



(12) 发明专利

(10) 授权公告号 CN 103403727 B

(45) 授权公告日 2016.01.06

(21) 申请号 201180068616.7

(22) 申请日 2011.09.12

(30) 优先权数据

2011-030746 2011.02.16 JP

(85) PCT国际申请进入国家阶段日

2013.08.16

(86) PCT国际申请的申请数据

PCT/JP2011/070723 2011.09.12

(87) PCT国际申请的公布数据

W02012/111189 JA 2012.08.23

(73) 专利权人 NEC 平台株式会社

地址 日本神奈川县川崎市

(72) 发明人 小宫山毅

(74) 专利代理机构 中国专利代理(香港)有限公司

72001

代理人 俞华梁 王忠忠

(51) Int. Cl.

G06F 21/10(2013.01)

权利要求书3页 说明书11页 附图4页

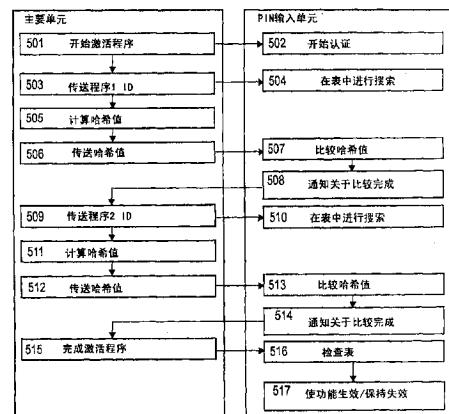
(54) 发明名称

附加功能单元的启用 / 禁用方法、其系统以及附加功能单元

(57) 摘要

本发明的目的是在信息处理装置中安装了未经授权程序时禁用附加功能单元的功能性，由此防止未经授权程序以未经授权方式从附加功能单元来获取信息。本发明是对其添加了附加功能单元的信息处理装置中的附加功能单元的启用 / 禁用方法，具有下列步骤：基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一定向函数值，以便在制造时将第一定向函数值存储到附加功能单元中；在启动了信息处理装置之后基于记录介质中包含的数据来计算第二定向函数值；以及在第一定向函数值和第二定向函数值不同时，禁用附加功能单元的功能性。

CN 103403727 B



1. 一种使对其添加附加功能单元的信息处理设备中的所述附加功能单元生效 / 失效的方法, 所述方法包括下列步骤 :

基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值, 并且在制造时将所述第一单向函数值存储在所述附加功能单元中;

在激活所述信息处理设备之后基于所述记录介质中包含的所述数据来计算第二单向函数值; 以及

当所述第一单向函数值和所述第二单向函数值不同时, 使所述附加功能单元的功能失效,

其中所述记录介质设置在所述信息处理设备中, 所述附加功能单元是添加到所述信息处理设备的单元, 所述信息处理设备是安装支付功能的掌上型终端, 以及所述附加功能单元是 PIN(个人标识号) 输入单元。

2. 如权利要求 1 所述的使所述附加功能单元生效 / 失效的方法, 其中 :

由所述信息处理设备来计算所述第二单向函数值;

将所述第二单向函数值从所述信息处理设备传送给所述附加功能单元; 以及

由所述附加功能单元来比较所述第一单向函数值和所述第二单向函数值。

3. 如权利要求 1 所述的使所述附加功能单元生效 / 失效的方法, 还包括下列步骤 :

基于多个应用程序的每个的数据来计算第三单向函数值, 并且在制造时将所述第三单向函数值存储在所述附加功能单元中;

在激活所述信息处理设备之后基于所述多个应用程序的每个的所述数据来计算第四单向函数值; 以及

当所述多个应用程序的至少一个的所述第三单向函数值和所述第四单向函数值不同时, 使所述附加功能单元的功能失效。

4. 如权利要求 3 所述的使所述附加功能单元生效 / 失效的方法, 其中 :

由所述信息处理设备来计算所述第四单向函数值;

将所述第四单向函数值从所述信息处理设备传送给所述附加功能单元; 以及

由所述附加功能单元来比较所述第三单向函数值和所述第四单向函数值。

5. 如权利要求 1 所述的使所述附加功能单元生效 / 失效的方法, 还包括下列步骤 :

基于多个应用程序的数据来计算第五单向函数值, 并且在制造时将所述第五单向函数值存储在所述附加功能单元中;

在激活所述信息处理设备之后基于所述多个应用程序的数据来计算第六单向函数值; 以及

当所述第五单向函数值和所述第六单向函数值不同时, 使所述附加功能单元的功能失效。

6. 如权利要求 5 所述的使所述附加功能单元生效 / 失效的方法, 其中 :

由所述信息处理设备来计算所述第六单向函数值;

将所述第六单向函数值从所述信息处理设备传送给所述附加功能单元; 以及

由所述附加功能单元来比较所述第五单向函数值和所述第六单向函数值。

7. 一种使对其添加附加功能单元的信息处理设备中的所述附加功能单元生效 / 失效的系统, 所述系统包括 :

基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值并且在制造时将所述第一单向函数值存储在所述附加功能单元中的部件；

在激活所述信息处理设备之后基于所述记录介质中包含的所述数据来计算第二单向函数值的部件；以及

当所述第一单向函数值和所述第二单向函数值不同时使所述附加功能单元的功能失效的部件，

其中所述记录介质设置在所述信息处理设备中，所述附加功能单元是添加到所述信息处理设备的单元，所述信息处理设备是安装支付功能的掌上型终端，以及所述附加功能单元是 PIN(个人标识号) 输入单元。

8. 如权利要求 7 所述的使所述附加功能单元生效 / 失效的系统，其中：

由所述信息处理设备来计算所述第二单向函数值；

将所述第二单向函数值从所述信息处理设备传送给所述附加功能单元；以及

由所述附加功能单元来比较所述第一单向函数值和所述第二单向函数值。

9. 如权利要求 7 所述的使所述附加功能单元生效 / 失效的系统，还包括：

基于多个应用程序的每个的数据来计算第三单向函数值并且在制造时将所述第三单向函数值存储在所述附加功能单元中的部件；

在激活所述信息处理设备之后基于所述多个应用程序的每个的所述数据来计算第四单向函数值的部件；以及

当所述多个应用程序的至少一个的所述第三单向函数值和所述第四单向函数值不同时使所述附加功能单元的功能失效的部件。

10. 如权利要求 9 所述的使所述附加功能单元生效 / 失效的系统，其中：

由所述信息处理设备来计算所述第四单向函数值；

将所述第四单向函数值从所述信息处理设备传送给所述附加功能单元；以及

由所述附加功能单元来比较所述第三单向函数值和所述第四单向函数值。

11. 如权利要求 7 所述的使所述附加功能单元生效 / 失效的系统，还包括：

基于多个应用程序的数据来计算第五单向函数值并且在制造时将所述第五单向函数值存储在所述附加功能单元中的部件；

在激活所述信息处理设备之后基于所述多个应用程序的数据来计算第六单向函数值的部件；以及

当所述第五单向函数值和所述第六单向函数值不同时使所述附加功能单元的功能失效的部件。

12. 如权利要求 11 所述的使所述附加功能单元生效 / 失效的系统，其中：

由所述信息处理设备来计算所述第六单向函数值；

将所述第六单向函数值从所述信息处理设备传送给所述附加功能单元；以及

由所述附加功能单元来比较所述第五单向函数值和所述第六单向函数值。

13. 一种添加到信息处理设备的附加功能单元，所述附加功能单元包括：

在制造时存储基于存储引导加载程序和操作系统的记录介质中包含的数据所计算的第一单向函数值的部件；以及

当激活所述信息处理设备之后基于所述记录介质中包含的数据所计算的第二单向函

数值和所述第一单向函数值不同时使所述附加功能单元的功能失效的部件，

其中所述记录介质设置在所述信息处理设备中，所述附加功能单元是添加到所述信息处理设备的单元，所述信息处理设备是安装支付功能的掌上型终端，以及所述附加功能单元是PIN(个人标识号)输入单元。

附加功能单元的启用 / 禁用方法、其系统以及附加功能单元

技术领域

[0001] 本发明涉及使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的方法、其系统及其程序，以及更具体来说，涉及使作为对其添加作为附加功能单元的 PIN 输入单元的信息处理设备的掌上型终端中的 PIN(个人标识号) 输入单元生效 / 失效的方法、其系统及其程序。

背景技术

[0002] 对与支付卡的安全性相关的国际统一标准标准化，针对用于输入信用卡的 PIN 的终端设备。虽然有可能通过提供 PIN 输入专用键盘和显示设备来防止 PIN 码被盗，但是使用 PIN 输入专用机器使得需要携带 PIN 输入专用机器和掌上型终端的两个设备，并且破坏便携性。此外，在一个设备中安装键盘和显示设备两者增加制造成本并且限制使用。

[0003] JP-A-2009-117887(专利文献 1) 公开一种在客户端侧记录证书并且在客户端与服务器之间执行认证处理的网络系统。

[0004] JP-A-62-275784(专利文献 2) 公开一种在存储电子货币的存储器中添加接收电子货币合法性校验功能和存储电子货币防伪功能的技术。

[0005] JP-A-2008-282112(专利文献 3) 公开一种认证负责支付操作的人员的发明。

[0006] JP-A-2002-258963(专利文献 4) 公开一种发明，其特征在于未经授权副本出现时显示告警消息的方法。

[0007] JP-A-2002-109439(专利文献 5) 公开一种使用密码或生物计量信息来防止未经授权支付处理的发明。

[0008] JP-A-2008-139910(专利文献 6) 公开一种通过移动电话来认证执行支付操作的用户的系统。

[0009] JP-A-2008-009681(专利文献 7) 公开一种认证负责操作能够执行支付的移动终端的人员的系统。

[0010] JP-A-2008-077256(专利文献 8) 公开一种认证用户以防止电子货币功能的未经授权使用的系统。

[0011] JP-A-2006-247192(专利文献 9) 公开一种使用服务器来认证用户的支付系统。

[0012] JP-A-2002-352165(专利文献 10) 公开一种基于用户的位置信息来执行认证的发明。

[0013] JP-A-2004-199269(专利文献 11) 公开一种基于预先登记的电话号码和个人信息来认证用户的发明。

[0014] {引文列表}

[0015] {专利文献}

[0016] {PTL 1} JP-A-2009-117887

[0017] {PTL 2} JP-A-62-275784

- [0018] {PTL 3} JP-A-2008-282112
- [0019] {PTL 4} JP-A-2002-258963
- [0020] {PTL 5} JP-A-2002-109439
- [0021] {PTL 6} JP-A-2008-139910
- [0022] {PTL 7} JP-A-2008-009681
- [0023] {PTL 8} JP-A-2008-077256
- [0024] {PTL 9} JP-A-2006-247192
- [0025] {PTL 10} JP-A-2002-352165
- [0026] {PTL 11} JP-A-2004-199269

发明内容

- [0027] {技术问题}
 - [0028] 为了输入信用卡的PIN, 使用与用于应用程序的键盘不同的PIN输入专用键盘。至于显示器, 用于输入PIN的显示设备与应用程序分离, 以便防止PIN码被盗。
 - [0029] 如果能够共享用于应用程序的键盘和显示设备以输入PIN, 则有可能使掌上型终端小型化, 并且因此改进便携性, 简化结构设计和制造过程, 降低制造成本, 以及改进用户友好性。
 - [0030] 但是, 当共享键盘和显示设备时, 未经授权程序被安装, 用于输入PIN的伪造输入屏幕被创建, 并且因此PIN码被盗。
 - [0031] 专利文献1中公开的发明在执行认证处理的未经授权程序被安装时是有弱点的。
 - [0032] 按照专利文献2至11的发明没有认证程序代码本身的合法性。
 - [0033] 本发明的一个目的是提供一种使附加功能单元生效 / 失效的方法、其系统及其程序, 它们在信息处理设备中安装未经授权程序时通过使附加功能单元的功能失效来防止未经授权程序从附加功能单元不适当当地得到信息。
 - [0034] {问题的解决方案}
 - [0035] 按照本发明的第一方面, 一种使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的方法包括如下步骤: 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值, 并且在制造时将第一单向函数值存储在附加功能单元中; 在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值; 以及当第一单向函数值和第二单向函数值不同时, 使附加功能单元的功能失效。
 - [0036] 此外, 按照本发明的第二方面, 一种使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的系统具有: 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值并且在制造时将第一单向函数值存储在附加功能单元中的部件; 在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值的部件; 以及当第一单向函数值和第二单向函数值不同时、使附加功能单元的功能失效的部件。
 - [0037] 此外, 按照本发明的第三方面, 使计算机用作使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的系统的程序, 使计算机用作: 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值并且在制造时将第一单向

函数值存储在附加功能单元中的部件；在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值的部件；以及当第一单向函数值和第二单向函数值不同时、使附加功能单元的功能失效的部件。

[0038] 更进一步，按照本发明的第四方面，添加到信息处理设备的附加功能单元具有：在制造时存储基于存储引导加载程序和操作系统的记录介质中包含的数据所计算的第一单向函数值的部件；以及在激活信息处理设备之后基于记录介质中包含的数据所计算的第二单向函数值以及第一单向函数值不同时、使附加功能单元的功能失效的部件。

[0039] 此外，按照本发明的第五方面，使计算机用作添加到信息处理设备的附加功能单元生效 / 失效的设备的程序使计算机用作：在制造时存储基于存储引导加载程序和操作系统的记录介质中包含的数据所计算的第一单向函数值的部件；以及在激活信息处理设备之后基于记录介质中包含的数据所计算的第二单向函数值以及第一单向函数值不同时、使附加功能单元的功能失效的部件。

[0040] {发明的有利效果}

[0041] 按照本发明，当未经授权程序安装在信息处理设备中时，有可能通过使附加功能单元的功能失效来防止未经授权程序从附加功能单元不适当当地得到信息。

附图说明

[0042] {图 1} 附图示出按照本发明的一个实施例、具有内置 PIN 输入单元的掌上型终端的框图。

[0043] {图 2} 附图示出按照本发明的实施例的程序认证信息表的配置图。

[0044] {图 3} 附图是示出按照本发明的实施例、安装模块的准备和设备的登记的视图。

[0045] {图 4} 附图是示出按照本发明的实施例的 ROM 认证过程的视图。

[0046] {图 5} 附图是示出按照本发明的实施例的应用程序认证过程的视图。

具体实施方式

[0047] 下面将参照附图详细描述用于实现本发明的实施例。

[0048] 在本实施例中，在能够通过共同键盘和显示设备来运行信用卡的 PIN 的输入和显示以及应用程序操作处理的输入和显示的安装支付功能的掌上型终端中，PIN 输入单元具有认证主要单元的引导加载程序、OS（操作系统）和应用程序的功能。

[0049] 在能够执行信用卡的 PIN 输入处理的 PIN 输入单元的存储器中，登记由主要单元所运行的引导加载程序、OS 和应用程序的认证信息。

[0050] 基于认证信息，PIN 输入单元执行认证将要由主要单元所运行的引导加载程序、OS 和应用程序是否为经授权程序的处理，以及当检验由主要单元所运行的引导加载程序、OS 和应用程序经过 授权时，使 PIN 输入单元的功能生效。在通过认证处理发现不适当，使 PIN 输入单元的功能失效。

[0051] 通过这种方式，当发现针对盗用 PIN 码的未经授权引导加载程序、OS 和应用程序时，使 PIN 输入单元的功能失效，并且键码通知功能也停止，以使得无法运行按键输入，并且有可能防止 PIN 码被盗。同时，使 PIN 输入单元的功能失效至少包括输入 PIN 码，并且使向主要单元传送 PIN 码的功能失效。此外，使 PIN 输入单元的功能失效可包括从接触式 IC

卡或者非接触式 IC 卡来读取数据，并且使向主要单元传送这个数据的功能失效。

[0052] 安装支付功能的掌上型终端的配置将参照图 1 来描述。

[0053] 参照图 1，按照本发明的实施例的安装支付功能的掌上型终端具有主要单元和 PIN 输入 / 通用数字小键盘。主要单元具有存储装置 101、ROM(只读存储器)102、RAM(随机存取存储器)103、中央控制单元(主 CPU(中央处理单元))104 和显示单元 105。PIN 输入 / 通用数字小键盘包括副 CPU 106、程序存储存储器 107、数据存储存储器 108、键盘 109 和 IC 卡单元 110。

[0054] 存储装置 101 是存储应用程序的存储器。ROM 102 是存储引导加载程序和 OS 的存储器。RAM 103 是存储第一种类的执行程序的存储器。同时，第一种类的执行程序表示引导加载程序、OS 和应用程序之中将要由中央控制单元 104 所运行的程序。中央控制单元(主 CPU)104 运行第一种类的执行程序。显示单元 105 显示屏幕。副 CPU 106 控制 PIN 输入 / 通用数字小键盘单元。程序存储存储器 107 是存储将要由副 CPU 106 所运行的第二种类的执行程序的存储器。同时，第二种类的执行程序是键盘控制程序、IC 卡控制程序和 PIN 输入控制程序。数据存储存储器 108 存储程序认证信息表和加密密钥(例如公共密钥系统的公共密钥)。键盘 109 输入 PIN。IC 卡单元 110 从插入的接触式 IC 卡(例如信用卡)或者经过的非接触式 IC 卡来读取信息。

[0055] 随后，将主要参照图 2、图 3、图 4 和图 5 来描述认证主要单元中实现的引导加载程序、OS 和应用程序的方法。

[0056] 程序认证信息表的配置将参照图 2 来描述。程序认证信息表存储在数据存储存储器 108 中。

[0057] 程序认证信息表包括一个或多个记录 203，并且各记录与一个程序关联。同时，程序表示引导加载程序、OS 和应用程序。各记录包括程序 ID 的字段 201 和程序的哈希值。程序 ID 例如是程序的名称。程序的哈希值是通过将预定哈希函数应用于程序文件的整个图像数据所得到的值。

[0058] 将要安装在设备上的 ROM 的准备和设备的登记将参照图 3 来描述。

[0059] 在程序开发环境中，开发将要在设备上运行的引导加载程序和 OS(301)。

[0060] 创建存储作为执行程序的引导加载程序和 OS 的 ROM，并且计算基于 ROM 的整个图像数据的哈希值(302)。同时，ROM 具有 EPROM(可擦可编程只读存储器)、EEPROM(电可擦可编程只读存储器)、闪速存储器、MRAM(磁随机存取存储器)以及其电力由电池来保持的 RAM(随机存取存储器)。ROM 可以是任何记录介质，只要 ROM 保持作为存储执行程序的引导加载程序和 OS，并且允许程序被读取。另外，不是计算基于 ROM 的整个图像数据的哈希值，而是可计算基于引导加载程序的整个图像数据和 OS 的整个图像数据的哈希值。

[0061] 作为程序 ID 的“ROM”的字符串的代码连同基于 ROM 的整个图像数据的哈希值一起登记在 OS/ 引导加载程序认证信息表中。

[0062] 为了防止 OS/ 引导加载程序认证信息表在 PIN 输入单元 中登记 OS/ 引导加载程序认证信息表的过程期间被伪造，OS/ 引导加载程序认证信息表使用 OS/ 引导加载程序公共密钥 305 来加密(304)。

[0063] PIN 输入单元中登记的 OS/ 引导加载程序公共密钥 308 是 OS/ 引导加载程序开发环境中的 OS/ 引导加载程序公共密钥，并且与在对 OS/ 引导加载程序认证信息表的加密时

使用的 OS/ 引导加载程序公共密钥是相同的。由 PIN 输入单元从 OS/ 引导加载程序开发环境所输入的加密 OS/ 引导加载程序认证信息表使用 PIN 输入单元中存储的 OS/ 引导加载程序公共密钥 308 来解码（解密），并且解码 OS/ 引导加载程序认证信息表登记在 PIN 输入单元中（309）。

[0064] 在主要单元与 PIN 输入单元之间认证 ROM 的过程将参照图 4 来描述。

[0065] 激活掌上型终端的主要单元（401），并且激活 PIN 输入单元。紧接激活 PIN 输入单元之后，PIN 输入单元的功能是无效的。当激活 PIN 输入单元时，激活 PIN 输入单元的 ROM 认证功能。

[0066] 另一方面，当激活主要单元时，首先激活引导加载程序（403）。引导加载程序计算 ROM 的哈希值（404），并且将所计算的哈希值传送给 PIN 输入单元（405）。另外，在上述步骤 302 时，可计算基于引导加载程序的整个图像数据和 OS 的整个图像数据的哈希值，而不是计算基于 ROM 的整个图像数据的哈希值。

[0067] PIN 输入单元将从主要单元所接收的哈希值和 PIN 输入单元中保存的认证信息表中登记的哈希值进行比较（406）。

[0068] 当两个哈希值不同时，判定在主要单元中实现并且在 ROM 中存储的引导加载程序、OS 或者两者是未经授权的，PIN 输入单元的功能的失效状态被保持，以及处理完成。另外，对于本发明，保持失效状态又称作“失效”。在以保持 PIN 输入单元的功能的失效状态来完成处理之前，PIN 输入单元可向主要单元通知关于 ROM 中存储的引导加载程序、OS 或者两者是未经授权的，并且主要单元可显示这个通知。

[0069] 虽然当两个哈希值作为比较的结果为相同时，判定在主要单元中实现并且在 ROM 中存储的引导加载程序和 OS 均是经授权的，但使 PIN 输入单元的功能有效被延迟直到因以下所述的应用程序的认证而判定应用程序也经过授权。

[0070] 接下来将参照图 3 和图 5 来描述一种在 ROM 认证之后执行的、认证在主要单元的存储装置 101 中实现的应用程序的方法。当判定 ROM 中存储的引导加载程序、OS 或者两者为未经授权时，不执行应用程序的认证。

[0071] 将参照图 3 来描述主要单元的存储装置中存储的应用程序的准备和设备的登记。

[0072] 在应用程序开发环境中，创建将要在主要单元上运行的应用程序的执行文件（310）。通过对哈希函数应用执行文件的图像数据的所有项，计算执行程序的哈希值。作为程序 ID 的执行程序的文件名连同哈希值一起在应用程序认证信息表中登记（312）。当存在多个应用程序时，计算各应用程序的执行文件的哈希值，并且在应用程序认证信息表中登记各应用程序的程序 ID 及其哈希值。

[0073] 为了防止应用程序认证信息表在 PIN 输入单元中登记应用程序认证信息表的过程期间被伪造，应用程序认证信息表使用应用程序公共密钥来加密（313）。

[0074] PIN 输入单元中登记的应用程序公共密钥 317 与应用程序开发环境中包含的应用程序公共密钥 314 是相同的。应用程序公共密钥由掌上型终端制造商来创建，并且提供给应用程序的开发人员。掌上型终端制造商在制造掌上型终端时在 PIN 输入单元中登记应用程序公共密钥 317。

[0075] 应用程序的执行文件存储在主要单元的存储装置 316 中。由 PIN 输入单元从应用程序开发环境所输入的加密应用程序认证 信息表使用 PIN 输入单元中登记的应用程序公

共密钥 317 来解码，并且在 PIN 输入单元的存储器中作为应用程序认证信息表 318 来登记。

[0076] 将参照图 5 来描述 PIN 输入单元认证主要单元中的应用程序的过程。

[0077] 在从主要单元向 PIN 输入单元通知应用程序的激活的开始时 (501)，PIN 输入单元开始认证处理 (502)。从主要单元向 PIN 输入单元通知作为 ID 的、将要在主要单元上运行的第一应用程序的执行文件名 (503)。PIN 输入单元从 PIN 输入单元中登记的应用程序认证信息表来获取第一程序哈希值 (504)。另一方面，主要单元计算第一程序哈希值 (505)，并且将这个哈希值传送给 PIN 输入单元。PIN 输入单元将从主要单元所接收的哈希值和应用程序认证信息表中登记的哈希值进行比较 (507)。

[0078] 当两个哈希值不同时，判定主要单元中实现的第一应用程序的执行文件是未经授权的，并且暂时存储判定结果。

[0079] 当两个哈希值相同时，判定主要单元中实现的第一应用程序的执行文件是经过授权的，并且暂时存储判定结果。

[0080] 当两个或更多应用程序在主要单元中实现时，对第一应用程序所执行的上述方法对其余应用程序重复进行。

[0081] 此外，对于其余应用程序的各应用程序来判定 PIN 输入单元的应用程序认证信息表中存储的哈希值和主要单元所计算并且传送给 PIN 输入单元的哈希值是否匹配，并且暂时存储判定结果。

[0082] 当关于第一应用程序和所有其余应用程序的判定完成时，研究这些判定结果。当至少一个应用程序的判定结果指示这个应用程序的执行文件未经授权，则 PIN 输入单元的功能保持为失效。另一方面，当所有应用程序的判定结果指示这些应用程序的执行文件经过授权，则使 PIN 输入单元的功能生效。

[0083] 下面将描述在主要单元中实现两个应用程序时的后续 操作。

[0084] PIN 输入单元向主要单元通知关于第一应用程序的比较完成 (508)。

[0085] 从主要单元向 PIN 输入单元通知作为 ID 的、将要在主要单元上运行的第二应用程序的执行文件名 (509)。PIN 输入单元从 PIN 输入单元中登记的应用程序认证信息表来获取第二程序的哈希值 (510)。另一方面，主要单元计算第二程序的哈希值 (511)，并且将这个哈希值传送给 PIN 输入单元 (512)。PIN 输入单元将从主要单元所接收的哈希值和应用程序认证信息表中登记的哈希值进行比较 (513)。

[0086] PIN 输入单元在主要单元中暂时存储关于第二应用程序的执行文件的判定结果，并且通知主要单元关于第二应用程序的比较完成 (514)。

[0087] 在将要运行的所有应用程序的激活已经完成时，主要单元通知 PIN 输入单元关于应用程序的激活完成 (515)。

[0088] 当通知关于激活完成时，PIN 输入单元检查哈希值比较结果 (516)。当认证信息表中登记的所有程序在哈希值的比较时具有相同值 (517)，则使 PIN 输入单元的功能生效。

[0089] 在哈希值的比较时检测到不同的值，其哈希值被比较的应用程序的数量小于所登记应用程序的数量或者检测到没有登记的程序时，判定差错发生，并且使 PIN 输入单元的功能失效。另外，在从 PIN 输入单元中登记的应用程序认证信息表来获取程序的哈希值时，如果关键程序 ID 没有在应用程序认证信息表中登记，则有可能检测到没有登记的程序。

[0090] 按照本实施例的效果包括通过改写 ROM 来防止未经授权程序被运行，并且通过当

PIN 输入单元安装在主要单元中时认证其中存储引导加载程序和 OS 的 ROM 以及通过当 ROM 未经授权时使 PIN 输入的功能失效来防止信用卡的 PIN 码被盗。此外,效果包括通过改写应用程序的执行文件来防止未经授权执行文件被运行,并且通过当 PIN 输入单元安装在主要单元中时认证应用程序的执行文件以及通过当应用程序的执行文件未经授权时使 PIN 输入单元的功能失效来防止信用卡的 PIN 码被盗。

[0091] 因此,应用程序和 PIN 输入程序能够共享键盘和显示设备,以使得有可能共享平台并且有效地推广产品。此外,有可能使设备小型化,简化设备的结构设计,简化制造设备的过程,并且降低制造成本。

[0092] 虽然在上述实施例中针对每一应用程序来计算哈希值,但是可对于主要单元中的所有应用程序来计算哈希值。

[0093] 本发明并不局限于使用掌上型终端的主要单元的情况,并且甚至当使用任何信息处理设备而不是掌上型终端的主要单元时也能够使用本发明。

[0094] 此外,本发明并不局限于使用 PIN 输入单元的情况,并且甚至当使用任何附加功能单元而不是 PIN 输入单元时,本发明也是可适用的。

[0095] 此外,本发明并不局限于使用哈希值的情况,并且甚至当使用任何单向函数值而不是哈希值时,本发明也是可适用的。

[0096] 另外,使附加功能单元生效 / 失效的上述系统的各组件能够通过硬件、软件或者它们的组合来实现。此外,由使附加功能单元生效 / 失效的上述系统所执行的使附加功能单元生效 / 失效的方法也能够通过硬件、软件或者它们的组合来实现。同时,系统或方法通过软件来实现表示系统或方法在计算机读取和运行程序时实现。

[0097] 程序使用各种类型的非暂时计算机可读介质来存储,并且能够提供给计算机。非暂时计算机可读介质包括各种类型的有形存储介质。非暂时计算机可读介质的示例包括磁记录介质(例如软盘、磁带和硬盘驱动器)、磁光介质(例如磁光盘)、CD-ROM(只读存储器)、CD-R、CD-R/W、半导体存储器(例如掩模型 ROM、PROM(可编程 ROM)、EPROM(可擦 PROM)、闪速 ROM 和 RAM(随机存取存储器))。此外,程序可通过各种类型的暂时计算机可读介质来提供给计算机。暂时计算机可读介质的示例包括电信号、光信号和电磁波。暂时计算机可读介质能够通过诸如导线或光纤之类的有线通信信道或者无线通信信道将程序提供给计算机。

[0098] 虽然能够如以下补充注释中一样来描述上述实施例的部分或整体,但是上述实施例的部分或整体并不局限于以下内容。

[0099] (补充注释 1)

[0100] 一种使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的方法,包括下列步骤:

[0101] 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值,并且在制造时将第一单向函数值存储在附加功能单元中;

[0102] 在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值;以及

[0103] 当第一单向函数值和第二单向函数值不同时,使附加功能单元的功能失效。

[0104] (补充注释 2)

- [0105] 在补充注释 1 所述的使附加功能单元生效 / 失效的方法中，
由信息处理设备来计算第二单向函数值，
将第二单向函数值从信息处理设备传送给附加功能单元，以及
由附加功能单元来比较第一单向函数值和第二单向函数值。
[0109] (补充注释 3)
- [0110] 补充注释 1 中所述的使附加功能单元生效 / 失效的方法还包括下列步骤：
[0111] 针对每一应用程序基于应用程序的数据来计算第三单向函数值，并且在制造时将第三单向函数值存储在附加功能单元中；
[0112] 在激活信息处理设备之后针对每一应用程序基于应用程序的数据来计算第四单向函数值；以及
[0113] 当应用程序的至少一部分的第三单向函数值和第四单向函数值不同时，使附加功能单元的功能失效。
[0114] (补充注释 4)
- [0115] 在补充注释 3 所述的使附加功能单元生效 / 失效的方法中，
由信息处理设备来计算第四单向函数值，
将第四单向函数值从信息处理设备传送给附加功能单元，以及
由附加功能单元来比较第三单向函数值和第四单向函数值。
[0119] (补充注释 5)
- [0120] 补充注释 1 中所述的使附加功能单元生效 / 失效的方法还包括下列步骤：
[0121] 基于多个应用程序的数据来计算第五单向函数值，并且在制造时将第五单向函数值存储在附加功能单元中；
[0122] 在激活信息处理设备之后基于多个应用程序的数据来计算第六单向函数值；以及
[0123] 当第五单向函数值和第六单向函数值不同时，使附加功能单元的功能失效。
[0124] (补充注释 6)
- [0125] 在补充注释 5 所述的使附加功能单元生效 / 失效的方法中，
由信息处理设备来计算第六单向函数值，
将第六单向函数值从信息处理设备传送给附加功能单元，以及
由附加功能单元来比较第五单向函数值和第六单向函数值。
[0129] (补充注释 7)
- [0130] 一种使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的系统，具有：
[0131] 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值并且在制造时将第一单向函数值存储在附加功能单元中的部件；
[0132] 在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值的部件；以及
[0133] 当第一单向函数值和第二单向函数值不同时使附加功能单元的功能失效的部件。
[0134] (补充注释 8)
- [0135] 在补充注释 7 所述的使附加功能单元生效 / 失效的系统中，
由信息处理设备来计算第二单向函数值，

- [0137] 将第二单向函数值从信息处理设备传送给附加功能单元, 以及
- [0138] 由附加功能单元来比较第一单向函数值和第二单向函数值。
- [0139] (补充注释 9)
- [0140] 补充注释 7 中所述的使附加功能单元生效 / 失效的系统还具有 :
- [0141] 针对每一应用程序基于应用程序的数据来计算第三单向函数值并且在制造时将第三单向函数值存储在附加功能单元中的部件 ;
- [0142] 在激活信息处理设备之后针对每一应用程序基于应用程序的数据来计算第四单向函数值的部件 ; 以及
- [0143] 当应用程序的至少一部分的第三单向函数值和第四单向函数值不同时使附加功能单元的功能失效的部件。
- [0144] (补充注释 10)
- [0145] 在补充注释 9 所述的使附加功能单元生效 / 失效的系统中,
- [0146] 由信息处理设备来计算第四单向函数值,
- [0147] 将第四单向函数值从信息处理设备传送给附加功能单元, 以及
- [0148] 由附加功能单元来比较第三单向函数值和第四单向函数值。
- [0149] (补充注释 11)
- [0150] 补充注释 7 中所述的使附加功能单元生效 / 失效的系统还具有 :
- [0151] 基于多个应用程序的数据来计算第五单向函数值并且在制造时将第五单向函数值存储在附加功能单元中的部件 ;
- [0152] 在激活信息处理设备之后基于多个应用程序的数据来计算第六单向函数值的部件 ; 以及
- [0153] 当第五单向函数值和第六单向函数值不同时使附加功能单元的功能失效的部件。
- [0154] (补充注释 12)
- [0155] 在补充注释 11 所述的使附加功能单元生效 / 失效的系统中,
- [0156] 由信息处理设备来计算第六单向函数值,
- [0157] 将第六单向函数值从信息处理设备传送给附加功能单元, 以及
- [0158] 由附加功能单元来比较第五单向函数值和第六单向函数值。
- [0159] (补充注释 13)
- [0160] 一种使计算机用作使对其添加附加功能单元的信息处理设备中的附加功能单元生效 / 失效的系统的程序, 使计算机用作 :
- [0161] 基于存储引导加载程序和操作系统的记录介质中包含的数据来计算第一单向函数值并且在制造时将第一单向函数值存储在附加功能单元中的部件 ;
- [0162] 在激活信息处理设备之后基于记录介质中包含的数据来计算第二单向函数值的部件 ; 以及
- [0163] 当第一单向函数值和第二单向函数值不同时使附加功能单元的功能失效的部件。
- [0164] (补充注释 14)
- [0165] 补充注释 13 中所述的程序还使计算机令 :
- [0166] 信息处理设备计算第二单向函数值 ;
- [0167] 信息处理设备将第二单向函数值传送给附加功能单元 ; 以及

- [0168] 附加功能单元比较第一单向函数值和第二单向函数值。
- [0169] (补充注释 15)
- [0170] 在补充注释 13 中所述的程序还使计算机用作：
- [0171] 针对每一应用程序基于应用程序的数据来计算第三单向函数值并且在制造时将第三单向函数值存储在附加功能单元中的部件；
- [0172] 在激活信息处理设备之后针对每一应用程序基于应用程序的数据来计算第四单向函数值的部件；以及
- [0173] 当应用程序的至少一部分的第三单向函数值和第四单向函数值不同时使附加功能单元的功能失效的部件。
- [0174] (补充注释 16)
- [0175] 在补充注释 15 中所述的程序还使计算机令：
- [0176] 信息处理设备计算第四单向函数值；
- [0177] 信息处理设备将第四单向函数值传送给附加功能单元；以及
- [0178] 附加功能单元比较第三单向函数值和第四单向函数值。
- [0179] (补充注释 17)
- [0180] 在补充注释 13 中所述的程序还使计算机用作：
- [0181] 基于多个应用程序的数据来计算第五单向函数值并且在制造时将第五单向函数值存储在附加功能单元中的部件；
- [0182] 在激活信息处理设备之后基于多个应用程序的数据来计算第六单向函数值的部件；以及
- [0183] 当第五单向函数值和第六单向函数值不同时使附加功能单元的功能失效的部件。
- [0184] (补充注释 18)
- [0185] 在补充注释 17 中所述的程序还使计算机令：
- [0186] 信息处理设备计算第六单向函数值；
- [0187] 信息处理设备将第六单向函数值传送给附加功能单元；以及
- [0188] 附加功能单元比较第五单向函数值和第六单向函数值。
- [0189] (补充注释 19)
- [0190] 一种添加到信息处理设备的附加功能单元，具有：
- [0191] 在制造时存储基于存储引导加载程序和操作系统的记录介质中包含的数据所计算的第一单向函数值的部件；以及
- [0192] 当激活信息处理设备之后基于记录介质中包含的数据所计算的第二单向函数值和第一单向函数值不同时使附加功能单元的功能失效的部件。
- [0193] (补充注释 20)
- [0194] 在补充注释 19 中所述的附加功能单元，还具有：
- [0195] 在制造时针对每一应用程序来存储基于应用程序的数据所计算的第三单向函数值的部件；以及
- [0196] 当激活信息处理设备之后针对每一应用程序基于应用程序的数据所计算的第四单向函数值和第三单向函数值不同时使附加功能单元的功能失效的部件。
- [0197] (补充注释 21)

- [0198] 在补充注释 19 中所述的附加功能单元,还具有 :
- [0199] 在制造时存储基于多个应用程序的数据所计算的第五单向函数值的部件;以及
- [0200] 当激活信息处理设备之后基于多个应用程序的数据所计算的第六单向函数值和第五单向函数值不同时使附加功能单元的功能失效的部件。
- [0201] (补充注释 22)
- [0202] 一种使计算机用作使添加到信息处理设备的附加功能单元生效 / 失效的设备的程序,使计算机用作 :
- [0203] 在制造时存储基于存储引导加载程序和操作系统的记录介质中包含的数据所计算的第一单向函数值的部件;以及
- [0204] 当激活信息处理设备之后基于记录介质中包含的数据所计算的第二单向函数值和第一单向函数值不同时使附加功能单元的功能失效的部件。
- [0205] (补充注释 23)
- [0206] 在补充注释 22 中所述的程序还使计算机用作 :
- [0207] 在制造时针对每一应用程序来存储基于应用程序的数据所计算的第三单向函数值的部件;以及
- [0208] 当激活信息处理设备之后针对每一应用程序基于应用程序的数据所计算的第四单向函数值和第三单向函数值不同时使附加功能单元的功能失效的部件。
- [0209] (补充注释 24)
- [0210] 在补充注释 22 中所述的程序还使计算机用作 :
- [0211] 在制造时存储基于多个应用程序的数据所计算的第五单向函数值的部件;以及
- [0212] 当激活信息处理设备之后基于多个应用程序的数据所计算的第六单向函数值和第五单向函数值不同时使附加功能单元的功能失效的部件。
- [0213] 本申请基于日本专利申请 No. 2011-030746(2011 年 2 月 16 日提交),并且根据巴黎公约要求基于日本专利申请 No. 2011-030746 的优先权。参照日本专利申请 No. 2011-030746,将日本专利申请 No. 2011-030746 的公开结合到本描述中。
- [0214] 虽然详细描述了本发明的典型实施例,但是应当理解,能够进行各种变更、替换及替代,而没有背离附权利要求书所限定的本发明的精神和范围。此外,如果在提交申请时修正权利要求书,则发明人意在保持所要求保护发明的统一范围。
- [0215] { 参考标号列表 }
- [0216] 101 存储装置
- [0217] 102 ROM
- [0218] 103 RAM
- [0219] 104 中央控制单元
- [0220] 105 显示单元
- [0221] 106 副 CPU
- [0222] 107 程序存储器
- [0223] 108 数据存储器
- [0224] 109 键盘
- [0225] 110 IC 卡单元

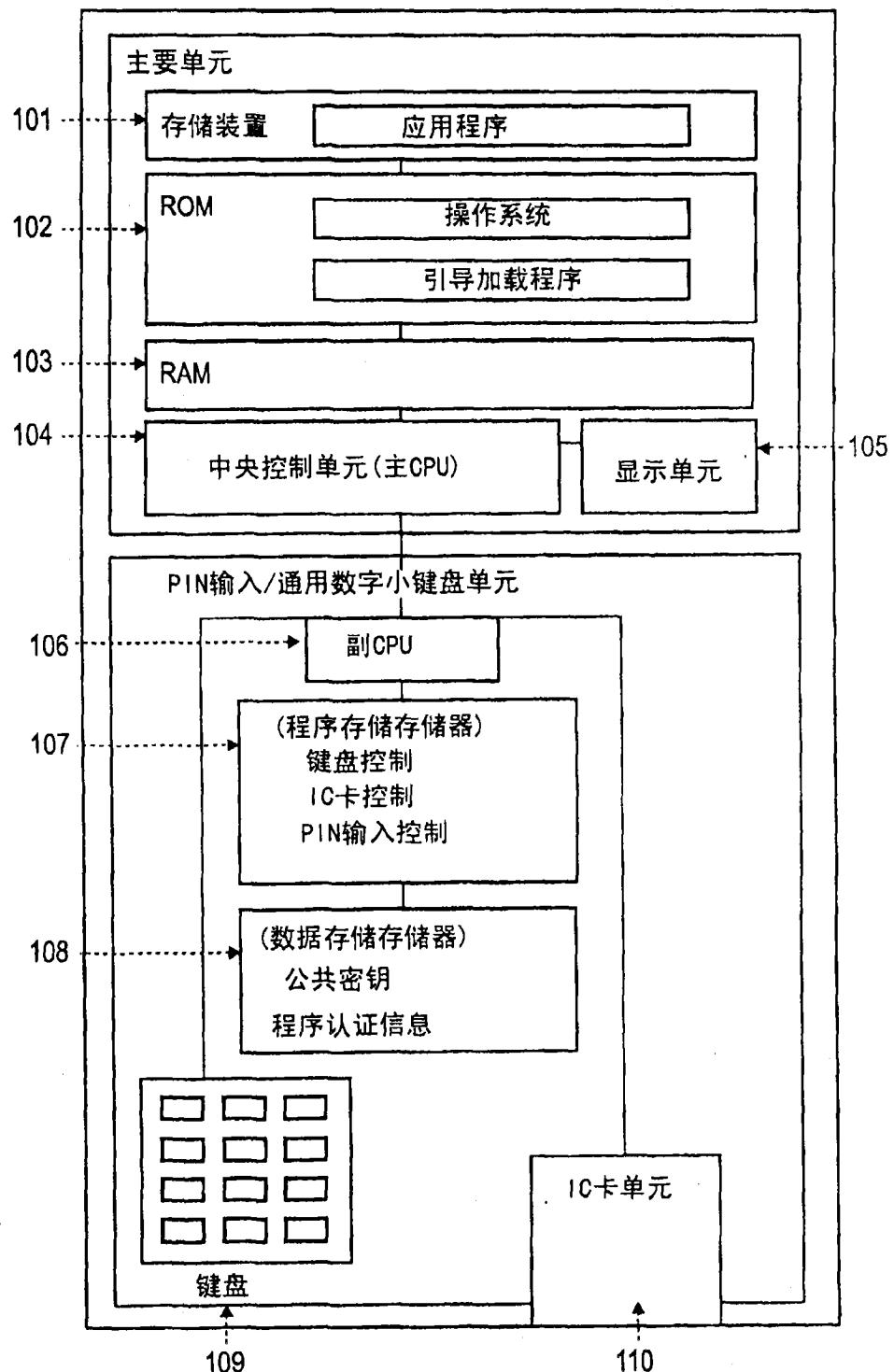


图 1

201 程序ID	202 程序哈希值

图 2

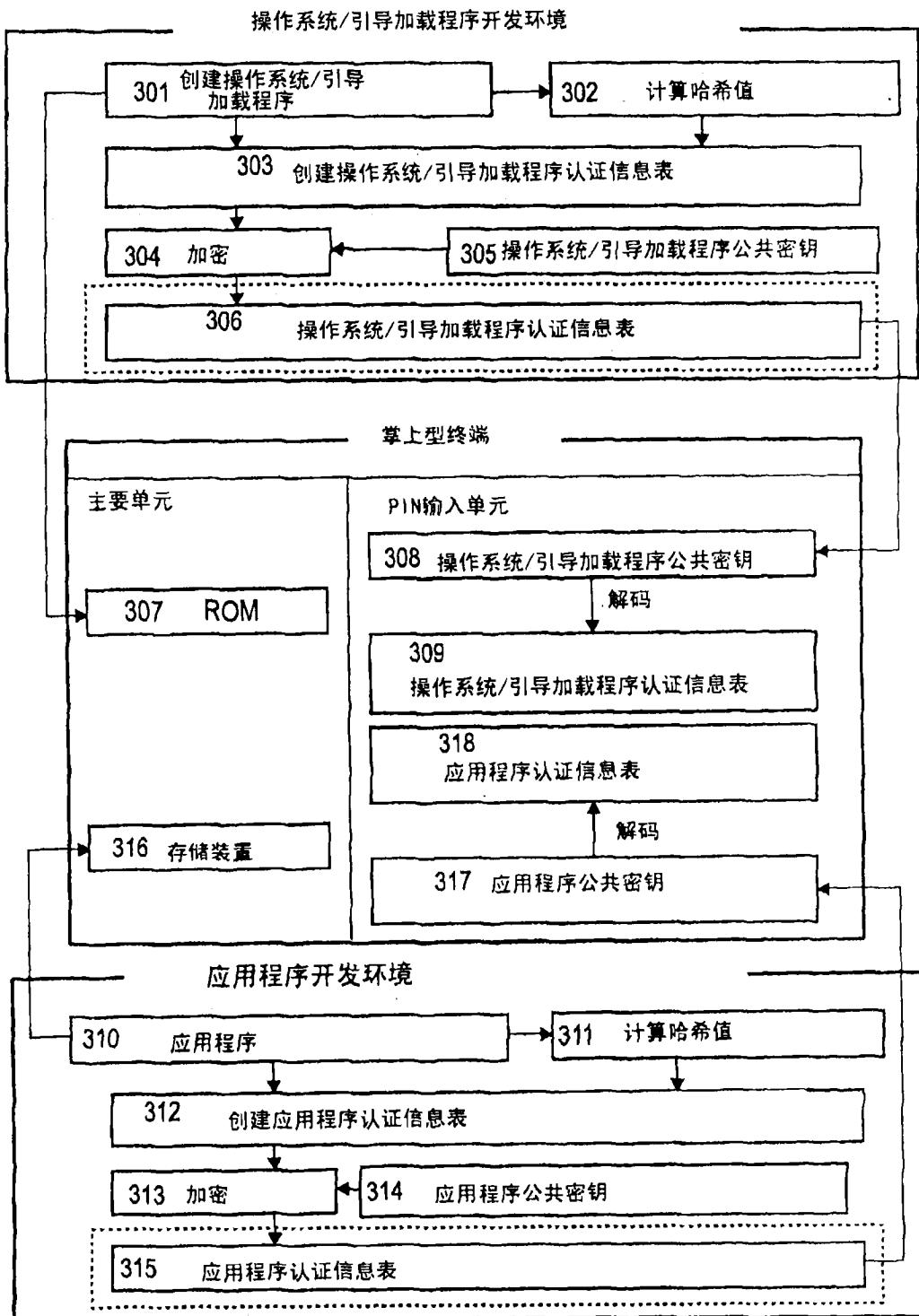


图 3

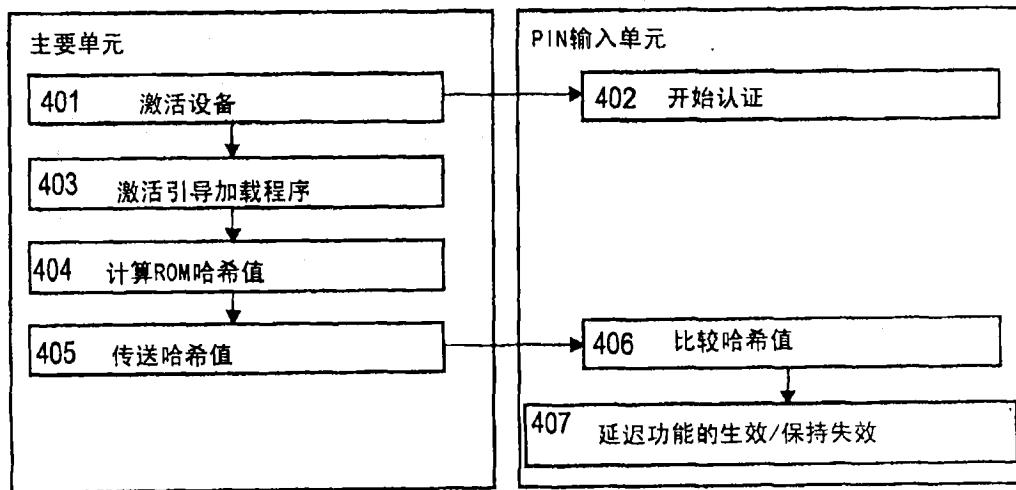


图 4



图 5