(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 104583026 B
(45)授权公告日 2018.07.20

(21)申请号 201380043120.3

(22)申请日 2013.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 104583026 A

(43)申请公布日 2015.04.29

(30)优先权数据
61/695,155 2012.08.30 US
13/969,133 2013.08.16 US

(85)PCT国际申请进入国家阶段日
2015.02.13

(86)PCT国际申请的申请数据
PCT/US2013/057603 2013.08.30

(87)PCT国际申请的公布数据
WO2014/036453 EN 2014.03.06

(73)专利权人 德克萨斯仪器股份有限公司
地址 美国德克萨斯州

(72)发明人 J-M·霍

(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民

(51)Int.Cl.
B60R 25/10(2013.01)
B60R 25/24(2013.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
G07C 9/00(2006.01)

(56)对比文件
US 2010/0208894 A1,2010.08.19,
US 2012/0155645 A1,2012.06.21,
CN 1914393 A,2007.02.14,
CN 102114826 A,2011.07.06,
CN 201570073 U,2010.09.01,

审查员 王天华

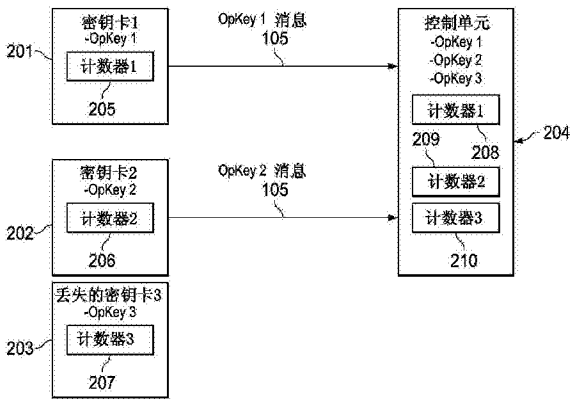
权利要求书2页 说明书4页 附图4页

(54)发明名称

单向密钥卡和交通工具配对的验证、保留及撤销

(57)摘要

本发明实施例提供了用于密钥卡进行控制单元验证、保留和撤销的方法。在密钥卡(201,202)与控制单元(204)之间的初始配对之后,设备就共享秘密的操作密钥(OpKey1,2)。对于验证,密钥卡将128位计数器的8个最低阶位和计数器(208,209)的AES-128OpKey加密值的一些位发送到控制单元(204)。对于密钥撤销和保留,控制单元(204)经提示进入OpKey保留和撤销模式。随后,由用户提示剩余的或新的密钥卡(201,202)中的每一个将验证消息(105)发送到控制单元(204)。当控制单元(204)经提示离开OpKey保留和撤销模式时,其仅保留刚好在进入和离开OpKey保留和撤销模式之前发送有效验证消息(105)的密钥卡(201,202)的OpKey。



CN 104583026 B

1.一种密钥卡设备,其包括:

发送器,其被配置为发送信号;

存储器,其被配置为储存密钥卡计数器和操作密钥即OpKey;以及

耦合到所述发送器和存储器的处理器,所述处理器被配置为:

生成所述密钥卡计数器的OpKey加密值;

发送消息,其中发送的消息包括未使用所述OpKey加密的所述密钥卡计数器的选定数目的最低阶位和所述密钥卡计数器的所述OpKey加密值的一些预定数目的位。

2.根据权利要求1所述的密钥卡设备,其中所述密钥卡计数器的所述选定数目的最低阶位为8位。

3.根据权利要求1所述的密钥卡设备,其中所述密钥卡计数器为128位计数器。

4.根据权利要求1所述的密钥卡设备,所述处理器进一步被配置为在发送所述消息之后将所述密钥卡计数器递增一。

5.根据权利要求1所述的密钥卡设备,其中所述消息进一步包括识别可由接收所述消息的控制单元执行的命令的数据字段。

6.根据权利要求1所述的密钥卡设备,其中所述处理器被配置为使所述发送器发送撤销信号用于启动撤销程序。

7.根据权利要求1所述的密钥卡设备,其中所述密钥卡计数器值由基于AES-128加密的Opkey进行加密。

8.一种控制单元设备,其包括:

接收器,其被配置为接收信号;

存储器,其被配置为储存控制单元计数器和操作密钥即OpKey;以及

耦合到所述接收器和存储器的处理器,所述处理器被配置为:

接收消息,所述消息包括密钥卡计数器的OpKey加密值的预定数目的位以及未使用所述OpKey加密的所述密钥卡计数器的选定数目的最低阶位,所述密钥卡计数器与所述控制单元分开;

基于接收位以及所述控制单元计数器的对应位更新所述控制单元计数器;

在更新所述控制单元计数器之后,生成所述控制单元计数器的OpKey加密值;

验证所述密钥卡计数器的OpKey加密值的所述预定数目的位是否匹配来自所述控制单元计数器的所述OpKey加密值的预定数目的位。

9.根据权利要求8所述的控制单元设备,其中所述密钥卡计数器的OpKey加密值和所述控制单元计数器的OpKey加密值由基于AES-128加密的Opkey进行加密。

10.根据权利要求8所述的控制单元设备,其中所述控制单元计数器的所述选定数目的最低阶位为8位。

11.根据权利要求8所述的控制单元设备,所述处理器进一步被配置为如果所述密钥卡计数器的OpKey加密值的所述预定数目的位匹配来自所述控制单元计数器的所述OpKey加密值的所述预定数目的位,则启动控制操作。

12.根据权利要求8所述的控制单元设备,其中所述控制单元计数器为128位计数器。

13.根据权利要求8所述的控制单元设备,所述处理器进一步被配置为在未能验证所述密钥卡计数器的OpKey加密值的所述预定数目的位匹配来自所述控制单元计数器的OpKey

加密值的所述预定数目的位之后，将所述控制单元计数器恢复到所述更新之前的值。

14.根据权利要求8所述的控制单元设备，其中所述消息进一步包括识别将由所述控制单元执行的命令的数据字段。

15.根据权利要求8所述的控制单元设备，所述处理器进一步被配置为：

当检测到启动所述OpKey撤销程序的命令时，开始记录与从一个或多个密钥卡接收到的消息相关的OpKey；以及

当检测到终止OpKey撤销程序的命令时，结束记录与从所述一个或多个密钥卡接收到的消息相关的OpKey。

16.根据权利要求15所述的控制单元设备，所述处理器进一步被配置为删除在当检测到启动所述OpKey撤销程序的所述命令与检测到终止所述OpKey撤销程序的所述命令之间的时段内未记录的任何储存的OpKey。

17.根据权利要求15所述的控制单元设备，所述处理器进一步被配置为删除在当检测到启动所述OpKey撤销程序的所述命令与检测到终止所述OpKey撤销程序的所述命令之间的时段内未记录的任何储存的OpKey，或删除刚好在检测到启动所述OpKey撤销程序的所述命令之前未记录的任何储存的OpKey。

18.一种用于选择将被保留在控制单元处的密钥卡操作密钥即OpKey的方法，其包括：

由所述控制单元接收命令以启动OpKey撤销程序；

开始记录与在所述撤销程序期间从一个或多个密钥卡接收到的一个或多个消息相关的OpKey，其中接收的所述一个或多个消息中的每个对应于所述一个或多个密钥卡的相应一个并且包括：

由相应密钥卡的OpKey加密的相应密钥卡的密钥卡计数器值的预定数目的位；以及

未由相应密钥卡的OpKey加密的相应密钥卡的密钥卡计数器的预定数目的最低阶位；

由所述控制单元接收命令以终止所述OpKey撤销程序；以及

结束记录与从密钥卡接收到的消息相关的OpKey。

19.根据权利要求18所述的方法，其进一步包括：删除在当接收到启动所述OpKey撤销程序的所述命令时与当接收到终止所述OpKey撤销程序的所述命令之间的时段内未记录的任何储存的OpKey。

20.根据权利要求18所述的方法，其进一步包括：删除在当接收到启动所述OpKey撤销程序的所述命令时与接收到终止所述OpKey撤销程序的所述命令之间的时段内未记录的任何储存的OpKey，或删除刚好在检测到启动所述OpKey撤销程序的所述命令之前未记录的任何储存的OpKey。

单向密钥卡和交通工具配对的验证、保留及撤销

技术领域

[0001] 本发明总体涉及安全性，并且更具体地涉及用于密钥卡(key fob)交通工具操作的密钥验证、保留及撤销的方法。

背景技术

[0002] 密钥卡可以与控制单元诸如交通工具控制单元配对，以执行众所周知的动作，诸如打开/关闭和锁定/解锁交通工具门。密钥卡可以仅能够发送，由于不能双向通信，所以其限制了通过从控制单元发送的询问消息来验证由密钥卡所发送的命令可用的认证过程。控制单元必须能够验证所接收命令的有效性并且拒绝未授权命令，包括回放来自有效密钥卡的较早发送。

[0003] 偶尔，密钥卡将丢失，或者其持有人可能不再被授权访问控制单元。在这种情况下，就必须有允许控制单元识别哪些密钥卡仍然有效以及哪些密钥卡应被忽略的过程。

发明内容

[0004] 所描述的实施例提供了用于密钥卡进行控制单元验证、保留及撤销的方法。在初始配对之后，密钥卡和交通工具单元共享秘密的操作密钥(OpKey)。对于验证，密钥卡将标识符发送到控制单元，该标识符可以为128位计数器的8个最低阶位以及计数器的AES-128OpKey加密值的一些位(bit)。

[0005] 在一个或多个密钥卡与诸如交通工具控制单元的控制单元配对之后，密钥卡各自具有与控制单元秘密共享的它们自己的OpKey。密钥卡需要验证共享的OpKey对控制单元的占有，以便控制单元采取指定的动作，诸如锁定/解锁或打开/关闭交通工具门。即使密钥卡能够发送但不能接收，该发明仍然解决了这个问题。此外，在此描述的实施例防止第三方通过回放更早发送的消息来模仿合法的密钥卡。另外，在密钥卡丢失之后，其OpKey可以被撤销，而剩余的或新的密钥卡的OpKey则可以被保留。

[0006] 对于OpKey撤销和保留，合法的控制单元用户提示剩余的或新的密钥卡将验证消息发送到控制单元。然后，控制单元经提示进入OpKey保留和撤销模式。随后，用户提示剩余的或新的密钥卡中的每一个将验证消息发送到控制单元。控制单元最终经提示退出OpKey保留和撤销模式，仅保留其分别在刚好进入OpKey保留与撤销模式之前和在OpKey保留与撤销模式期间从中接收有效验证消息的密钥卡的OpKey。

附图说明

[0007] 已经这样概括地描述了该发明，现在将参考附图，其中：

[0008] 图1示出密钥卡和控制单元的正常操作。

[0009] 图2示出在一个实施例中可以用于使密钥卡无效的密钥卡保留和撤销过程。

[0010] 图3为示出根据一个实施例使用OpKey验证的密钥卡和控制单元的正常操作的流程图。

[0011] 图4为示出OpKey的保留和撤销过程的流程图。

[0012] 图5为根据一个实施例的示例密钥卡的方框图。

[0013] 图6为根据一个实施例的示例控制单元的方框图。

具体实施方式

[0014] 现在将参照附图在下文中更完整地描述本发明。然而，本发明可以以许多不同的形式呈现，并且不应被解释为局限于在此阐述的实施例。确切地说，提供这些实施例以使得本公开将是全面且完整的，并且将本发明的范围完整地传达给本领域技术人员。本领域技术人员可以能够使用该发明的各种实施例。

[0015] 这些实施例使密钥卡(key fob)能够发送但不能接收，以验证秘密OpKey对交通工具控制单元的占有，同时防止第三方通过回放由密钥卡较早发送给控制单元用于验证的消息来模仿合法密钥卡。另外，本发明也允许合法的交通工具用户撤销已丢失或过期的密钥卡的OpKey，但保留每个依然有效的密钥卡的OpKey。

[0016] 图1示出密钥卡101和控制单元102的正常操作。在初始配对之后，密钥卡101和控制单元102共享秘密的OpKey。例如，密钥卡101和控制单元102可以使用在于2013年8月16日提交的题为“One-Way Key Fob and Vehicle Pairing”的在审的美国专利申请第13/969,154号中所公开的系统和方法来配对，该申请的公开内容在此通过引用以其整体并入本申请。

[0017] 除了在密钥卡101与控制单元102两者之间共享的OpKey之外，这两个设备均具有128位计数器103,104。在其他实施例中，可以使用不同大小的计数器。在正常操作中，密钥卡101创建计数器103的AES-128OpKey加密值。然后，密钥卡101将128位计数器103的8个最低阶位和计数器103的AES-128OpKey加密值的一些预定位发送(105)给控制单元102。从初始计数器值(例如1)开始，在每次发送之后，密钥卡就将其计数器值递增1。消息105本身的发送可以表示来自密钥卡101的命令，诸如解锁/锁定交通工具门。可选地，在消息105中可以包括单独的命令数据字段以识别来自密钥卡101的期望命令。

[0018] 当接收到消息105时，控制单元102使用从密钥卡101接收的8个计数器位来设定128位计数器104的8个最低阶位，并且如果所接收的8位的值不大于计数器104的8个最低阶位的值，就将计数器104的剩余位的值递增1。另外，控制单元102创建计数器104的AES-128OpKey加密值。然后，控制单元102将来自计数器104的其OpKey加密值的预定位与表示计数器103的OpKey加密值的位进行比较。控制单元102验证消息105，并且因此如果这些位匹配则验证OpKey。

[0019] 如果验证失败，则控制单元102将计数器104恢复到变化之前的值。

[0020] 如果非法的或假的密钥卡106试图在不配对的情况下将消息107发送至控制单元，则控制单元102将拒绝该消息107。假密钥卡106不具有用于控制单元102的有效OpKey。另外，假密钥卡106不知道用于有效消息的控制单元102的正确计时器值。

[0021] 图2示出在一个实施例中可用于使密钥卡无效的密钥卡保留和撤销过程。在该示例中，三个密钥卡201-203与相同的控制单元204配对。每个配对的密钥卡201-203具有与控制单元204共享的唯一的、秘密的OpKey(OpKey1,OpKey2,OpKey3)。另外，每个密钥卡201-203具有它自己的计数器205-207。对于每个密钥卡201-203，控制单元204保持单独的计数

器208-210。

[0022] 当密钥卡203丢失或需要撤销时，用户可以执行以下步骤。首先，用户提示控制单元204进入OpKey撤销模式。OpKey撤销模式可以通过来自剩余密钥卡201、202的消息或/和通过到控制单元204的一些其它输入来触发。

[0023] 当控制单元204处于OpKey撤销模式时，用户提示每个剩余密钥卡201、202用控制单元204执行正常操作。例如，每个密钥卡201、202将来源于其OpKey的消息(诸如消息105(图1))发送至控制单元204。在每个剩余密钥卡201、202已经发送其消息或已经用控制单元204执行操作之后，用户提示控制单元退出OpKey保留模式。因为密钥卡203丢失或不再被授权，所以它在撤销模式期间将不发送消息。

[0024] 控制单元204仅保留在退出撤销模式之前接收到的OpKey。在一个实施例中，控制单元204保留在进入撤销模式之前接收到的最后OpKey和在撤销模式期间接收到的所有OpKey。在其他实施例中，控制单元204仅保留在撤销模式期间接收到的OpKey。所有其他的OpKey(例如，OpKey 3)均被控制单元204删除。这就防止丢失或未授权的密钥卡在撤销程序之后对控制单元204进行操作。

[0025] 图3为示出使用OpKey验证的密钥和控制单元的正常操作过程的流程图。在步骤301中，密钥卡读取128位计数器的8个最低阶位。在步骤302中，密钥卡生成密钥卡计数器的AES-128OpKey加密值。在步骤303中，所述8个最低阶位和来自密钥卡计数器的AES-128OpKey加密值的一些选定位被发送给控制单元。这个信息可以与密钥卡的特定命令或请求相关联。

[0026] 在步骤304中，控制单元基于从密钥卡接收到的8个最低阶位更新控制单元计数器。根据一个实施例，通过将控制单元计数器的8个最低阶位设定为接收到的密钥卡计数器的8个最低阶位，并且如果密钥卡计数器的接收位的值不大于控制单元计数器的对应位的值，则将控制单元计数器的剩余位的值递增1，由此来完成所述更新。在步骤305中，控制单元生成已更新的控制单元计数器的AES-128OpKey加密值。控制单元将控制单元计数器的AES-128OpKey加密值的选定位与从密钥卡接收到的密钥卡计数器的AES-128OpKey加密值的选定位进行比较。

[0027] 如果这些选定位匹配，其表明两个设备均使用相同的OpKey和计数器值，则控制单元验证来自密钥卡的命令或请求。

[0028] 图4是示出OpKey的保留和撤销过程的流程图。在步骤401中，紧随着在剩余的(即未丢失的)或新的密钥卡完成正常操作之后，用户提示控制单元进入OpKey撤销模式。然后，用户提示每个剩余的或核准的密钥卡使用控制单元执行正常操作。正常操作可以包括如图1和图3所示的发送或者允许密钥卡将OpKey加密值发送给控制单元的任何操作。

[0029] 在步骤403中，在所有剩余的或核准的密钥卡已经完成正常操作之后，用户提示控制单元退出OpKey撤销模式。例如，用户可以激活“结束”按钮以退出撤销模式，或者撤销模式可以在设定的一段时间之后结束。

[0030] 在步骤404中，除了与在进入OpKey撤销模式之前操作的最后密钥卡相关的OpKey以及与在撤销模式结束之前使用的密钥卡相关的任何OpKey之外，控制单元删除所有的OpKey。因为丢失的或未核准的密钥卡不可能在短暂的撤销模式持续期间操作，所以丢失的或未核准的设备的OpKey将从控制单元中删除。因此丢失的或未核准的设备不再与控制单

元配对并且不再能够用于向控制单元发送命令。在另一个实施例中，仅保留与在撤销模式期间操作的密钥卡相关的OpKey，并且删除在撤销模式期间不执行操作的所有其他OpKey。

[0031] 图5和图6分别为示例密钥卡500和控制单元600的方框图。密钥卡400和控制单元600各自包括处理器501、601、存储器502、602和收发器603或发送器503。设备的处理器501、601可以用于执行正常操作，诸如保持和更新计数器、生成OpKey加密值以及比较此类值以验证仅来自配对设备的OpKey被使用。处理器可以是标准的CPU、微控制器、低功率数字信号处理器等，并且可以能够在短时间内执行复杂的计算。

[0032] 设备的存储器502、602可以用于储存OpKey、计数器值、加密值和在密钥卡与控制单元之间交换的其他位。存储器可以是非易失性存储设备，诸如闪存或EEPROM。

[0033] 密钥卡发送器503和控制单元收发器603可以是有线的(未示出)、无线的或两者均可。在正常操作期间和在撤销模式期间，设备可以使用收发器和发送器来传达计数器值、OpKey加密数据和其他的位。密钥卡允许远程进入和控制交通工具或其他设备，并且可以使用无线技术如蓝牙、LF或UHF来进行那些发送。密钥卡发送器503能够仅发送，而不从控制单元600接收信号。

[0034] 本领域的技术人员将认识到，可以对所描述的实施例做出修改，并且还将认识到，在所要求保护的发明范围内，许多其他实施例是可能的。

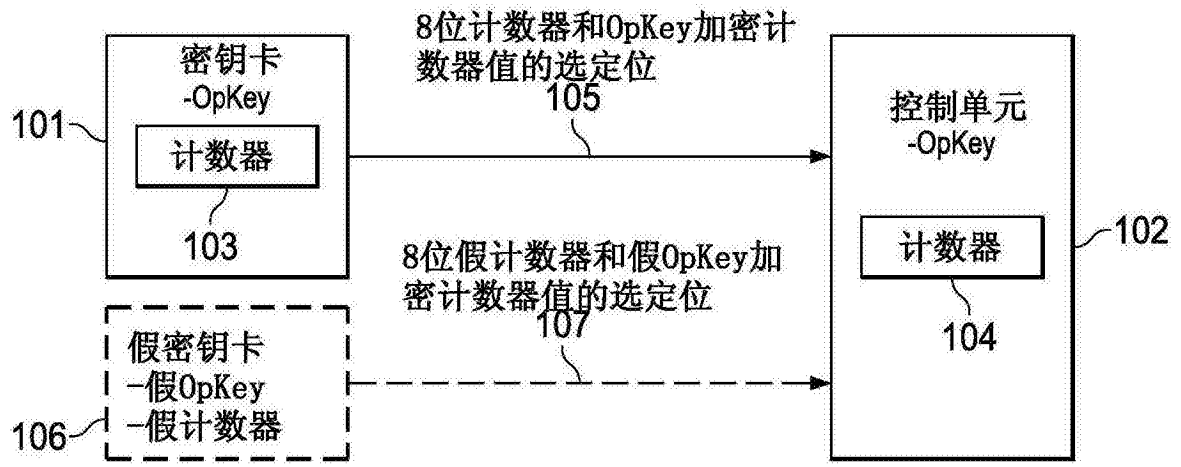

密钥卡
-OpKey
计数器
101
103
8位计数器和OpKey加密计数器值的选定位
105
控制单元
-OpKey
计数器
102
104
8位假计数器和假OpKey加密计数器值的选定位
107
假密钥卡
-假OpKey
-假计数器
106

图1

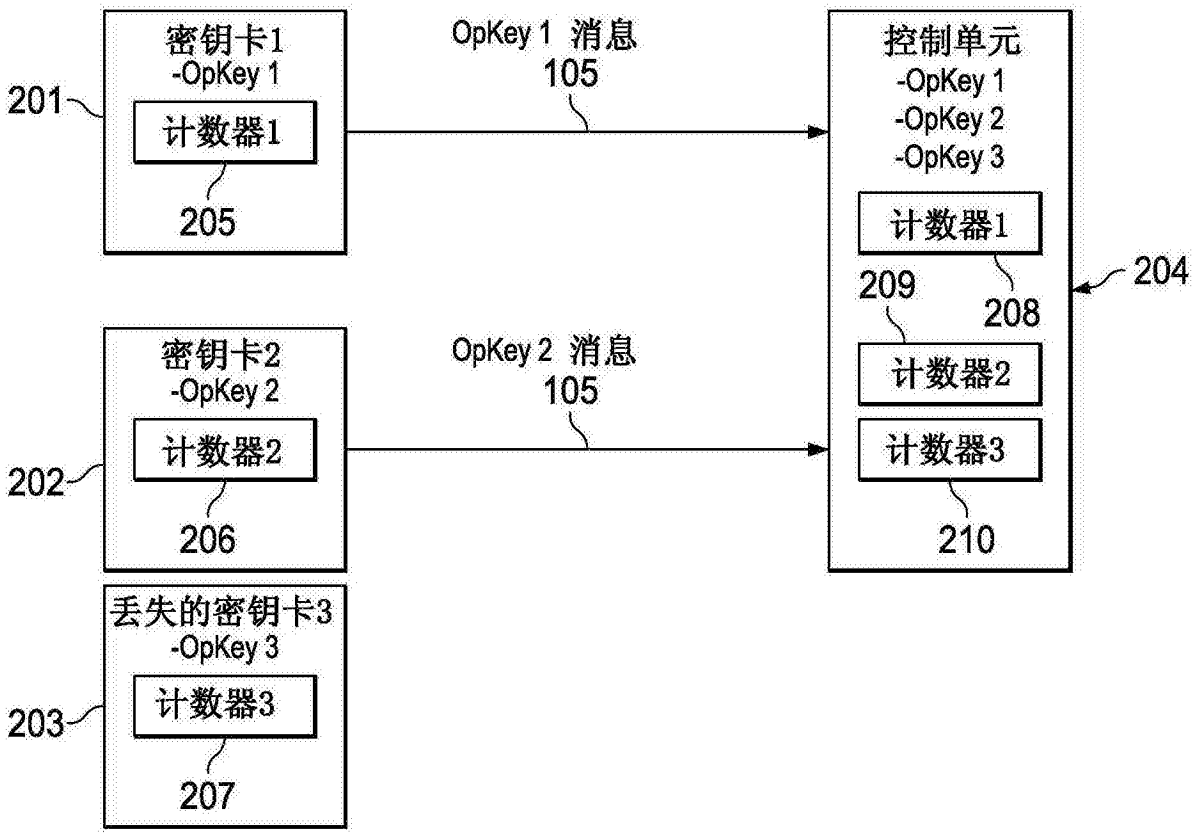

密钥卡1
-OpKey 1
计数器1
201
205
OpKey 1 消息
105
控制单元
-OpKey 1
-OpKey 2
-OpKey 3
计数器1
209
208
204
计数器2
计数器3
210
密钥卡2
-OpKey 2
计数器2
202
206
OpKey 2 消息
105
丢失的密钥卡3
-OpKey 3
计数器3
203
207

图2

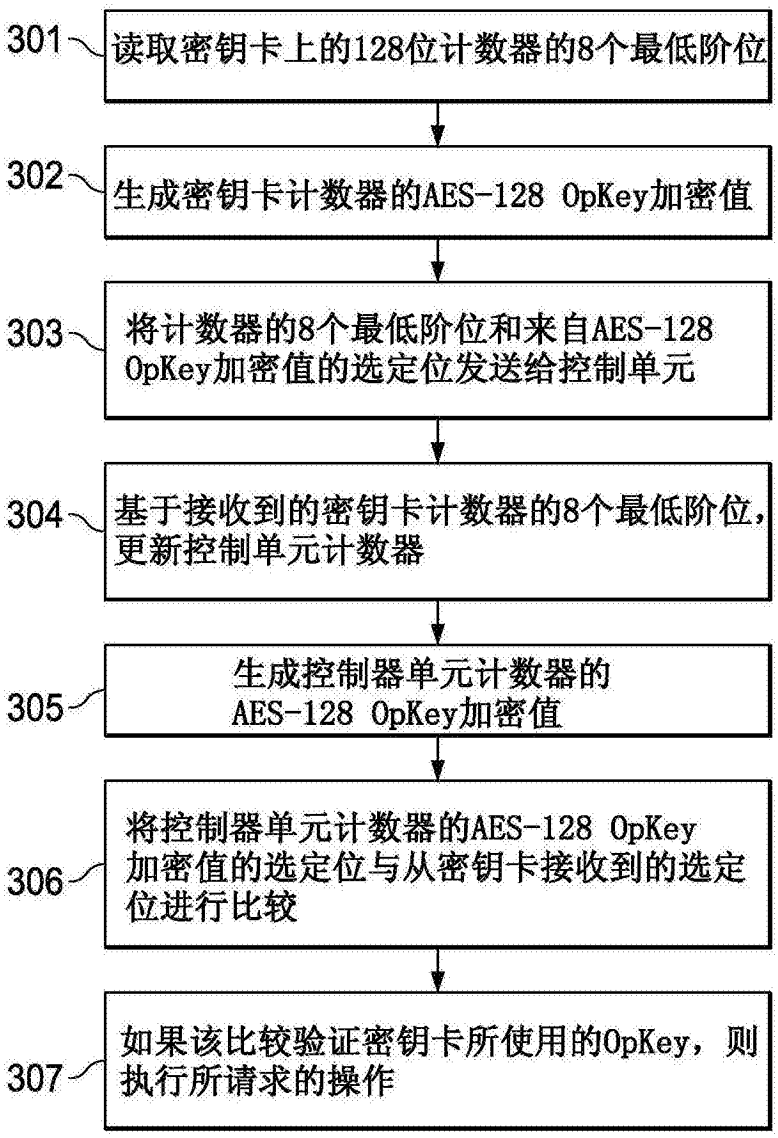

301
读取密钥卡上的128位计数器的8个最低阶位
302
生成密钥卡计数器的AES-128 OpKey加密值
303
将计数器的8个最低阶位和来自AES-128 OpKey加密值的选定位发送给控制单元
304
基于接收到的密钥卡计数器的8个最低阶位，更新控制单元计数器
305
生成控制器单元计数器的AES-128 OpKey加密值
306
将控制器单元计数器的AES-128 OpKey加密值的选定位与从密钥卡接收到的选定位进行比较
307
如果该比较验证密钥卡所使用的OpKey，则执行所请求的操作

图3

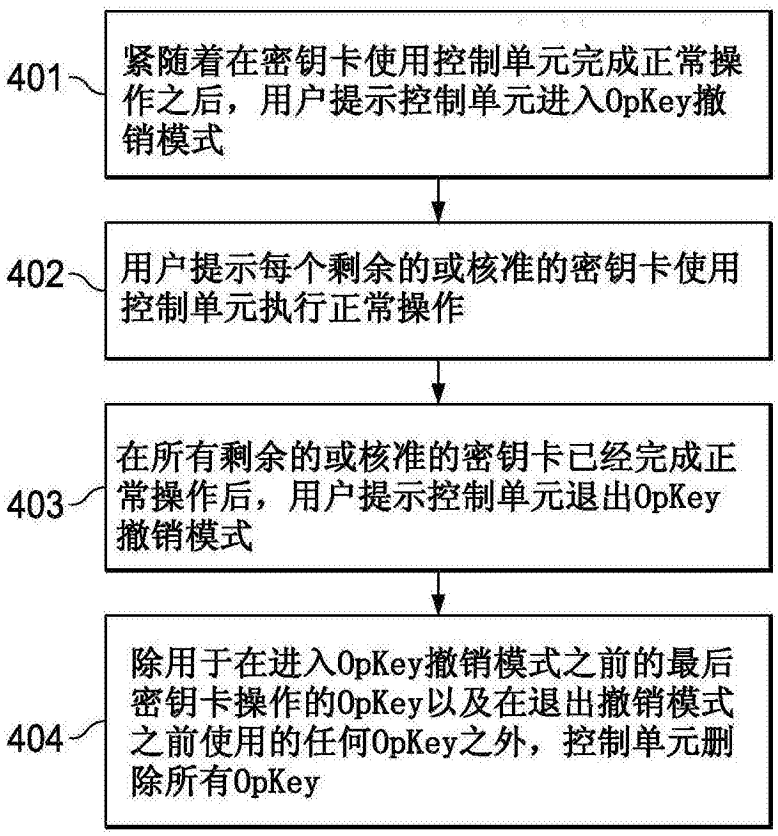

401
紧随着在密钥卡使用控制单元完成正常操作之后，用户提示控制单元进入OpKey撤销模式
402
用户提示每个剩余的或核准的密钥卡使用控制单元执行正常操作
403
在所有剩余的或核准的密钥卡已经完成正常操作后，用户提示控制单元退出OpKey撤销模式
404
除用于在进入OpKey撤销模式之前的最后密钥卡操作的OpKey以及在退出撤销模式之前使用的任何OpKey之外，控制单元删除所有OpKey

图4

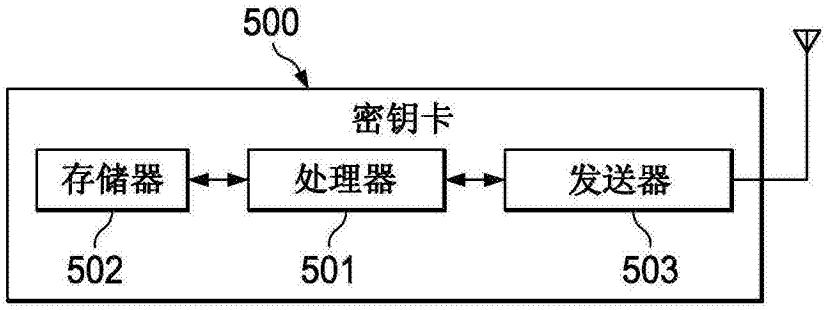

500
密钥卡
存储器
处理器
发送器
502
501
503

图5

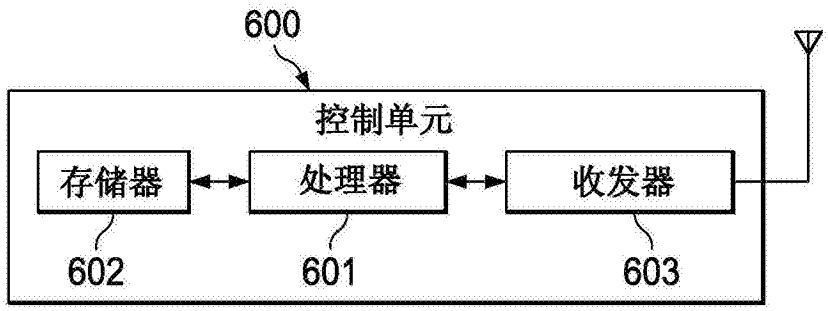


图6