(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 103701599 B
(45)授权公告日 2017.01.18

(21)申请号 201310682166.1

(22)申请日 2013.12.12

(65)同一申请的已公布的文献号
申请公布号 CN 103701599 A

(43)申请公布日 2014.04.02

(73)专利权人 珠海市金邦达保密卡有限公司
地址 519070 广东省珠海市香洲区前山镇福溪金邦达大厦

(72)发明人 李军 杨宁 于鸽

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 彭瑞欣 陈源

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
US 6883717 B1,2005.04.26,
CN 100501754 A,2013.02.13,
CN 1845185 A,2006.10.11,

审查员 何花

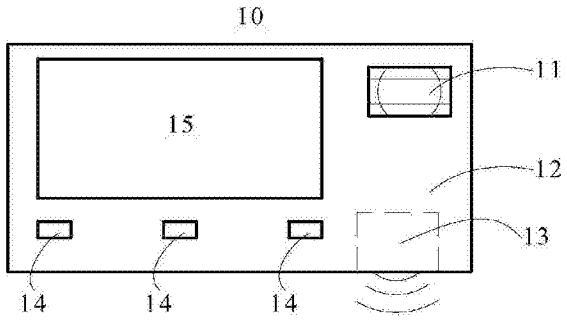
权利要求书3页 说明书10页 附图4页

(54)发明名称

安全设备、加密机、安全设备操作系统及操作方法

(57)摘要

本发明提供一种安全设备，包括芯片。该芯片中设置有第一运算单元，且芯片中还存储有上一次操作的年轮数据或初始年轮数据，第一运算单元能够进行第一次运算以生成第一验证数据，参与第一次运算的数据包括本次操作数据和上一次操作的年轮数据或初始年轮数据，安全设备能够将第一验证数据和本次操作数据发送至与安全设备对应的加密机进行验证，当第一验证数据通过加密机的验证时，第一运算单元能够进行第二次运算以生成本次操作的年轮数据，参与第二次运算的数据包括本次操作的计数器和上一次操作的年轮数据或初始年轮数据本发明还提供一种加密机、一种安全设备操作系统和一种操作方法。本发明所提供的安全设备具有很高的安全性，不易被克隆。



CN 103701599 B

1.一种安全设备，该安全设备包括芯片，其特征在于，所述芯片中设置有第一运算单元，当所述安全设备未经过操作时，所述芯片中还存储有初始年轮数据，当所述安全设备被操作过至少一次时，所述芯片中还存储有上一次操作的年轮数据，所述第一运算单元进行没有逆运算的第一次运算以生成第一验证数据，参与所述第一次运算的数据包括本次操作数据和所述上一次操作的年轮数据或所述初始年轮数据，所述安全设备将所述第一验证数据和所述本次操作数据发送至与所述安全设备对应的加密机进行验证，当所述第一验证数据通过所述加密机的验证时，所述第一运算单元进行没有逆运算的第二次运算以生成本次操作的年轮数据，

当本次操作为首次操作时，参与第二次运算的数据包括本次操作的计数器和所述初始年轮数据；

当本次操作为第二次或第二次以后的操作时，参与第二次运算的数据包括本次操作的计数器和所述上一次操作的年轮数据。

2.根据权利要求1所述的安全设备，其特征在于，所述第一次运算和所述第二次运算均为哈希运算。

3.根据权利要求1或2所述的安全设备，其特征在于，所述芯片中设置有电可擦写存储器，所述上一次操作的年轮数据、所述初始年轮数据和所述本次操作的年轮数据均存储在所述电可擦写存储器中。

4.根据权利要求1或2所述的安全设备，其特征在于，所述芯片中存储有密钥、安全设备数据和生成第一随机数的第一随机数协处理器，所述第一运算单元利用所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子，且所述第一运算单元对所述初始年轮数据生成因子进行没有逆运算的第二次初始运算，以生成所述初始年轮数据，并将所述初始年轮数据存储在所述芯片中。

5.根据权利要求4所述的安全设备，其特征在于，所述第一次初始运算为分散式算法，所述第二次初始运算为哈希运算。

6.根据权利要求4所述的安全设备，其特征在于，所述安全设备数据至少包括所述安全设备的持有者的姓名、出生日期、居住地址、身份证号、所述安全设备的发行机构的名称和所述安全设备的有效期。

7.一种加密机，其特征在于，所述加密机对应于权利要求1至6中任意一项所述的安全设备，所述加密机上存储有第二运算单元和所述上一次操作的年轮数据或所述初始年轮数据，且所述加密机对所述第一验证数据进行验证，当所述第一验证数据通过验证时，所述加密机向设置有安全设备账户的密钥管理中心发送验证通过回执和所述本次操作数据，以及向所述安全设备发送所述验证通过回执，并且所述第二运算单元进行与所述第二次运算相同的第四次运算以生成所述本次操作的年轮数据。

8.根据权利要求7所述的加密机，其特征在于，所述加密机中存储有第二运算单元和所述上一次操作的年轮数据或所述初始年轮数据，所述第二运算单元进行与所述第一次运算相同的第三次运算，以生成第二验证数据，所述加密机将所述第一验证数据和所述第二验证数据进行比对，当所述第一验证数据与所述第二验证数据相同时，生成所述验证通过回执。

9.根据权利要求8所述的加密机，其特征在于，当所述安全设备的芯片中存储有密钥、

安全设备数据和生成第一随机数的第一随机数协处理器时，所述加密机中存储有所述密钥、所述安全设备数据和生成第二随机数的第二随机数协处理器，所述第一随机数与所述第二随机数相同，所述第二运算单元利用所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子，且所述第二运算单元对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据。

10.一种安全设备操作系统，其特征在于，所述安全设备操作系统包括权利要求7至9中任意一项所述的加密机、密钥管理中心和权利要求1至6中任意一项所述的安全设备，所述密钥管理中心中设置有与所述安全设备对应的安全设备账户，当所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，所述密钥管理中心更改所述安全设备账户的备案记录。

11.根据权利要求10所述的安全设备操作系统，其特征在于，所述安全设备账户为所述安全设备的持有者的货币存储账户，所述备案记录为所述安全设备账户的余额；或者所述安全设备账户为所述安全设备的持有者的户籍账户。

12.一种安全设备操作系统的操作方法，其特征在于，所述安全设备操作系统为权利要求10或11所述的安全设备操作系统，所述操作方法包括以下步骤：

S1、所述安全设备利用所述第一运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第一次运算，以生成第一验证数据；

S2、所述安全设备将所述第一验证数据和所述本次操作数据发送至所述加密机；

S3、所述加密机对所述第一验证数据进行验证；

当所述第一验证数据通过验证时，所述操作方法还包括：

S41、所述加密机生成通过验证回执，并向所述密钥管理中心发送所述本次操作数据和所述验证通过回执，以及向所述安全设备发送所述验证通过回执；

S42、所述加密机利用所述上一次操作的年轮数据和本次操作的流水号进行第四次运算生成本次操作的年轮数据；

S51、所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，更改所述安全设备账户的备案记录；

S61、所述安全设备接收到所述验证通过回执后利用所述上一次操作的年轮数据和本次操作的流水号进行第二次运算生成本次操作的年轮数据。

13.根据权利要求12所述的操作方法，其特征在于，当所述第一验证数据未通过验证时，所述操作方法还包括：

S43、所述加密机生成验证失败回执，并向所述密钥管理中心和所述安全设备发送所述验证失败回执；

S52、当所述密钥管理中心接收到所述验证失败回执时，冻结所述安全设备账户。

14.根据权利要求13所述的操作方法，其特征在于，所述步骤S3中的对所述第一验证数据进行验证具体包括：

S31、所述加密机利用所述第二运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第三次运算，以生成第二验证数据；

S32、所述加密机将所述第一验证数据和所述第二验证数据进行比对；

当所述第一验证数据与所述第二验证数据相同时，则进行所述步骤S41，当所述第一验证数据与所述第二验证数据不同时，则进行所述步骤S43。

15.根据权利要求14所述的操作方法，其特征在于，当所述安全设备的芯片中存储有密钥、安全设备数据和生成第一随机数的第一随机数协处理器、且所述加密机中存储有所述密钥、所述安全设备数据和生成第二随机数的第二随机数协处理器时，所述操作方法还包括在所述安全设备中进行的：

S01、利用所述第一运算单元对所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子；

S02、利用所述第一运算单元对所述初始年轮数据生成因子进行第二次初始运算，以生成所述初始年轮数据；

S03、使得所述安全设备中的初始年轮数据生成因子消失；

以及在所述加密机中进行的：

S04、利用所述第二运算单元对所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子；

S05、利用所述第二运算单元对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据；

S06、使得所述加密机中的初始年轮数据生成因子消失。

安全设备、加密机、安全设备操作系统及操作方法

技术领域

[0001] 本发明涉及安全设备领域，具体地，涉及一种安全设备、一种与该安全设备对应的加密机、一种包括所述安全设备和所述加密机的安全设备操作系统和一种操作所述安全设备操作系统的操作方法。

背景技术

[0002] 目前的安全设备(例如，银行卡或购物卡等)中多存储有诸如个人识别码、密钥、数字签名等个人信息。该个人信息用于对安全设备持有者进行身份验证，或者上述个人信息可以用于在进行操作时计算某些校验数据。

[0003] 安全设备发行完成后，写入安全设备的个人信息不可更改，但是，由于在在操作的过程中，所述个人信息出现在链路中，因此很有可能被人恶意截获。一旦个人信息被他人获取，就可以克隆所述安全设备，并且克隆获得的安全设备的身份也是“合法”的。上述情况会对安全设备的持有者造成损失。

[0004] 因此，如何避免安全设备被克隆成为本领域亟待解决的技术问题。

发明内容

[0005] 本发明的目的在于提供一种安全设备、一种与该安全设备对应的加密机、一种包括所述安全设备和所述加密机的安全设备操作系统和一种操作所述安全设备操作系统的操作方法。所述安全设备不易被克隆。

[0006] 为了实现上述目的，作为本发明的一个方面，提供一种安全设备，该安全设备包括芯片，其中，所述芯片中设置有第一运算单元，且所述芯片中还存储有上一次操作的年轮数据或初始年轮数据，所述第一运算单元能够进行没有逆运算的第一次运算以生成第一验证数据，参与所述第一次运算的数据包括本次操作数据和所述上一次操作的年轮数据或所述初始年轮数据，所述安全设备能够将所述第一验证数据和所述本次操作数据发送至与所述安全设备对应的加密机进行验证，当所述第一验证数据通过所述加密机的验证时，所述第一运算单元能够进行没有逆运算的第二次运算以生成本次操作的年轮数据，参与第二次运算的数据包括本次操作的计数器和所述上一次操作的年轮数据或所述初始年轮数据。

[0007] 优选地，所述第一次运算和所述第二次运算均为哈希运算。

[0008] 优选地，所述芯片中设置有电可擦写存储器，所述上一次操作的年轮数据、所述初始年轮数据和所述本次操作的年轮数据均存储在所述电可擦写存储器中。

[0009] 优选地，所述芯片中存储有密钥、安全设备数据和生成第一随机数的第一随机数协处理器，所述第一运算单元能够利用所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子，且所述第一运算单元能够对所述初始年轮数据生成因子进行没有逆运算的第二次初始运算，以生成所述初始年轮数据，并将所述初始年轮数据存储在所述芯片中。

[0010] 优选地，所述第一次初始运算为分散式算法，所述第二次初始运算均哈希运算。

[0011] 优选地，所述安全设备数据至少包括所述安全设备的持有者的姓名、出生日期、居住地址、身份证号、所述安全设备的发行机构的名称和所述安全设备的有效期。

[0012] 作为本发明的另一个方面，提供一种加密机，其中，所述加密机对应于本发明所提供的上述安全设备，所述加密机上设置有第二运算单元和所述上一次操作的年轮数据或所述初始年轮数据，且所述加密机能够对所述第一验证数据进行验证，当所述第一验证数据通过验证时，所述加密机能够向设置有安全设备账户的密钥管理中心发送验证通过回执和本次操作数据，以及向所述安全设备发送所述验证通过回执，并且所述第二运算单元能够进行与所述第二次运算相同的第四次运算以生成所述本次操作的年轮数据。

[0013] 优选地，所述加密机中存储有第二运算单元和所述上一次操作的年轮数据或所述初始年轮数据，所述第二运算单元能够进行与所述第一次运算相同的第三次运算，以生成第二验证数据，所述加密机能够将所述第一验证数据和所述第二验证数据进行比对，当所述第一验证数据与所述第二验证数据相同时，生成所述验证通过回执。

[0014] 优选地，所述加密机中存储有所述密钥、所述安全设备数据和能够生成第二随机数的第二随机数协处理器，所述第一随机数与所述第二随机数相同，所述第二运算单元能够利用所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子，且所述第二运算单元能够对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据。

[0015] 作为本发明的再一个方面，提供一种安全设备操作系统，其特中，所述安全设备操作系统包括本发明所提供的上述加密机、密钥管理中心和本发明所提供的上述安全设备，所述密钥管理中心中设置有与所述安全设备对应的安全设备账户，当所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，所述密钥管理中心能够更改所述安全设备账户的备案记录。

[0016] 优选地，所述安全设备账户为所述安全设备的持有者的货币存储账户，所述备案记录为所述安全设备账户的余额；或者所述安全设备账户为所述安全设备的持有者的户籍账户。

[0017] 作为本发明的还一个方面，提供一种安全设备操作系统的操作方法，其中，所述安全设备操作系统为本发明所提供的上述安全设备操作系统，所述操作方法包括以下步骤：

[0018] S1、所述安全设备利用所述第一运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第一次运算，以生成第一验证数据；

[0019] S2、所述安全设备将所述第一验证数据和所述本次操作数据发送至所述加密机；

[0020] S3、所述加密机对所述第一验证数据进行验证；

[0021] 当所述第一验证数据通过验证时，所述操作方法还包括：

[0022] S41、所述加密机生成通过验证回执，并向所述密钥管理中心发送所述本次操作数据和所述验证通过回执，以及向所述安全设备发送所述验证通过回执；

[0023] S42、所述加密机利用所述上一次操作的年轮数据和本次操作的流水号进行第四次运算生成本次操作的年轮数据；

[0024] S51、所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，更改所述安全设备账户的备案记录；

[0025] S61、所述安全设备接收到所述验证通过回执后利用所述上一次操作的年轮数据和本次操作的流水号进行第二次运算生成本次操作的年轮数据。

[0026] 优选地，当所述第一验证数据未通过验证时，所述操作方法还包括：

[0027] S43、所述加密机生成验证失败回执，并向所述密钥管理中心和所述安全设备发送所述验证失败回执；

[0028] S52、当所述密钥管理中心接收到所述验证失败回执时，冻结所述安全设备账户。

[0029] 优选地，所述步骤S3中的对所述第一验证数据进行验证具体包括：

[0030] S31、所述加密机利用所述第二运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第三次运算，以生成第二验证数据；

[0031] S32、所述加密机将所述第一验证数据和所述第二验证数据进行比对；

[0032] 当所述第一验证数据与所述第二验证数据相同时，则进行所述步骤S41，当所述第一验证数据与所述第二验证数据不同时，则进行所述步骤S43。

[0033] 优选地，所述操作方法还包括在所述安全设备中进行的：

[0034] S01、利用所述第一运算单元对所述密钥、所述安全设备数据和所述随机数进行第一次初始运算，以获得初始年轮数据生成因子；

[0035] S02、利用所述第一运算单元对所述初始年轮数据生成因子进行第二次初始运算，以生成所述初始年轮数据；

[0036] S03、使得所述安全设备中的初始年轮数据生成因子消失；

[0037] 以及在所述加密机中进行的：

[0038] S04、利用所述第二运算单元对所述密钥、所述安全设备数据和所述随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子；

[0039] S05、利用所述第二运算单元对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据；

[0040] S06、使得所述加密机中的初始年轮数据生成因子消失。

[0041] 在对本发明所提供的安全设备进行操作的整个过程中，无论是初始年轮数据、上一次操作的年轮数据和本次操作的年轮数据均没有以任何明文的形式出现在操作链路中，因此不会被直接截获。由于第一次运算和第二次运算均没有逆运算，因此，即便第一验证数据被恶意截获，也不会由该第一验证数据反推出初始年轮数据或上一次操作的年轮数据。因此，即使获得了所述安全设备的个人信息，仍然不能获得安全设备上的年轮数据，没有年轮数据的安全设备产生的第一验证数据并不能通过加密机验证，仍然不能对所述安全设备进行操作。因此，本发明所提供的安全设备具有很高的安全性，难以被克隆。

附图说明

[0042] 附图是用来提供对本发明的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本发明，但并不构成对本发明的限制。在附图中：

[0043] 图1是本发明所提供的安全设备的一种实施方式的示意图；

[0044] 图2是本发明所提供的安全设备的另一种实施方式的示意图；

[0045] 图3是本发明所提供的交易系统的示意图；

[0046] 图4是本发明所提供的交易方法的流程示意图；

[0047] 图5是图4中所示的交易方法中的步骤S3的优选实施方式；

[0048] 图6是在安全设备中生成初始年轮数据的流程示意图；

[0049] 图7是在加密机中生成初始年轮数据的流程示意图。

[0050] 附图标记说明

[0051] 10：安全设备 11：芯片

[0052] 12：卡本体 13：内置通讯模块

[0053] 14：内置输入模块 15：内置显示模块

[0054] 16：连接端 20：操作终端

[0055] 21：外接显示模块 22：外接输入模块

[0056] 30：加密机 40：密钥管理中心

具体实施方式

[0057] 以下结合附图对本发明的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本发明，并不用于限制本发明。

[0058] 作为本发明的一个方面，如图1和图2所示，提供一种安全设备10，该安全设备10包括芯片11，其中，该芯片11中设置有第一运算单元，且芯片11中还存储有上一次操作的年轮数据或初始年轮数据，所述第一运算单元可以进行没有逆运算的第一次运算以生成第一验证数据，参与所述第一次运算的数据包括本次操作数据和所述上一次操作的年轮数据或所述初始年轮数据，安全设备10可以将所述第一验证数据和所述本次操作数据发送至与安全设备10对应的加密机进行验证，当所述第一验证数据通过所述加密机的验证时，所述第一运算单元可以进行没有逆运算的第二次运算以生成本次操作的年轮数据，参与第二次运算的数据包括本次操作的流水号和所述上一次操作的年轮数据或所述初始年轮数据。

[0059] 在本发明中“年轮数据”是一种形象的说法，像树木的年轮随着生长时间而增加一样，安全设备中的“年轮数据”能够随着操作次数而不断改变。“年轮数据”的本质为经过特定计算(包括第一次运算和第二次运算)的一组表征所述安全设备的操作历史的数据。

[0060] 应当理解的是，如果在进行本次操作之前，安全设备10并没有进行过操作(即，安全设备10为刚制造完成的安全设备或者制造完成尚未使用)，则安全设备10中存储的是初始年轮数据，参与第一次运算的数据包括本次操作数据和所述初始年轮数据，参与第二次运算的数据包括本次操作的流水号和所述初始年轮数据；如果在进行本次操作之前，安全设备10进行过操作，则安全设备中存储的是上一次操作的年轮数据，参与第一次运算的数据包括所述上一次操作的年轮数据和本次操作数据，参与第二运算的数据包括本次操作的计数器和所述上一次操作的年轮数据。

[0061] 在本发明中，对安全设备的类型并不做限定，因此，对操作的类型也不做限定。

[0062] 例如，所述安全设备可以用作银行卡，对所述银行卡进行的操作则为货币交易。在这种情况中，所述本次操作数据可以包括本次货币交易的金额、安全设备的账户信息(包括安全设备的账户名和安全设备的账号)等。

[0063] 再例如，所述安全设备可以为手机卡，所述操作可以为对所述手机卡进行充值。在这种情况中，所述本次操作数据可以包括本次充值的金额、手机卡的手机号等。

[0064] “本次操作的计数器”是一组数字，可以用于表征本次操作的顺序号。例如，所述

“本次操作的计数器”可以为本次操作的流水号。

[0065] 对于一个安全设备10而言，每进行一次操作都会生成一个本次操作的年轮数据，并且生成该本次操作的年轮数据时需要用到上一次操作的年轮数据。因此，不同的安全设备10上的年轮数据都不相同。而且，每个安全设备上的年轮数据都是滚动变化的，通过验证安全设备上的年轮数据可以验证该安全设备的合法性，降低安全设备被克隆盗用的风险。

[0066] 在整个操作的过程中，无论是初始年轮数据、上一次操作的年轮数据和本次操作的年轮数据均没有以明文的形式出现在操作链路中，因此不会被直接截获。

[0067] 由于第一次运算和第二次运算均没有逆运算，因此，即便第一验证数据被人恶意截获，也难以由该第一验证数据反推出初始年轮数据或上一次操作的年轮数据。因此，即使获得了所述安全设备10的个人信息，仍然不能获得安全设备上的年轮数据，没有年轮数据的安全设备10产生的第一验证数据并不能通过加密机验证，仍然不能进行操作。因此，本发明所提供的安全设备10具有很高的安全性，难以被克隆。

[0068] 即使安全设备被克隆盗用，由于对该安全设备进行操作时需要和后台(下文中的密钥管理中心)发生操作数据传递，错误的年轮数据会被后台即可发现，从而即可锁定被盗用的安全设备。

[0069] 在本发明中，对第一次运算和第二次运算的具体类型并没有具体限制，只要没有逆运算即可。在数学领域中，没有逆运算的运算类型有很多种，例如，第一次运算和第二次运算可以均为哈希运算。一长列数据经哈希运算后可以生成短列数据，因此，第一次运算和第二次运算均采用哈希运算的优点还在于，可以使得生成较短的第一验证数据以及本次操作的年轮数据，节省安全设备的存储空间。

[0070] 在本发明中，对哈希运算的类型并不做限定，例如，所述第一次运算可以为MD5运算，也可以为SHA1运算，也可以为SHA256运算。同样地，第二次运算可以为MD5运算，也可以为SHA1运算，也可以为SHA256运算。

[0071] 当所述安全设备丢失时，安全设备的持有人可以重新补办一个安全设备，该安全设备中只存储有初始年轮数据，且该初始年轮与源安全设备的初始年轮数据也不相同。补办的安全设备可以与原来的安全设备共用一个卡号，但由于两个安全设备中的年轮数据不同，在利用安全设备进行操作的过程中，加密机只识别补办的安全设备的年轮数据，原来的安全设备相当于自动挂失，避免对安全设备的持有人造成损失。

[0072] 例如，如果安全设备为购物卡，当购物卡丢失时，持有人重新补办购物卡，原购物卡自动挂失，即便有人捡到原购物卡也不能进行消费，从而减小了购物卡持有人的损失。

[0073] 与原安全设备相比，补办的安全设备的卡号并没有变化，因此减少了很多不必要的麻烦。例如，如果安全设备为工资卡，如果工资卡丢失，持有人只需补办一张，而无需通知财务更改工资卡账号，省去了不必要的麻烦。

[0074] 下文中将描述如何利用所述加密机对第一验证数据进行验证，这里先不赘述。

[0075] 如上文中所述，为了增加操作的安全性，优选地，参与所述第一次运算的数据还可以包括本次操作的计数器。容易理解的是，在对所述安全设备进行每次操时作都会产生一个新的计数器。

[0076] 在本发明中，对所述初始年轮数据、上一次操作的年轮数据和本次操作的年轮数据的存储方式并没有特殊的限定。例如，可以将所述初始年轮数据、上一次操作的年轮数据

和本次操作的年轮数据均存储在安全设备10的芯片内，即，将所述初始数据和历次操作的年轮数据均存储在安全设备10的芯片内。

[0077] 为了减小年轮数据占用的空间，并且便于第一运算单元调用所述上一次操作的年轮数据，优选地，可以在芯片11中设置有电可擦写存储器，将所述上一次操作的年轮数据、所述初始年轮数据和所述本次操作的年轮数据均存储在所述电可擦写存储器中。

[0078] 电可擦写存储器的特性为断电后仍然可以保存该电可擦写存储器存储的数据，并且电可擦写存储器具有可擦除性，便于利用上一次操作的年轮数据生成本次操作的年轮数据。所以，所述上一次操作的年轮数据、所述初始年轮数据和所述本次操作的年轮数据并不是同时存在的。即，在进行本次操作之前，电可擦写存储器中存储的是上一次操作的年轮数据或所述初始年轮数据，在进行本次操作之后，电可擦写存储器中存储的是本次操作的年轮数据。

[0079] 如上文中所述，第一验证数据可以发送至于安全设备10对应的加密机，因此，作为本发明的一种优选实施方式，如图1所示，安全设备10可以包括内置通讯模块13，该内置通讯模块13可以与安全设备10对应的加密机进行通讯，以将所述本次操作数据和安全设备10上生成的所述第一验证数据发送至所述加密机。

[0080] 进一步地，安全设备10还可以包括内置输入模块14和/或内置显示模块15，内置输入模块14可以向芯片11输入操作指令，内置显示模块15可以显示操作界面。

[0081] 容易理解的是，安全设备10可以包括卡本体12，内置通讯模块13、内置输入模块14和内置显示模块15均设置在卡本体12上。

[0082] 在图1中所示的实施方式中，安全设备10还可以包括内置的电源模块，该电源模块可以在对所述安全设备进行操作时为芯片11、内置通讯模块13、内置输入模块14和内置显示模块15供电。

[0083] 当然，如图2所示，作为本发明的另一种优选实施方式，安全设备10可以包括连接端16，该连接端16用于和外接输入模块22、外接显示模块21和外接通讯模块中的至少一者相连。即，安全设备10可以通过连接端16与操作终端20相连，通过操作终端20的外接输入模块22可以向芯片11输入操作指令，外接显示模块21可以显示操作界面，外接通讯模块可以与加密机通讯，以将所述本次操作数据和安全设备10上生成的所述第一验证数据发送至所述加密机。

[0084] 在图2所示的实施方式中，安全设备10也可以包括卡本体12，芯片11和连接端16均设置在卡本体12上。并且，在图2所示的实施方式中，操作终端20可以为芯片11供电。操作终端可以为手机、电脑、PAD等。连接端16可以为USB接口。

[0085] 如上文中所述，当安全设备10在进行本次操作之前并未进行过操作时，安全设备10中存储有初始年轮数据。在本发明中，对生成初始年轮数据的方法并不做限定。为了进一步防止安全设备10被克隆，从而进一步提高安全设备10的安全性，优选地，芯片11中可以存储有密钥、安全设备数据和生成第一随机数的第一随机数协处理器，所述第一运算单元可以利用所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子，且所述第一运算单元可以对所述初始年轮数据生成因子进行没有逆运算的第二次初始运算，以生成所述初始年轮数据，并将所述初始年轮数据存储在所述芯片中。所述初始年轮数据生成因子相当于过程密钥，生成所述初始年轮数据后，所述初始年轮

数据生成因子自动消失。此处的“自动消失”是指，可以将所述初始年轮数据生成因子从所述安全设备中删除，也可以利用其它数据覆盖所述初始年轮数据生成因子。

[0086] 在本发明中，当所述安全设备为银行卡或电子钱包等可以进行货币交易的设备时，所述安全设备数据可以包括安全设备的账号、安全设备的持有人信息等。

[0087] 当所述安全设备为该安全设备的持有人的身份证时，所述安全设备数据包括所述安全设备的持有者的姓名、出生日期、居住地址和身份证号。更进一步地，所述安全设备数据还包括所述安全设备的发行机构的名称和所述安全设备的有效期。

[0088] 所述本次操作数据可以包括新的安全设备数据，例如，安全设备的持有者的新居住地址等。

[0089] 当本发明所提供的安全设备用作身份证时，可以防止有人恶意伪造身份证件。具体地，安全设备中除了存储有所述安全设备的持有者的姓名、出生日期、居住地址和身份证号、所述安全设备的发行机构的名称和所述安全设备的有效期等安全设备数据之外，还存储有上一次操作的年轮数据或者初始年轮数据。在掌握了上述安全设备数据的情况下，如没有掌握所述上一次操作的年轮数据或所述初始年轮数据，伪造的身份证并不能通过加密机的验证，所以并不能使用。而所述上一次操作的年轮数据或所述初始年轮数据并不会以任何明文的形式出现在操作的链路中，所以不会被截获。

[0090] 当所述安全设备用作身份证时，对安全设备的操作可以是更改所述安全设备的持有者的居住地、延长所述安全设备的有效期等。每更改一次安全设备数据，将生成本次操作的年轮数据。

[0091] 第一次初始运算可以为分散式算法，即，在加密机端对所述密钥、所述安全设备数据和所述第一随机数进行分散，以生成所述初始年轮数据生成因子。

[0092] 为了增加安全设备的安全性，第二次初始运算应当没有逆运算。因此，通过初始年轮数据并不能反推出所述安全设备的初始年轮数据。在所述安全设备进行操作的过程中，所述初始年轮数据生成因子和所述初始年轮数据均没有以任何明文的形式出现在操作链路中。

[0093] 作为本发明的一种优选实施方式，第二次初始运算可以为哈希运算。此处采用哈希运算的有益效果与第一次运算和第二次运算采用哈希运算的有益效果类似，这里不再重述。

[0094] 此处所述的第一随机数是由第一随机数协处理器随机产生的数据，如何利用第一随机数协处理器产生第一随机数是本领域所公知的，这里不再赘述。

[0095] 作为本发明的另一个方面，如图3所示，提供一种与所述安全设备对应的加密机30，该加密机30中存储有第二运算单元和所述上一次操作的年轮数据或所述初始年轮数据，且加密机30可以对所述第一验证数据进行验证，当所述第一验证数据通过验证时，加密机30可以向设置有安全设备账户的密钥管理中心40发送验证通过回执和本次操作数据，并且加密机30还可以向安全设备10发送所述验证通过回执，此外，所述第二运算单元可以进行与所述第二次运算相同的第四次运算以生成所述本次操作的年轮数据。此处，第四次运算与第二次运算相同是指，第四次运算的算法与第二次运算相同，且参与第四次运算的数据与参与第二次运算的数据相同。

[0096] 在加密机30中可以同步产生并存储与安全设备10中相同的上一次操作的年轮数

据和本次操作的年轮数据，从而可以确保初始年轮数据、上一次操作的年轮数据和本次操作的年轮数据不会出现在操作链路中，从而提高了操作的安全性。

[0097] 在本发明中，对如何对第一验证数据进行验证并不作具体限定。例如，加密机30中的所述第二运算单元可以进行与所述第一次运算相同的第三次运算，以生成第二验证数据。此处，第三次运算与第一次运算相同是指，第一次运算和第三次运算采用的算法相同，且参与所述第三次运算的数据与参与所述第一次运算的数据相同。在对第一验证数据进行验证时，加密机30可以将所述第一验证数据和所述第二验证数据进行比对，当所述第一验证数据与所述第二验证数据相同时，生成所述验证通过回执。随后加密机30向密钥管理中心40发送所述验证通过回执和本次操作数据，并向安全设备10发送所述验证通过回执。

[0098] 优选地，如果安全设备10发送的第一验证数据不能通过加密机30的验证，则加密机30产生验证失败回执，并且，加密机30可以将所述验证失败回执发送至密钥管理中心40和安全设备10，以便于后续的操作（例如，密钥管理中心40在接收到验证失败回执后，将安全设备10对应的安全设备账户冻结）。

[0099] 如上文中所述，在进行本次操作之前，安全设备10并未进行过其他操作时，安全设备10中存储有所述初始年轮数据，相应地，加密机30中也存储有所述初始年轮数据。为了产生初始年轮数据并避免该初始年轮数据以明文的形式出现在操作链路中，优选地，加密机30中可以存储有所述密钥、所述安全设备数据和可以生成第二随机数（与安全设备10中的第一随机数相同）的第二随机数协处理器，所述第二运算单元可以利用所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三初始次运算，以获得所述初始年轮数据生成因子，且所述第二运算单元能够对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次运算，以生成所述初始年轮数据。生成所述初始年轮数据后，所述初始年轮数据生成因子自动消失。此处的“自动消失”是指，可以在加密机端将所述初始年轮数据生成因子从所述安全设备中删除，也可以利用其它数据覆盖所述初始年轮数据生成因子。

[0100] 应当理解的是，此处的第一次初始运算与所述第三次初始运算相同是指，第一次初始运算与第三次初始运算的算法相同，且参与第一次初始运算的数据和参与第三次初始运算的数据相同。同样地，第二次初始运算与所述第四次初始运算相同是指，第二次初始运算与第四次初始运算的算法相同，且参与第二次初始运算的数据和参与第四次初始运算的数据相同。

[0101] 在所述安全设备中进行完第一次初始运算之后，在安全设备中生成所述初始年轮数据因子，在所述加密机中进行完第三次初始运算之后，生成所述初始年轮数据因子。通过上述操作，安全设备和相应的加密机中存在相同的初始年轮数据因子，并且初始年轮数据因子并没有出现在操作链路中，因此不会在操作的过程中被人恶意截获。同样地，在所述安全设备中对该安全设备中的所述初始年轮数据因子进行第二次初始运算，以及在所述加密机中对该加密机中的所述初始年轮数据因子进行第四次初始运算可以分别且独立地在安全设备中和所述加密机中生成相同的初始年轮数据。该初始年轮数据也没有出现在操作链路中，因此不会在操作的过程中被人恶意截获。

[0102] 作为本发明的再一个方面，如图3所示，提供一种安全设备操作系统，起重，该安全设备操作系统包括本发明所提供的上述的加密机30、密钥管理中心40和本发明所提供的上

述安全设备10，密钥管理中心40上设置有与安全设备10对应的安全设备账户，当密钥管理中心40接收到所述验证通过回执和所述本次操作数据后，更改所述安全设备账户的备案记录。

[0103] 应当理解的是，当安全设备10通过连接端16与操作终端20相连时，所述操作系统还包括操作终端20。密钥管理中心40相当于安全设备的后台服务器。

[0104] 如上文中所述，所述安全设备可以具有多种不同的具体实施方式。例如，所述安全设备可以用作银行卡，或者所述安全设备可以用作该安全设备的持有者的身份证等。所述备案记录根据所述安全设备的应用场合的不同而不同。

[0105] 例如，当所述安全设备账户为所述安全设备的持有者的货币存储账户时(即，所述安全设备用作银行卡时)，所述备案记录为所述安全设备账户的余额。

[0106] 在上述实施方式中，密钥管理中心40更改安全设备10对应的安全设备账户的余额的同时，可以更改收款方的账户余额，或者向收款方账户所在的密钥管理中心发送指示，更改收款方账户的余额，以完成整个操作。

[0107] 当所述安全设备账户为所述安全设备的持有者的户籍账户(即，所述安全设备用作该安全设备的持有者的身份证)，户籍账户中对应的信息由安全设备的持有者的姓名、出生日期、居住地等，这些信息与所述安全设备数据一致。上文中所述的“更改所述安全设备账户的备案记录”可能包括更改安全设备的持有者的居住地址等信息。

[0108] 如果安全设备10发出的第一验证数据未能通过验证，则加密机30向安全设备10以及密钥管理中心40发出验证失败回执，密钥管理中心冻结安全设备10对应的安全设备账户，确保用户的财产安全。

[0109] 加密机30可以通过有线通讯或无线通讯与密钥管理中心40进行通讯。

[0110] 作为本发明的还一个方面，如图4所示，提供利用上述一种安全设备操作系统的操作方法，其中，所述安全设备操作系统为本发明所提供的上述安全设备操作系统，所述操作方法包括以下步骤：

[0111] S1、所述安全设备利用所述第一运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第一次运算，以生成第一验证数据；

[0112] S2、所述安全设备将所述第一验证数据和所述本次操作数据发送至所述加密机；

[0113] S3、所述加密机对所述第一验证数据进行验证；

[0114] 当所述第一验证数据通过验证时，所述操作方法还包括：

[0115] S41、所述加密机生成通过验证回执，并向所述密钥管理中心发送所述本次操作数据和所述验证通过回执，以及向所述安全设备发送所述验证通过回执；

[0116] S42、所述加密机利用所述上一次操作的年轮数据和本次操作的流水号进行第四次运算生成本次操作的年轮数据；

[0117] S51、所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，更改所述安全设备账户的备案记录；

[0118] S61、所述安全设备接收到所述验证通过回执后利用所述上一次操作的年轮数据和本次操作的流水号进行第二次运算生成本次操作的年轮数据。

[0119] 当第一验证数据未通过验证时，加密机不向密钥管理中心发送本次操作数据和验证通过回执。

[0120] 或者，为了进一步保护安全设备持有者的财产安全，优选地，当所述第一验证数据未通过验证时，所述操作方法还包括：

[0121] S43、所述加密机生成验证失败回执，并向所述密钥管理中心和所述安全设备发送所述验证失败回执；

[0122] S52、当所述密钥管理中心接收到所述验证失败回执时，冻结所述安全设备账户。

[0123] 如上文中所述，本发明对如何验证第一验证数据并没有特殊的规定，优选地，所述步骤S3中的对所述第一验证数据进行验证具体包括：

[0124] S31、所述加密机利用所述第二运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第三次运算，以生成第二验证数据；

[0125] S32、所述加密机将所述第一验证数据和所述第二验证数据进行比对；

[0126] 当所述第一验证数据与所述第二验证数据相同时，则进行所述步骤S41，当所述第一验证数据与所述第二验证数据不同时，则进行所述步骤S43。

[0127] 当安全设备在进行本次操作之前，并未进行过其他操作时，安全设备和加密机中存储有初始年轮数据。因此，优选地，所述操作方法还包括在所述安全设备中进行的生成所述初始年轮数据的步骤和在所述加密机中生成所述初始年轮数据的步骤。

[0128] 具体地，在所述安全设备中生成所述初始年轮数据的步骤包括：

[0129] S01、利用所述第一运算单元对所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子；

[0130] S02、利用所述第一运算单元对所述初始年轮数据生成因子进行第二次初始运算，以生成所述初始年轮数据；

[0131] S03、使得所述安全设备中的初始年轮数据生成因子消失。此处，可以将所述初始年轮数据生成因子删除，也可以利用其它数据将所述初始年轮数据生成因子覆盖。

[0132] 具体地，在所述加密机中生成所述初始年轮数据的步骤包括：

[0133] S04、利用所述第二运算单元对所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子；

[0134] S05、利用所述第二运算单元对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据；

[0135] S06、使得所述加密机中的初始年轮数据生成因子消失。此处，可以将所述初始年轮数据生成因子删除，也可以利用其它数据将所述初始年轮数据生成因子覆盖。

[0136] 容易理解的是，在所述安全设备中进行的生成所述初始年轮数据的步骤和在所述加密机中生成所述初始年轮数据的步骤可以是同时进行的。

[0137] 可以理解的是，以上实施方式仅仅是为了说明本发明的原理而采用的示例性实施方式，然而本发明并不局限于此。对于本领域内的普通技术人员而言，在不脱离本发明的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本发明的保护范围。

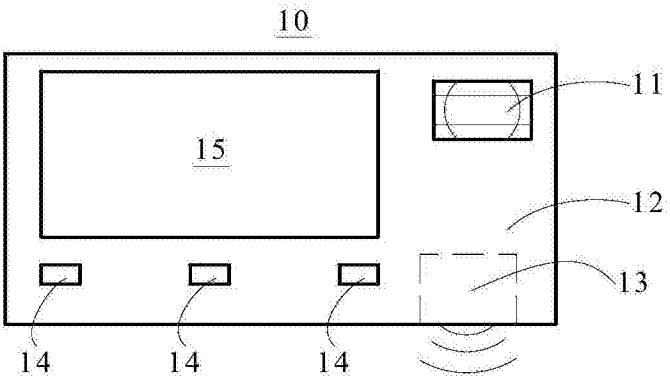

10
11
15
12
13
14
14
14

图1

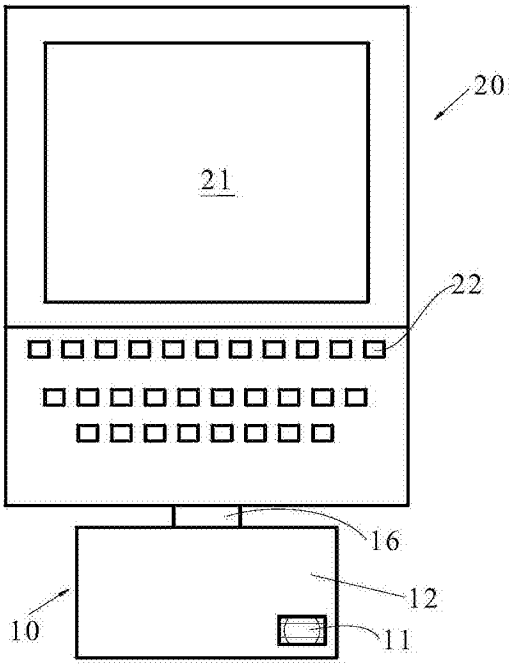

20
21
22
16
12
10
11

图2

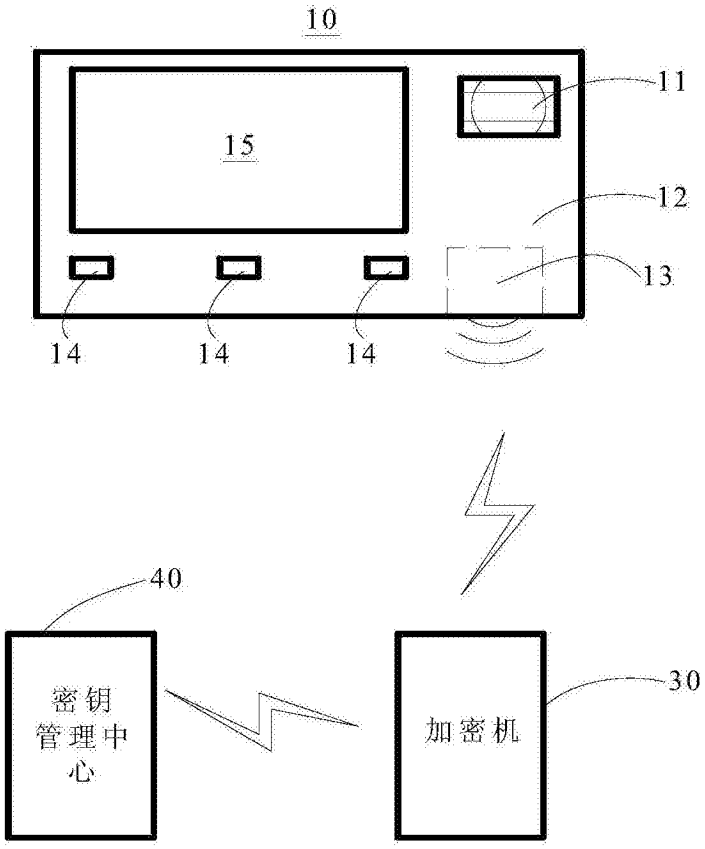

10
11
15
12
13
14
14
14
40
密钥管理中心
加密机
30

图3

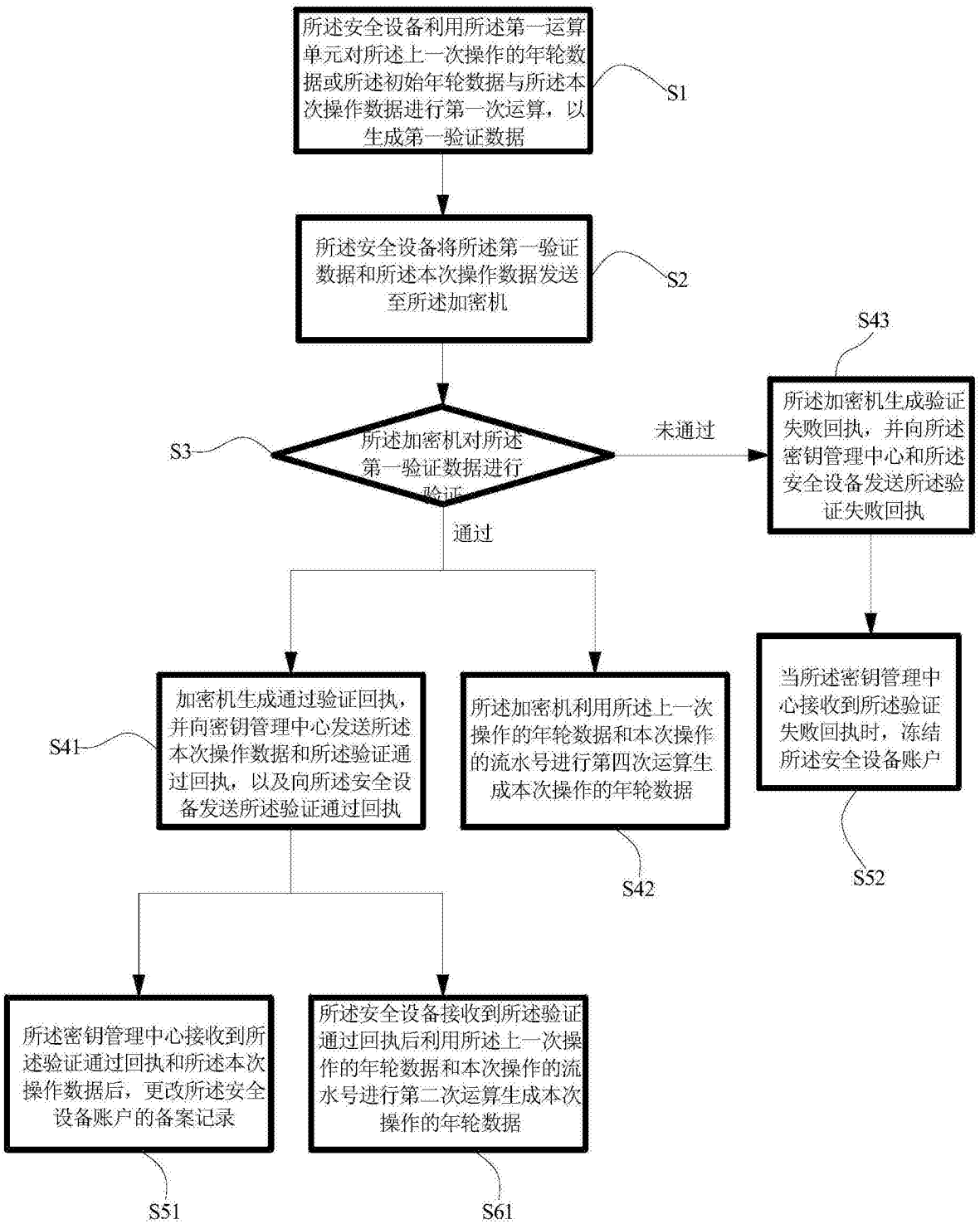

所述安全设备利用所述第一运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第一次运算，以生成第一验证数据
S1
所述安全设备将所述第一验证数据和所述本次操作数据发送至所述加密机
S2
S3
所述加密机对所述第一验证数据进行验证
未通过
S43
所述加密机生成验证失败回执，并向所述密钥管理中心和所述安全设备发送所述验证失败回执
通过
加密机生成通过验证回执，并向密钥管理中心发送所述本次操作数据和所述验证通过回执，以及向所述安全设备发送所述验证通过回执
S41
所述加密机利用所述上一次操作的年轮数据和本次操作的流水号进行第四次运算生成本次操作的年轮数据
S42
当所述密钥管理中心接收到所述验证失败回执时，冻结所述安全设备账户
S52
所述密钥管理中心接收到所述验证通过回执和所述本次操作数据后，更改所述安全设备账户的备案记录
S51
所述安全设备接收到所述验证通过回执后利用所述上一次操作的年轮数据和本次操作的流水号进行第二次运算生成本次操作的年轮数据
S61

图4

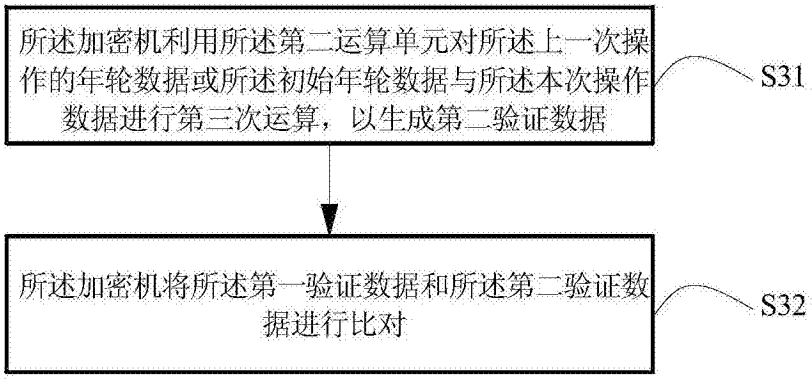

所述加密机利用所述第二运算单元对所述上一次操作的年轮数据或所述初始年轮数据与所述本次操作数据进行第三次运算，以生成第二验证数据
S31
所述加密机将所述第一验证数据和所述第二验证数据进行比对
S32

图5

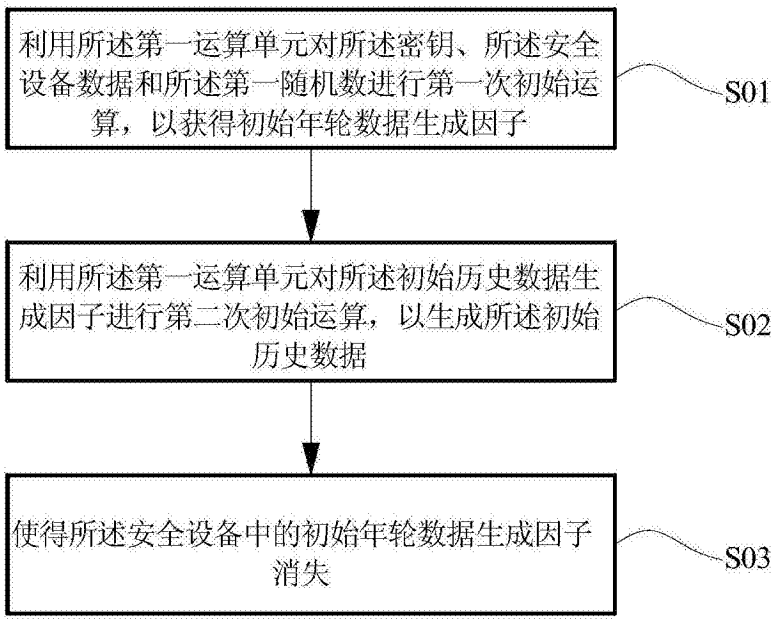

利用所述第一运算单元对所述密钥、所述安全设备数据和所述第一随机数进行第一次初始运算，以获得初始年轮数据生成因子
S01
利用所述第一运算单元对所述初始历史数据生成因子进行第二次初始运算，以生成所述初始历史数据
S02
使得所述安全设备中的初始年轮数据生成因子消失
S03

图6

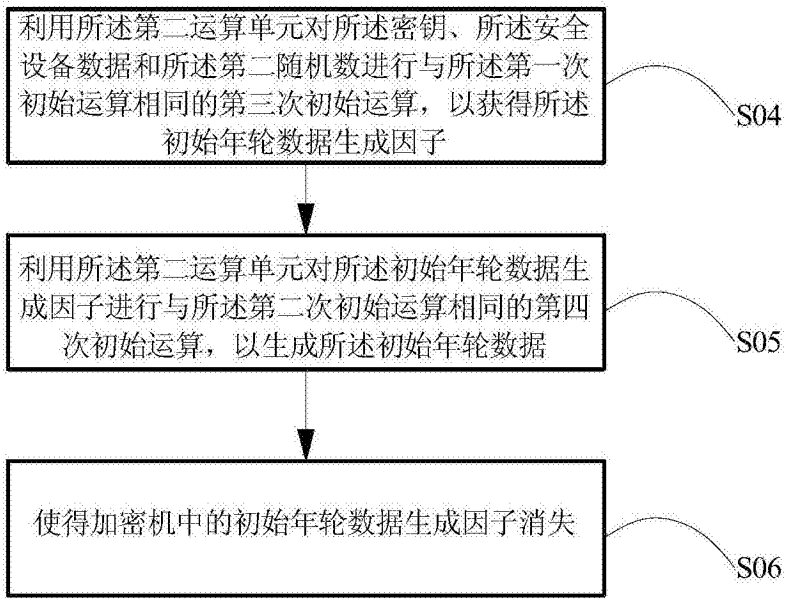

利用所述第二运算单元对所述密钥、所述安全设备数据和所述第二随机数进行与所述第一次初始运算相同的第三次初始运算，以获得所述初始年轮数据生成因子
S04
利用所述第二运算单元对所述初始年轮数据生成因子进行与所述第二次初始运算相同的第四次初始运算，以生成所述初始年轮数据
S05
使得加密机中的初始年轮数据生成因子消失
S06

图7