码，使该访客密码失效，而该预设额条件可以通过用户手动触发，或者密码锁基于设置好的失效机制触发该预设条件。

[0044] 另外，步骤706只要在步骤702之后执行即可，不限定其与步骤703～步骤705的先后顺序。

[0045] 上述技术方案中，用户可以通过关联设备在密码锁中添加访客密码，使得他人可以通过访客密码通过密码验证，而不会泄露自己的核心密码。而且访客密码会在预设条件满足时被无效，保证密码锁的安全，进而实现在保护密码锁安全的情况下，给其他用户短期的通过密码锁验证的权限。

[0046] 可选的，本发明实施例中，密码锁判断是否满足预设条件，包括但不限于如下方式：

[0047] 方式1，用户手动删除访客密码。

[0048] 密码锁接收关联设备发送的删除访客密码的请求；密码锁响应请求，确定预设条件满足。

[0049] 具体的，用户可以通过关联设备手动删除访客密码，关联设备将该删除访客密码的请求发送至密码锁之后，密码锁在接收到该请求之后，即可确定预设条件满足，触发访客密码的删除，使得访客密码无效。实际情况中，用户也可以直接在密码锁上进行删除访客密码的操作。

[0050] 方式2，用户设置访客密码失效机制，密码锁根据该机制让密码锁失效。

[0051] 失效机制一，密码锁接收关联设备发送的访客密码的有效次数；密码锁对通过访客密码完成密码验证的次数进行计数；在次数达到有效次数时，密码锁确定预设条件满足。

[0052] 具体的，用户通过关联设备设置访客密码在使用k次之后失效，则关联设备将该有效次数k发送至密码锁，其中，关联设备可以在发送访客密码的同时将该有效次数k发送至密码锁，也可以在发送访客密码之后向密码锁发送有效次数。

[0053] 密码锁在对用户输入的验证密码进行验证后，若验证通过的密码与访客密码匹配，则进行计数。当计数达到有效次数k时，表明已使用访客密码通过密码验证的次数达到k，密码锁将基于失效机制一，从预设密码集合中删除访客密码，使访客密码失效。

[0054] 失效机制二，密码锁接收关联设备发送的访客密码的失效时间；在失效时间到达时，密码锁确定预设条件满足。

[0055] 具体的，用户通过关联设备设置访客密码在失效时间之后失效，则关联设备将该失效时间发送至密码锁，其中，关联设备可以在发送访客密码的同时将该失效时间发送至

密码锁，也可以在发送访客密码之后向密码锁发送失效时间。

[0056] 密码锁在收到失效时间之后，无论该访客密码的验证情况如何，将将基于失效机制二，从预设密码集合中删除访客密码，使访客密码失效。

[0057] 失效机制三，结合前述失效机制一，在用户未设置有效次数的情况下，密码锁将有效次数设置为默认的缺省值k_1，如缺省值k_1的值为1次，换言之，访客密码内一次性的，如果有用户通过该访客密码通过密码验证，则密码锁立即从预设密码集合中删除该访客密码，使访客密码失效。

[0058] 失效机制四，结合前述失效机制二，在用户未设置失效时间的情况下，密码锁将失效时间设置为接收访客密码的默认时长之后的时刻，如默认时长为3小时，密码锁将在接收到访客密码3小时之后使访客密码失效。

[0059] 通过上述任一方式，能够使访客密码被无效，保证给予他人的通过密码锁的权限只是短期的、临时的，保障密码锁的安全。

[0060] 在一些可能的实现方式中，步骤704：密码锁判断预设密码集合中是否存在与验证密码相匹配的密码，包括但不限于如下实现方式：

[0061] 方式一，严格匹配方式。即，验证密码与预设密码集合中的第一预设密码完全相同时，验证密码才与第一密码匹配。

[0062] 方式二，冗余匹配方式。即，密码锁判断验证密码中是否存在与预设密码集合中任一密码相同的字符串，该字符串的字符数小于验证密码的字符数；在验证密码中存在与预设密码集合中的第一预设密码相同的字符串时，第一预设密码与验证密码相匹配。

[0063] 具体的，所谓冗余匹配方式指的是，用户可以输入长于预设密码的字符串作为验证密码，只要该验证密码中包括与任一预设密码相同的字符串，该验证密码即与该预设密码相匹配。

[0064] 例如，用户如果知道预设密码为“800008”，则其可以输入“xx…800008…xx”作为验证密码，并通过密码验证，其中xx为任意字符。

[0065] 这么做的好处在于，用户在输入验证密码时，可以输入冗余字符，而这些冗余字符可以扰乱偷窥用户输入验证密码的人，使其难以记住用户输入的包含冗余字符的一长串验证密码，进而使其难以知晓真正的有效地密码，起到防止他人偷窥密码的作用，保护密码安全。

[0066] 可选的，结合上述方式二，密码锁记录通过上述方式二的方式完成密码验证的验证密码，并在之后的密码验证中接收到同样的验证密码时，向关联设备发送提示消息，或者，要求用户进行二次验证(可以为其他形式的验证，也可以为要求用户输入其他的验证密码进行验证)，或者，以该验证密码有风险为由，确定密码验证未通过。

[0067] 通过上述方式，能够避免他人通过完全记录用户输入的冗余密码通过密码验证的情况，保证密码安全。

[0068] 在一些可能的实现方式中，密码锁在通过输入单元获取用户输入的验证密码时，亦即在用户输入访客密码的过程中，密码锁提示用户输入随机字符。

[0069] 具体的，在前述步骤704的方式二中，用户可以通过输入冗余字符的方式防止他人窥视密码，但是这需要用户在输入验证密码时刻意输入冗余字符，而这种刻意输入冗余字符的行为与用户的下意识是相违背的，用户通常难以确定具体输入哪些冗余字符，这反而

给用户带来困扰。

[0070] 本实现方式中，密码锁在检测到用户在输入验证密码时，会主动生成随机字符作为冗余字符，并通过提示单元60提示用户输入这些冗余字符，帮助用户完成冗余字符的输入，既起到密码防窥视的作用，又不会给用户带来如何确定冗余字符的困扰。

[0071] 在一些可能的实现方式中，在步骤704的判断结果为否时则执行如下步骤：

[0072] 步骤707：若预设密码集合中不存在与验证密码相匹配的密码，则密码锁确定密码验证未通过，且向关联设备发送告警消息。

[0073] 具体的，在预设密码集合中所有的预设密码均与用户输入的验证密码不匹配时，密码锁确定密码验证未通过，并向关联设备发送告警消息，以告知用户他人正试图使用非法的验证密码打开密码锁。

[0074] 其中，告警消息中还可以包括密码锁上设置的摄像头，或者与密码锁关联的独立摄像头所采集密码锁前方的照片，以使用户能够知晓是谁在视图打开密码锁，确保财产安全。

[0075] 可选的，密码锁具体在密码验证连续失败次数达到阈值t之后，才向关联设备发送所述告警消息，以减少对用户的干扰。

[0076] 上述技术方案中，密码锁在密码验证未通过后，向关联设备发送告警消息，对用户进行安全提示，进而使其能够及时保护财产安全。

[0077] 基于相同的发明构思，本发明实施例提供一种密码锁，继续参照图1，该密码锁包括处理单元10、存储单元20、输入单元30以及接收单元40。

[0078] 其中，接收单元40用于收关联设备发送的访客密码。

[0079] 存储单元20用于存储访客密码以及预设密码集合。

[0080] 输入单元30用于获得用户输入的字符。

[0081] 处理单元10分别与接收单元40、存储单元20以及输入单元30耦合，用于将访客密码添加入预设密码集合，且在预设条件满足时将访客密码从预设密码集合中删除；以及在输入单元30获得用户输入的验证密码后，判断预设密码集合中是否存在与验证密码相匹配的密码；若存在，则确定密码验证通过。

[0082] 在一种可能的实现方式中，接收单元40还用于：接收关联设备发送的删除访客密码的请求；

[0083] 处理单元10还用于：响应请求，确定预设条件满足。

[0084] 在一种可能的实现方式中，接收单元40还用于：接收关联设备发送的访客密码的有效次数；

[0085] 处理单元10还用于：对通过访客密码完成密码验证的次数进行计数；并在次数达到有效次数时，确定预设条件满足。

[0086] 在一种可能的实现方式中，接收单元40还用于：接收关联设备发送的访客密码的失效时间；

[0087] 处理单元10还用于：在失效时间到达时，确定预设条件满足。

[0088] 在一种可能的实现方式中，处理单元10用于：判断预设密码集合中是否存在与验证密码相匹配的密码，包括：判断验证密码中是否存在与预设密码集合中任一密码相同的字符串，所述字符串的字符数小于所述验证密码的字符数；若验证密码中存在与预设密码

集合中的第一预设密码相同的字符串，则确定第一预设密码与验证密码相匹配。

[0089] 在一种可能的实现方式中，密码锁还包括提示单元60，用于向用户输出提示信息；

[0090] 处理单元10还用于：在用户输入访客密码的过程中，通过提示单元60提示用户输入随机字符。

[0091] 在一种可能的实现方式中，密码锁还包括：

[0092] 发送单元50，用于向关联设备发送消息；

[0093] 处理单元10还用于：在判断出预设密码集合中不存在与验证密码相匹配的密码后，确定密码验证未通过，且通过发送单元50向关联设备发送告警消息。

[0094] 上述密码锁中各组成单元所实现的功能可以参照图2的密码验证方法中各步骤的实现方式，且密码锁中各组成单元的实现方式请参照前面对图1中各单元的描述，在此不再赘述。

[0095] 本发明实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

[0096] 用户可以通过关联设备在密码锁中添加访客密码，使得他人可以通过访客密码通过密码验证，而不会泄露自己的核心密码。而且访客密码会在预设条件满足时被无效，保证密码锁的安全，进而实现在保护密码锁安全的情况下，给其他用户短期的通过密码锁验证的权限。

[0097] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0098] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0099] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0100] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0101] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

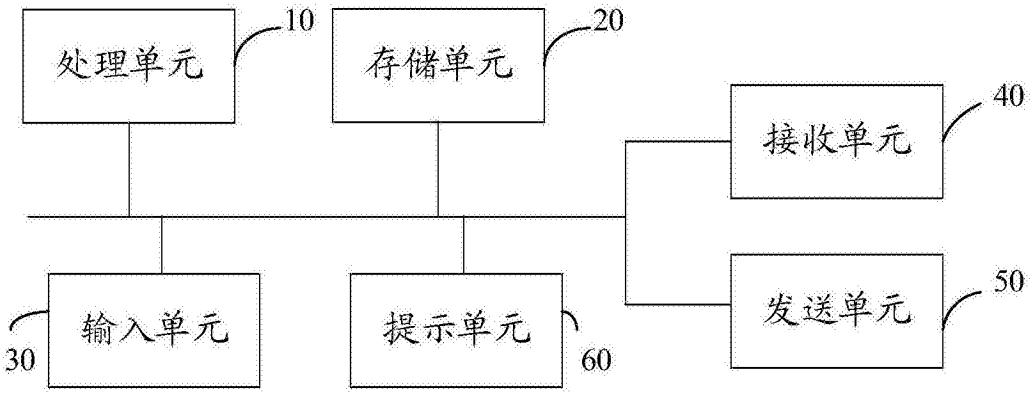

处理单元
10
存储单元
20
接收单元
40
输入单元
30
提示单元
60
发送单元
50

图1

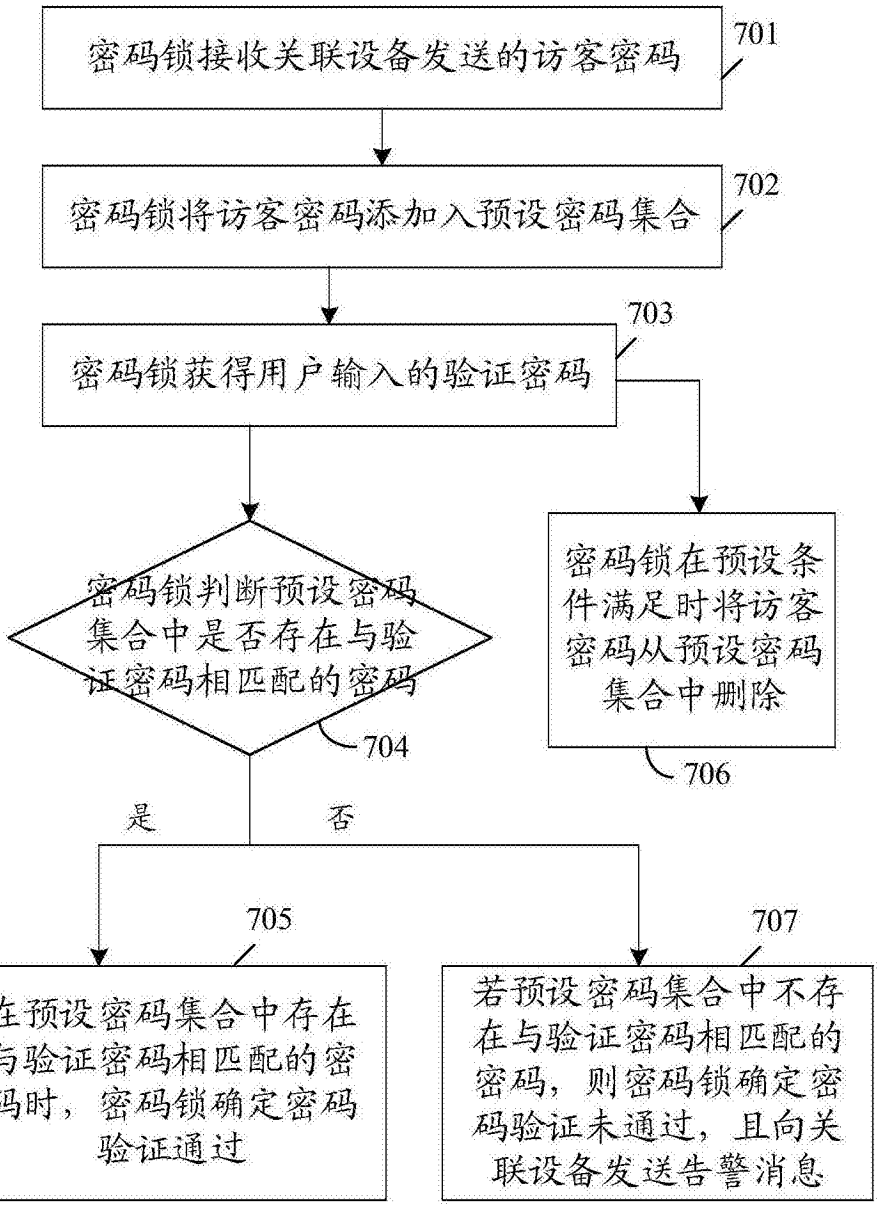

密码锁接收关联设备发送的访客密码
701
密码锁将访客密码添加入预设密码集合
702
密码锁获得用户输入的验证密码
703
密码锁判断预设密码集合中是否存在与验证密码相匹配的密码
704
密码锁在预设条件满足时将访客密码从预设密码集合中删除
706
是
否
705
在预设密码集合中存在与验证密码相匹配的密码时，密码锁确定密码验证通过
707
若预设密码集合中不存在与验证密码相匹配的密码，则密码锁确定密码验证未通过，且向关联设备发送告警消息

图2