[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 1/00

[12]发明专利申请公开说明书

[21]申请号 00807632.4

[43]公开日 2002年5月22日

[11]公开号 CN 1350670A

[22]申请日 2000.5.15 [21]申请号 00807632.4
[30]优先权
[32]1999.5.17 [33]US [31]09/313,295
[86]国际申请 PCT/US00/13239 2000.5.15
[87]国际公布 WO00/70429 英 2000.11.23
[85]进入国家阶段日期 2001.11.16
[71]申请人 波系统股份有限公司
地址 美国马萨诸塞州
[72]发明人 S·K·斯普拉格
G·J·卡滋梅尔克扎克

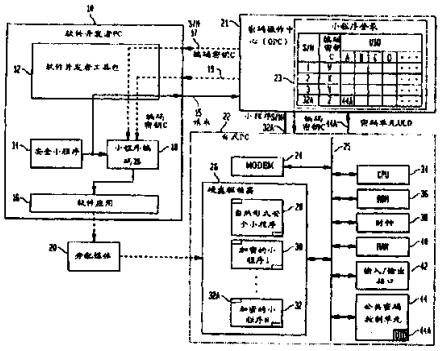
[74]专利代理机构 上海专利商标事务所
代理人 李 湘

权利要求书6页 说明书16页 附图页数11页

[54]发明名称 公共密钥控制单元及其系统

[57]摘要

一个普遍适用的公共密码控制单元(密码单元)被用于被多个独立用户共享 的密码系统。作外围设备安装在通用计算机的密码单元加载和卸载加密的安全小 程序到运行每个安全小程序的密码单元的 RAM 存储器。密码单元和包括它的系统 提供一个安全的内部环境,其中只有预先批准的安全小程序被授予加载和运行的 许可。在密码单元中的计算环境由于与每个密码单元通讯的密码操作中心(OPC) 而成为安全的。在分配给定的安全小程序以便得到对给定安全小程序的必要的许 可以前,软件开发者提交一个提出的安全小程序给 OPC。仅当从 OPC 得到所有必 要的许可时,一个给定的安全小程序才被允许去密码单元内加载运行。当第一安 全小程序结束运行时,密码将加密形式的当前加载的第一安全小程序卸载(换上) 到 PC 的硬盘,并加载(换入)下一个安全小程序。每个安全小程序的密码内容 被保存储存在 PC 硬盘驱动器的文件中。以那样的方式,单个密码单元在多个独 立的用户之间被共享。



ISSN1008-4274

权 利 要 求 书

1、一种用于密码密钥分配系统的方法，系统包括一个具有一个密码控制单元的用户计算机、一个软件开发者计算机和一个密码操作中心，其特征在于所述方法包括：

在所述的软件开发者计算机上产生另一个安全小程序；

将所述的第一程序从所述软件开发者计算机发送到所述密码操作中心；

在所述的软件开发者计算机上从所述的密码操作中心接收第一密码密钥；

在所述软件开发者计算机上从所述密码操作中心接收第一序列号；

在加密所述第一安全小程序以形成第一加密的安全小程序的过程中使用所述的第一密码密钥；

将所述第一序列号附列至所述第一加密安全小程序上以形式第一安全包；以及

分配所述第一安全包到所述用户计算机。

2、如权利要求 1 所述的方法，其特征在于所述密码控制单元包括一个程序控制存储器，所述方法还包括；

将所述第一系列号从所述密码控制单元发送到所述密码操作中心；

在所述密码控制单元接收来自所述密码操作中心的第一密码密钥；

在从所述第一加密安全小程序解密所述第一安全小程序的过程中使用第一密码密钥；以及

将所述第一安全小程序加载到所述程序控制存储器。

3、如权利要求 1 所述的方法，其特征在于在加密所述第一安全小程序以形成一加密的安全小程序的过程中使用所述第一密码密钥的所述步骤还包括：

在所述软件开发者计算机上借助于程序员密钥加密所述第一安全小程序以形成程序员加密的安全小程序；

在所述软件开发者计算机上借助于所述第一密码密钥加密所述程序员密钥以形成第一加密的程序员密钥；

附上所述第一加密的程序员密钥和所述第一程序员加密的安全小程序以形成所述第一加密的安全小程序。

4、如权利要求 2 所述的方法，其特征在于所述软件开发者计算机还包括借助所述第一密码密钥加密的程序员密钥以形成在所述第一加密的安全小程序中的第一加密的程序员密钥；而且当在所述用户计算机上从所述第一加密安全小程序解密所述第一安全小程序的过程中使用所述第一密码密钥的所述步骤包括：

在所述用户计算机上接收包括所述第一程序员加密的安全小程序的所述第一

安全包；

在所述用户计算机借助于所述第一密码密钥解密所述第一加密的程序员密钥以形成一个复原的程序员密钥；以及

借助所述复原的程序员密钥解密所述第一程序员加密安全小程序以复原所述的第一安全小程序。

5、如权利要求 1 所述的方法，其特征在于还包括：

存储一个记录多个安全小程序、密码密钥和序列号之间对应关系的安全小程序登录表，所述安全小程序登录表具有一个条目，指出所述第一序列号和所述第一密码密钥对应于所述第一安全小程序。

6、如权利要求 2 所述的方法，其特征在于所述用户计算机包括第一用户识别号，所述方法还包括：

从所述用户计算机将所述第一用户识别号发送到所述密码操作中心；

存储一个记录多个安全小程序、密码密钥、序列号和用户识别号之间对应关系的安全小程序登录表，所述安全小程序登录表具有一个条目，指出所述第一序列号，所述第一密码密钥和所述第一用户识别号对应于所述第一安全小程序。

7、如权利要求 2 所述的方法，其特征在于所述用户计算机还包括一个用户计算机硬盘驱动存储器，且所述系统还包括第二软件开发者计算机、一个具有相应第二序列号及与之对应的第二密码密钥的第二安全小程序，所述方法还包括：

在使用第一用户计算机密钥形成第一加密的安全内容的过程中加密所述用户控制存储器的内容；

将所述第一加密的安全内容储存在所述用户计算机硬盘驱动存储器；且在所述程序控制存储器加载所述第二安全小程序。

8、如权利要求 7 所述的方法，其特征在于还包括：

在使用第二用户计算机密钥形成第二加密安全内容的过程中加密所述用户控制存储器的内容；

将所述第二加密的安全内容存储在所述用户计算机的硬盘驱动器；

在使用所述第一用户计算机密钥复原所述第一安全内容的过程中解密所述第一加密安全内容；且

在所述程序控制存储器加载所述第一安全内容。

9、一种用于密码密钥分配系统的装置，系统包括一个具有一个密码控制单元的用户计算机、一个软件开发者计算机和一个密码操作中心，其特征在于所述装置包括：

用于在所述软件开发者计算机上产生第一安全小程序的装置；

用于将所述第一安全小程序从所述软件开发者计算机发送到所述密码操作中

心的装置；

用于在所述软件开发者计算机从所述密码操作中心接收第一密码密钥的装置；

用于在所述软件开发者计算机从所述密码操作中心接收第一序列号的装置；

用于在解密所述第一安全小程序以形成第一解密安全小程序的过程中使用的第一密码密钥的装置；

用于将所述第一序列号附在所述第一解密安全小程序以形成第一安全包的装置；和

用于将所述第一安全包分配到所述用户计算机的装置。

10、如权利要求 9 所述的装置，其特征在于所述密码控制单元包括一个程序控制存储器，所述装置还包括：

用于将所述第一序列号从所述密码控制单元发送到所述密码操作中心的装置；

用于在所述密码控制单元上从所述密码操作中心接收所述第一密码密钥的装置；

用于在从所述第一加密的安全小程序解密所述第一安全小程序的过程中使用所述密码密钥的装置；和

用于将所述第一安全小程序加载到所述程序控制存储器的装置。

11、如权利要求 9 所述的装置，其特征在于用于在加密所述第一安全小程序以形成第一加密安全小程序的过程中使用所述第一密码密钥的装置还包括：

用于在所述软件开发者计算机上借助一个程序员密钥加密所述第一安全小程序以形成第一程序员加密的安全小程序的装置；

用于在所述软件开发者计算机上借助所述第一密码密钥加密所述程序员密钥以形成第一加密的程序员密钥的装置；

用于附上所述第一加密的程序员密钥和所述第一程序员加密安全小程序以形成所述第一加密的安全小程序的装置。

12 如权利要求 10 所述的装置，其特征在于所述软件开发者计算机还包括一个借助于所述第一密码密钥加密的程序员密钥，它用于形成在所述第一加密安全小程序中的第一加密程序员密钥，而且用于所述用户计算机上从所述第一程序员加密的安全小程序解密所述第一安全小程序的过程中使用第一密码密钥的所述装置包括：

用于在所述用户计算接收包括所述第一程序员加密的安全小程序的所述第一安全包的装置；

用于在所述用户计算机上借助所述第一密码密钥解密所述第一加密程序员密

钥以形成一个复原的程序员密钥的装置；

用于借助所述复原的程序员密钥解密所述第一程序员加密的安全小程序以复原所述第一安全小程序的装置。

13、如权利要求 9 所述的装置，其特征在于还包括：

用于存储记录多个安全小程序、密码密钥和序列号之间对应关系的安全小程序登录表的装置，所述安全小程序登录表具有一个条目，指出第一序列号和所述第一密码密钥对应于所述第一安全小程序。

14、如权利要求 10 所述的装置，其特征在于所述用户计算机包括一个第一用户识别号，所述装置还包括：

用于将所述第一用户识别号从所述用户计算机发送到所述密码操作中心；

用于存储记录多个安全小程序、密码密钥、序列号和用户识别号之间对应关系的一个安全小程序登录表的装置，所述安全小程序登录表具有一个条目，指出所述第一序列号、所述第一密码密钥和所述第一用户识别号对应于所述第一安全小程序。

15、如权利要求 10 所述的装置，其特征在于所述用户计算机还包括一个用户计算机硬盘驱动存储器，且所述系统还包括一个第二软件开发计算机、一个具有相应的第二序列号及与之对应的第二密码密钥的第二安全小程序，所述装置还包括：

用于在使用第一用户计算机形成第一加密的安全内容的过程中加密所述用户控制存储器的装置；

用于将第一加密的安全内容存入所述用户计算机的硬盘驱动存储器装置；和

用于将所述第二安全小程序加载到的程序控制存储器的装置。

16、如权利要求 15 所述的装置，其特征在于还包括；

用于在使用第二用户计算机密钥形成第二加密安全内容的过程中加密所述用户控制存储器的装置；

用于将所述第二加密的安全内容存入所述用户计算机硬盘驱动存储器的装置；

用于在使用所述第一用户计算机密钥所述第一安全小程序的过程中解密所述第一加密的安全内容的装置；和

用于将所述第一安全内容加载到所述程序控制存储器的装置。

17、一种用于密码密钥分配系统的方法，系统包括一个具有一个密码控制单元的用户计算机、一个软件开发者计算机和一个密码操作中心，所述软件开发者计算机产生第一安全小程序，它在使用第一密码密钥形成第一加密的安全小程序的过程中加密所述的第一安全小程序，并将所述第一加密的安全小程序分配到所

述的用户计算机，其特征在于在所述密码操作中心上的密码密钥分配方法包括：

在所述密码操作中心从所述软件开发者计算机接收所述第一安全程序；

将第一序列号从所述密码操作中心发送到所述软件开发者计算机；

将第一密码密钥从所述密码操作中心发送到所述软件开发者计算机；

在所述密码操作中心从所述密码控制单元接收所述第一序列号；

将所述第一密码密钥从所述密码操作中心发送到所述密码控制单元。

18、如权利要求 17 所述的方法，其特征在于所述密码控制单元包括一个程序控制存储器，所述的方法还包括：

在所述密码控制单元接收包括第一序列号的第--加密安全小程序；

将所述第一序列号从所述密码控制单元发送到所述密码操作中心；

在所述密码控制单元从所述密码操作中心接收所述第一密码密钥；

在从所述第一加密的安全小程序解密所述第一安全小程序的过程中使用所述第一密码密钥；和

将所述第一安全小程序加载到所述程序控制存储器。

19、一种用于密码密钥分配系统的方法，系统具有一个软件开发者计算机和一个密码操作中信，所述软件开发者计算机产生一个由第一序列号识别的第一安全小程序并在使用第一密码密钥形成第一加密安全小程序的过程中加密所述第一安全小程序，所述系统进一步包括具有带一个程序控制存储器的密码控制单元的用户计算机，其特征在于所述方法包括：

在所述密码控制中心接收包括所述第一序列号的第一安全小程序；

将所述第一序列号发送到所述密码操作中心；

在所述密码控制单元从所述密码操作中心接收所述第一密码密钥；

在从所述第一加密安全小程序解密所述第一安全小程序的过程中使用所述第一密码密钥；和

将所述第一安全小程序加载到所述程序控制存储器。

20、在一个密码密钥分配系统中，包括一个具有密码控制单元的用户计算机、一个软件开发者计算机和一个密码操作中心，所述软件开发者计算机产生一个第一安全小程序并在使用第一密码密钥形成第一加密的安全小程序的过程中加密所述第一安全小程序，并将所述第一安全小程序分配到所述用户计算机，其特征在于所述密码操作中心处的密码密钥分配装置包括：

用于在所述密码操作中心从所述软件开发者计算机接收所述第一安全小程序的装置；

用于将第一序列号从所述密码操作中心发送到所述软件开发者计算机的装置；

用于将所述第一密码密钥从所述密码操作中心发送到所述软件开发者计算机的装置；

用于在所述密码操作中心从所述密码控制单元接收所述第一序列号的装置；

用于将所述第一密码密钥从所述密码操作中心发送到所述密码控制中心的装置。

21、如权利要求 20 所述的装置，其特征在于所述密码控制单元包括一个程序控制存储器，所述装置还包括：

用于在所述密码控制单元接收包括所述第一序列号的第一加密的安全小程序的装置；

用于将所述第一序列号从所述密码控制单元发送到所述密码操作中心的装置；

用于在所述密码控制单元从所述密码操作中心接收所述第一密码密钥的装置；

用于在从所述第一安全小程序解密所述第一安全小程序的过程中使用所述第一密码密钥的装置；和

用于将所述第一安全小程序加载到所述程序控制存储器的装置。

22、在一个密码密钥分配系统中，具有一个软件开发者计算机和一个密码操作中心，所述软件开发者计算机产生一个由第一序列号识别的第一安全小程序并在使用第一密码密钥形成第一加密安全小程序的过程中加密所述第一安全小程序，所述系统还包括具有带程序控制存储器的密码控制单元的用户计算机，其特征在于装置包括：

用于在所述密码控制单元接收包括第一序列号的第一安全小程序的装置；

用于将第一序列号发送到所述密码操作中心的装置；

用于在所述密码控制单元从所述密码操作中心接收所述第一密码密钥的装置；

用于在从所述第一加密的安全小程序解密所述第一安全小程序的过程中使用所述第一密码密钥的装置；

将所述第一安全小程序加载到所述程序控制存储器。

说　明　书

公共密钥控制单元及其系统

发明领域

本发明涉及密码系统，尤其是涉及一个密钥管理系统及一个共享的公共密码控制单元。

发明背景

许多计算机应用需要实现一个或多个安全功能。计算机程序的安全功能是它防止用户胡乱篡改的特点及操作。

例如，一个软件程序可以具有一个过时日期，在此日期之后程序变成不能运行。但是典型的软件过时功能是不安全的，因为只要将当地计算机时间设置成较早的时间，或者修改该软件使其跳过核时当地计算机时钟的软件，此功能就失效了。

作为另一个例子，一个保存从当地的加密数据度存放数据的记录用于支付当地加密数据库的登记使用的计算机程序通常具有两个关键的寄存器。第一个寄存器表示过去数据使用的量，另一个寄存器表示余数的量。如果更新该寄存器和存款寄存器不是一个安全的功能，用户能减少使用寄存器的内容和／或增加存款寄存器的内容使该系统失效。类似地，为租赁支付目的保存租赁软件的使用记录的租赁软件也需要防止用户对租赁记账寄存器和其他重要的内部寄存器及功能的胡乱篡改。

作为另一个例子，一个远程访问的数据库能对授权的用地该数据库的访问收费。常需要一个安全系统在授权访问该数据库之前识别每个用户的身份。然而另一个安全系统是密钥管理系统，即将密码密钥分配给授权的用户。

一类安全功能解决方法是在软件中实现安全功能。在软件中实现安全功能具有经济上的优点。软件实现也具有通用的优点。但是，在软件中实现软件安全性功能不象在硬件中实现安全功能那样安全。另一方面，与软件相比，硬件实现安全功能费用更高，且可能对每个应用需要专用的硬件。如果每个应用需要它本身的专用的硬件，硬件实现安全功能将是不通用的。

发明内容

本发明以一个方法和装置实现，使用密码控制单元作为在由多个独立的用户共享的系统中广泛适用的公共密码控制单元（密码单元）。

密码单元包括一个具有允许安全共享密码单元资源的专用硬件和固件的通用计算机处理器。尤其是该密码单元包括一个带有只读存储器（ROM）控制程序的专用核心的微处理器芯片，一个通用随机存储器（RAM），一个实时时钟和一个主机输入／输出接口（即与台式 PC 的连接）。此外，该密码单元包括一个 DES（数据加密标准）引擎，用于密码密钥的安全非易失性存储，一个签名寄存 RAM 存储器和专用访问寄存器。

密码单元作为外围设备安装在任何如台式 PC 那样的通用计算机中。使单元成为“公共”的密码控制单元是它作一个安全的计算资源适用于在 PC 上运行的主要应用程序。

为了使用密码单元资源，对应于安全功能的主应用程序的一个部分被储存在 PC 上。这里称为安全小程序（Secure Applet）的安全功能加载到运行每个安全小程序的密码单元的板上的 RAM 或从上卸载。模仿下载并运行内部浏览器的 Jave 小程序（Jave applet），安全小程序是可移植的、可执行的文件以便加载到适合的计算实体并实现一个或多个安全功能。在此意义上，此密码单元象一个专用的协处理器，适用于运行安全应用程序（小程序）。

PC 使安全小程序加载到密码单元的程序控制单元，后者运行该小程序并将安全功能的结果返回到 PC。但是，不象一个通常的协处理器，对密码单元的访问不完全在台式 PC 的控制下。即，台式 PC 可以不加载和运行任何安全小程序。密码单元和系统的一部分提供其安全内部环境，只有某些安全小程序被许可加载并在密码单元运行。

为保障在密码单元的计算环境，提供一个密码运行中心（OPC），它与密码单元通讯。尤其是首次遇到新安全小程序，并在该新安全小程序被允许在公共密码单元运行以前，该密码单元与 OPC 通讯。在新密码单元首次被安装在台式 PC 时该密码单元也与 OPC 通讯。该密码单元也在定期时间周期基础上与 OPC 通讯。此外，软件开发者在为了得到必要的许可，使给定的安全小程序加载并运行在该密码单元而分配给定的安全小程序以前也要与 OPC 通讯。仅当从 OPC 获得所有必要的许可时，给定的安全小程序被允许加载并运行在密码单元。

操作系统

密码单元操作系统（O/S）包括两个部分：一个 ROM 加载控制程序，和一个自然形式安全小程序（native mode security applet），ROM 加载控制程序是控制程序的压缩专用核心，它被储存在密码单元的 ROM 中。可以由软盘、CDROM 或电话线调制解调器分配的自然形式安全小程序是可移植及可写的文件，通常被存入台式 PC 的硬盘中。

重要的安全功能在 ROM 加载控制程中实现。尤其是，ROM 加载控制程序控制将安全小程序到密码单元及外部资源的加载和从其中卸载，包括将自然形式安全小程序的加载和卸载。

自然模式安全小程序具有两个主要功能：在首次使用密码单元时将密码单元登录到 OPC，并授予首次使用每个单元应用安全小程序的许可。作为一般规则，每当该密码单元与 OPC 通讯时使用自然形式安全小程序。

系统操作

在其安全软件应用程序中希望使用公共密码控制单元的应用软件开发者首先提交一份提出的安全小程序给 OPC 作为考虑。该提出的安全小程序必须满足包括安全标准的某些标准。例如，提出的安全小程序必须小到足以适合到在密码单元的板上 RAM。OPC 进一步审查该提出的安全小程序是否符合安全标准。

在完成所有安全符合性测试以后，OPC 授予或拒绝该提出的安全小程序使用庐密码的许可。允许使用所提出的安全小程序包括指定一个序列号及编码密钥 C 给该提出的安全小程序。序列号及编码密钥 C 被存入 OPC 中的小程序登录处。开发者在一个加密该建议的安全小程序的过程中使用庐编码密钥 C，并使用该序列号识别该加密的安全小程序。

在启动台式 PC 初始化时，密码 ROM 加载控制程序将自然形式安全小程序加载到在该密码单元的板上 RAM 中。虽然 ROM 加载控制程序以前已经从 OPC 授予加载到并在该密码单元运行的许可，它还测试该自然形式安全小程序。

ROM 加载控制程序方便了在多个用户之中共享使用该密码单元。尤其是，ROM 加载控制程序将自然形式安全小程序从在密码的板上 RAM 卸载（换出）到台式 PC 的硬盘上以便腾出空间来加载（换入）第一应用安全小程序到板上的 RAM。

然后，该 ROM 加载控制程序在加载第一应用安全小程序时予以检查。在确定该加载的第一应用安全小程序是有资格访问该密码单元资源以后，在该密码单元的微处理器运行该第一安全小程序，随后将该铁控制转移给该第一安全小程序。

当第一安全小程序完成时，该密码单元卸载（换出）加密形式的当前加载的第一安全小程序到 PC 的硬盘驱动器，并加载（换入）下一个安全小程序。每个安全小程序的密码内容被保存在储存在 PC 硬盘上的文件中。以那样的方式，单个密码单元在多个独立用户之中被共享。

如果遇到一个未知的应用安全小程序（即从未被加载到特定的密码单元的安全小程序），该 ROM 加载控制程序换回到自然上程序，它建立一个与 OPC 的安全通信会话。如果写此未知应用安全小程序的开发者以前被 OPC 授予加载和运行该安全应用程序的许可，则该密码单元将从 OPC 接收解密和运行该未知应用安全小

程序所必需的密码密钥。同时，OPC 在该小程序登录处记录该密码单元用户识别符，然后将该密码单元与该 OPC 授予加载及运行许可的安全小程序相关联。以后，该密码单元将加载与卸载该安全小程序而不必再与 OPC 通讯。

最后，当没有应用安全小程序与运行时，该 ROM 加载控制程序将自然形式安全小程序换回放入密码单元的板上 RAM。以这样的方式，每个单独的用户将密码单元使用于分别各自的安全应用程序。因此，使用多个单独的安全应用程序的多个单独的用户共享此密码单元。

附图概述

图 1 是按照本发明的一个公共密码系统的方块图。

图 2 是按照本发明的一个公共密码单元的广场图。

图 3A 是一个流程图，示出了按照本发明产生一个加密小程序的方法和装置。

图 3B 是一个流程图，示出了按照本发明一个加密的小程序并将该的小程序加载到一个公共密码控制系统的板上 RAM 中的方法和装置。

图 4 是用于在 PC 硬盘驱动存储器中储存一个加密的安全小程序的安全存储页格式的概图。

图 5 是一个流程图，示出按照本发明在密码运行中心一个安全小程序的台式开发者登录过程。

图 6 是一个流程图，示出按照本发明在密码运行中心一个安全小程序的台式 PC 机初始化过程。

图 7 是一个流程图，示出按照本发明由 O/S 的 ROM 加载控制程序部分做密码初始化的方法。

图 8A 是 O/S 的 ROM 加载控制程序部分的一个流程图，示出按照本发明从密码单元将一个安全小程序卸载（换出）到 PC 的方法。

图 8B 是 O/S 的 ROM 加载控制程序部分的一个流程图，示出按照本发明将一个安全小程序从 PC 加载（换入）到密码单元的方法。

图 9A 是一个方块图，示出按照本发明将对应于一个安全小程序的密码内容解密并从 PC 硬盘劝器加载（换入）到密码单元 RAM 存储器。

图 9B 是一个方块图，示了按照本发明将对应于一个安全小程序的密码内容加密并从密码单元 RAM 存储器卸载（换出到）到 PC 硬盘驱动器。

实施发明的较佳方式

系统操作

示于图 1 的一个公共密码系统的广场图包括一个密码运行中心 OPC21，一个台式 PC22，一个软件开发者 PC10 和一个发行媒体 20。软件开发者使用软件开发工具包建立安全小程序 14。设计安全小程序 14 实现给定的安全功能，作为主软件应用程序 16 的部分。软件开发者通过某个发行媒体 20 发行包括该加密的 18 安全小程序 14 的软件应用程序。

为了解密该安全小程序 14，在 PC10 的软件开发者通过如电话线调制解调器那样的达到 OPC21 的安全通讯链路发出一个请求 15。请求 15 包括实际提出的安全小程序 14。响应该请求 15，在 OPC21 审查安全小程序 14 是否符合安全标准。例如，提出的安全小程序 14 不应试图访问和输出被禁用的密码，不应搅乱内部的消逝时间计数器（一个安全时钟）或在密码单元设置许可位（下面讨论）以便授予自己访问敏感区。如果提出的安全小程序 14 由于某种原因不满足安全标准，它将被拒绝登录。

另一方面，如果 OPC21 认可安全小程序 14 登录，OPC21 将选择一个单独的序列号（S/N）17 及一个任意的编码密钥 C19 与该小程序相关联。S/N17 和编码密钥 C19 从 OPC21 通过请求 15 使用的同样的安全电话线调制解调连结通讯到软件开发者 PC10。OPC21 在一个小程序登录处 23 维持一个发出的 S/N 和对应的发出的编码密钥 C 的数据库。此提出的小程序就被正式登录，并由 OPC21 授予许可，能由任何公共密码控制单元使用（即运行）。

在 PC12 的软件开发者在一个小程序编码器 18 中使用接收到的编码密钥 C 进行处理，加密认可的安全小程序 14。在 PC12 的软件开发者还接收 S/N 序列号，在编码器 18 中处理以识别被认可的安全小程序 14。完成的安全小程序（使用编码密钥 C19 另密并使用 S/N17 识别）替代软件应用程序 16，并通过如软盘、CDROM、全球广播、卫星、有线电视等那样的发行媒体发行到台式 PC22。

在软件应用程序 16 安装到台式 PC22 以后，加密的安全小程序存入硬盘驱动器 26。硬盘驱动器 26 通常保存有多个加密的安全小程序 28，30，32，它们对应于在台式 PC22 上使用的多个软件应用程序。每个储存的小程序 32 包含一个识别的 S/N，如 S/N32A。台式 PC22 还包括标准 PC 的部件，如调制解调器 24，CPU34，ROM36，时钟 38，RAM40 通过标准 PC 总线 25 连续的输入 / 输出。此外，台式 PC22 包括一个具有单独单元识别（UID）44A 的密码单元，它也耦合到总线 25。

在运行时，首先存在台式 PC22 的硬盘驱动器 26 上的软件应用程序 16 需要执行加密的小程序 32，然后台式 PC22 建立与 OPC21 的一个安全通讯会话。台式 PC22 需要从 OPC21 来的许可，来使用加密的小程序 32。为获得许可，密码单元 22 将它的 UID44A 和安全小程序 32 的 S/N32A 发送到 OPC21。

OPC21 使用以前提供的单独的 S/N17 在小程序登录处 23 查找对应的随意提供

的编码密钥 C。而且，OPC12 通过另到小程序登录处 23 而进入事务（由密码单元 44 使用 S/N32A）。小程序登录处 23 记录了所有登录的安全小程序 S/N，对应于每个 S/N 的编码密钥 C，和所有被授予许可运行每个对应的安全小程序的密码单元 UID。例如，登录处 23 示出，对应于密码密钥 C＝Z 的加密小程序 S/N32A 已被登录，且那于 UID＝44A 的密码单元已被授予许可来解密并执行（运行）带 S/N＝32A 的被登录的小程序。

公共密码控制单元

在图 2 中的公共密码控制单元包括微处理器 206，RAM 存储器 222，224 和 ROM 存储器 208。分配 RAM 存储器作为签名寄存器 224 和主密码程序控制 222 区的存储。RAM208 包含 O/S 的加载控制程序部分。包括在密码单元 44 的仍然是一个 DES 引擎 218，一个非易失性存储器 220，一个消逝时间（实时时间）计数器 204 和访问控制寄存器 212。对了在密码单元 44 和主 PC 机之间的通讯提供一个主（台式）PC 机接口 202。在密码单元内部的通讯是在密码单元 44 中部件之间通过地址和数据的通用数据总成 210 上提供的。

DES 引擎 218 方便了在密码单元 44 的保护环境中的密码操作。例如，内部的非易失性存储器 220 提供了密码密钥的安全存储。的时间计数器 204 使得在密码单元 44 的安全环境中保护时间和日期的计算不被扰乱。一些重要的操作，如读写消逝时间计数器 204，访问和改变在非易失存储器 220 中的密码存储的内容，访问和改变签名寄存器 224 的内容被硬件所限止。尤其是，访问密码单元由设置访问寄存器 212 的单独许可位 216（下面讨论）所控制。

访问寄存器212包括专门的保护特征以保护加载到程序控制RAM222的安全小程序损害密码单元 44 的安全特征。尤其是，访问寄存器 212 包括一个许可寄存器，而且访问寄存器212 的单独的许可位 216 确定了给定的安全小程序允许访问哪些资源。例如，硬件连接信号（许可控制）226 提供了硬线连结的限止，加载在 RAM222 中的给定的安全小程序是否允许访问所有签名寄存器 224，消逝时间计数器 204 和客户密钥及安全密码存储区 220 或其中一部分。秘密的客户密钥对每个密码单元是单独的，且在制造时与其他密码密钥一起存入非易失性存储器 220。

仅当从访问寄存器 212 授予许可时，在 RAM222 中给定的安全小程序才允许访问（读或写）重要的操作。许可寄存器从解密安全小程序由加载控制 ROM208 程序加载。作为防止非授权访问的进一步措施，许可寄存器 216 可以只由加载控制 ROM208 的指定执行来访问。一旦许可寄存器被写入新值，就执行地址控制 214。尤其是，只有当地址检测指示出加载控制 ROM 正执行许可位加载，从地址检测 214 的写使能信号才被激活。以这样的方式，许可寄存器 216 只能由加载控制 ROM208

的适当的指令序列加载。因此，在 RAM222 以外运行的安全小程序不能改变许可寄存器 216 的许可位。

访问寄存器的许可位

访问寄存器 212 的单独许可位 216 提供对消逝时间计数器 204 的控制。尤其是，一个许可位控制消逝时间计数器 204 是否可读，另一个许可位控制消逝时间计数器 204 是否可写。只有 OPC 通过自然形安全小程序得到许可（通过许可位的设置）将值写入消逝时间计数器。

访问寄存器 212 的单独许可位 216 提供对在非易失存储器 220 中的客户密钥和安全密钥存储的控制。尤其是，一个许可位确定该小程序是具有读（不是写）客户密钥的访问。在客户密钥是工厂安装的，不能改变。此客户密钥可由软件开发者用于与安全小程序相关的密码计算。

储存在非易失性存储器 220 的其他密钥包括对特定软件开发者的私人密钥。即，特定的软件开发者可以不用共享的客户密钥。相反，对那样的特定一个私人密钥。在那样的情况，对应于一个专门的私人密钥的许可位允许由特定的软件开发者的安全小程序访问专用的私人密码。由其他软件开发者的安全小程序将不对那个专用的私人密钥设置许可位，因而不具有访问此坟门的私人密钥的资格。此外，访问寄存器 212 的分别的许可位 216 确定该 安全小程序是否可以写入一个新的专门的私人密钥来覆盖在非易失性存储器 220 中老的专人仫人密钥。除了专门的私人密钥以外，非易失性存储器 220 可以存储用于鉴别一个公共私人密钥对的公共密码部分的数字检验证。

访问寄存器 212 的单独许可位 216 与 RAM 的签名登记部分 224 结合被用于提供有关哪个安全小程序可以加载到密码或从中卸载的访问控制尤其是，在签名登记的一个入口设置一个删除标记将删除此的安全小程序。其后密码片将不加载或卸载在签名登记中由删除标记指明的安全小程序。最后，OPC 可以通过设置抑制整个密码单元。被抑制的密码单元 44 的适当的许可位 216 来抑制整个密码单元. 被抑制的密码单元 44 不能运行任何安全小程序,除非该密码单元 44 被 OPC 重新激活。

安全小程序登录

如上指出的，出应用程序开发者将安全小程序作为主应用程序的一部分来设计。写此安全小程序专门在密码单元 44 上运行。安全小程序必须压缩到足以能存入密码单元的板上 RAM（图 2 中的 222）。大得不能存入板上 RAM 的安全应用程序可以分成两部分，即分成两个安全小程序。在安全小程序能与主应用程序一

起发行并在密码单元上运行以前，开发者必须用 OPC 登录此安全小程序。如上指出，开发者建立了与 OPC 的安全通讯会话。一个适合与 OPC 安全通讯的系统示于美国专利 5，615，264，5，761，283 和 5，764，762。

图 5 示出在 OPC 上开发者的登录过程。在步骤 5100PC 接收一个安全小程序登录的请求。此请求包括实际指出的安全小程序。在步骤 5120PC 审查提出的安全小程序是否符合适当的密码标准。例如，提出的安全小程序可以不试图揭示对每个独立的密码单元是单独的客户密钥或任何其他安全密钥。既不能输出密码，也不能输入附加的密码，象在变址程序循环中那样，间接程序跳转是一个安全的危险。通过系统的安全性受分割的经验，可以设计许多测试以保证所提出的安全小程序是安全且恰当地设计的。如果该提出的安全小程序不能通过任何一个测试，在步骤 5120，PC 拒绝登录该提出的安全小程序。

如果所有的测试通过，在步骤 5140PC 选择一个序列号 S/N 和一个编码密钥 C。在步骤 514，OPC 还将 S/N 和编码密钥 C 输入到一个小程序登录（图 1 中的 23）中。在步骤 516，通过将对新登录小程序的 S/N 和编码密钥 C 发送到软件开发者而完成了登录过程。

使用的密码惯例

图 3A，3B，9A 和 9B 示出用符号表示的密码操作。如在此使用的，对加密和解密的较佳过程是数据加密标准（DES）。

简而言之，对 DES 的电子码书方式（Ele-ctronic code book mode - ECB），一个 64 位（8 个字节）的输入块按照 56 位码被转换成一个 64 位的输出块。对解密，完成逆过程，将 64 位输入住使用同样的 54 位码转换成 64 位输出位。通常 DES 密码以 64 位，8 个字节表示，每字节具有 7 位另 1 个奇偶校验位，或 56 密码位加 8 个奇偶校验位。

如在这里使用的，借助一个秘密密钥对一个变量完成一个密码操作意味着使用一个秘密密钥产生另一个密钥来加密（或解密）该变量。加密可以在一个单个密钥或多个密钥，如三个密钥的组的基础上完成。除非特别指出，加密或解密意味着在三个密钥的组的基础上 DES 加密或解密的 ECB 方式，对于三个密钥的加密，使用三个密钥（密钥 1，密钥 2，密钥 3）的组如下采用 DES 另密一个变量：用密钥 1 加密，用密钥 2 解密，并用密钥 3 加密。三密钥的解密是个逆过程一用密钥 3 加密，用密钥 2 加密，再用密钥 1 解密。CBC 意义是使用初始向量 IV，DES 标准的密码块连续模式（Cipher block chaining mode）。除非另加说明，对一个 CBC DES 加密或解密的 IV 将是 0。

密码单元初始化及登录

图 7 示出通过 ROM 加载控制程序密码单元初始化和登录的方法。在上电时，ROM 另载控制程序（在图 2 的 ROM208 中）在步骤 710 将一个初始自然形式安全小程序从硬盘驱动器（图 1 中的 26）加载到板上的 RAM（图 2 中的 222）中。ROM 加载控制程序认为初始自然方式安全小程序是预先认可并用固定密钥加密的。初始自然形式安全小程序通过将访问寄存器 216 的所有许可位均置成使能被授予对整个密码单元的资源访问的权限。加载以后，密码单元的控制被转移到刚加载到板上 RAM 的初始自小程序。

如果这是首次使用密码单元，在步骤 712 开始一个登录过程。在步骤 714 建立个 OPC 的安全通讯会话，且密码单元与 OPC716 进入登录过程。登录包括输入识别用户的数据（名字、地址等）并将与密码的 UID 相关的用户数据转送到 OPC。在步骤 714 与 OPC 通讯会话的过程中，OPC716 有机会下载任何程序的改变来更新初始自然形式安全小程序。在登录过程结束后，程序控制返回到台式 PC。然后，密码单元进入等待状态，直到台式 PC 准备好加载拟在密码单元运行的第一个安全小程序。

登录的安全小程序的加密

安全小程序要加密，图 3A 是用于安全小程序加密的加密密钥组的流程图。软件开发者从所希望的安全小程序 322 开始。如上指出，安全小程序 322 先前已被软件开发者发送到 OPC，且小程序的 S/N320 和编码密钥 C318 先前已作为小程序登录过程的部分被接收。

软件开发者选择了一个在步骤 302 自己挑选的编码密钥 A（编程者密钥）。然后，密码密钥 A 在加密器 304 中借助编码密钥 C 加密，形成加密的编码密钥 A’。安全小程序 322 是在加密器 324 中在编码密钥 A 下用了密码 CBC 加密。在加密器 326 中计算一个消息鉴别码（message authentication code - MAC）。MAC（也称为操纵检测码）是在加密的包后面的数字签名，它由该加密包的接收者检查，以难加密包的内容未被修改。在步骤 306，MAC 通过将 S/N320，编码密钥 A’ 和从加密器 324 的输入来的加密安全小程序组合到一个安全包中而产生的。

组合一个安全包 306 的目的是在加密器 326 中产生 MAC316，并将其在安全包的后面形成一个安全页。开发者的 MAC 密码是在加密器 328 中借助编码密钥 C318 由加密 S/N320 而形成。MAC 签名本身通过在安全包 306 上用三密钥 CBC 加密 326 而产生。尤其是加密器 326 的输出的最后部分形成 MAC 签名 316，它在安全包 306 之后。

计算的 MAC 与安全包结合形成一个安全页 306，它从密码单元输出，并最终

存入主 PC 机的硬盘驱动器。

为将加密的安全小程序存入 PC 的硬盘驱存储动器，安全存储页的格式示于图 4 中。安全存储页从安全包（S/N310 后面是编码密钥 A’ 312，再后面是加密的安全小程序 314）开始，由计算 MAC 结尾。

安全小程序的初始加载的解密

密码单元一个开始遇到的加密安全小程序，如在图 3B 的加密密钥组流程图所示。因为这是一个以前尚未运行的安全小程序的初始加载，在 RAM224 的小程序签名登录部分找不到 S/N310（在签名登录 224 中找到 S/N 的情况该加密的小程序以前已被运行，可应用图 9A）。如上面指出，对一个开始遇到的安全小程序，自然形式的安全小程序将 S/N338 发送到 OPC，并从 OPC 接收编码密钥 C336。

首先，在解密器 330 中借助密码密钥 C336 通过解密编码密钥 A’ 312 恢复软件开发者的编码密钥。加密的安全小程序 314 是在解码器 332 中借助从解码器 330 的输出得到的恢复的编码密钥 A 被三密钥 CBC 解码的。对安全包（S/N310，编码密钥 A’ 312 和加密的安全小程序 314）的 MAC 是借助开发者的 MAC 密钥在三密钥 CBC 加密器 340 中被计算。开发者的 MAC 密钥借助于在加密器 348 的编码密钥 C336 通过加密 S/N338 计算的，336 被耦合到加密器 340 的密码输入。

在加密器 340 的输出处的计算的 MAC 在比较器 342 中与接收到的 MAC316 比较。如果计算的 MAC 和接收的 MAC 相当等 334，则与（AND）门 334 使能，且在解码器 332 的输出处的解密的安全小程序被存入板上 RAM 的密码控制部分 222。但是，如果计算的 MAC 和接收的 MAC 不等 346，则该安全小程序不允许加载到板上 RAM222 上，且不允许运行。相反，与门 332 不使能，而且在解密器 332 输出处的解密的安全小程序不被存入板上 RAM 的密码控制部分 222。一个错误消息返回到台式 PC。

在安全小程序加载时的 OPC 控制

本系统给出不管安全小程序能否加载到给定的密码单元时的 OPC 控制。图 6 示出在 OPC 的初始加载控制过程。在步骤 610 从 OPC 处的台式 PC 接收 S/N 以后，OPC 在步骤 612 检查，该小否具有合法的 S/N。如果没有，OPC 返回一个错误消息，请安全小程序是“不合法（INVALID）的”。在步骤 614，OPC 检查，如果 S/N 碑是合法的，是否已被删除。如果确实如此，OPC 返回一个错误消息，该安全小程序已被“删除（CANCELLED）”。在步骤 6160PC 检查，由其 UID 识别的给定的密码单元是否允许加载此特定的安全小程序。 是，OPC 返回一个错误消息，该安全小程序的加载是“不允许（DISALLOWED）”。如果 S/N 是合法的，未被删除，且密码单元允许加载此安全小程序，则在步骤 618 在 OPC 处的小程序登录中查找编

码密钥 C，并发送到密码单元。

以这样的方式，在初始安全小程序安装过程中 OPC 维持控制。例如，如果一个安全小程序已被改写以修正一个问题，OPC 将不允许以后的用户将早期的版本安装到密码单元。如果一个给定的密码单元已知被泄密了，对此密码单元 UID 不再允许安全小程序的加载。

ROM 加载控制 O/S－密码内容的交换

密码单元的 ROM 加载控制程序（O/S）支持多个同时的用户。为了在用户之间切换，当前安全小程序的密码内容从密码单元卸载，并存入台式 PC 的硬盘驱动器。然后通过从台式 PC 的硬盘驱动器提取以前运行的安全小程序的以前存入的密码内容，此密码被恢复到对应于那个以前运行的安全小程序的以前的密码状态。如果这里使用，术语“加密的安全小程序”，“密码内容”和“在其密码内容中（带有或包括）的加密的安全小程序”都认为是基本上等价的术语。

在本实施例中，软件开发者配置该安全小程序在该程序存在以前将密码参数存入板上 RAM 的密码程序控制部分 222。软件开发者期望那个安全为其安全应用程序所需，并需要将密码单元恢复到它的以前密码状态，并继续此安全应用程序。

在某些安全应用程序中，需要密码单元的所有密码参数来恢复该密码单元。在另外一些安全应用程序中，只需密码的一个子集。在又一个实施便中，密码单元自动地将它本身（密码单元）的整个密码状态存入与每个安全小程序有关的一个单独的文件。在后面的情况，切换密码状态（存储和恢复密码状态）的重担自动地由密码单元的操作完成而不必要开发者的软件干预。

在本实施例中，对每个给定的安全小程序的密码内容文件程序加上密码单元的密码状态。下面给出密码内容的格式：

表 I－密码内容（29K）

明文表头 序列号（S/N），大小 修订版本号，时间标记
程序数据－安全小程序
永久性寄存器存储
堆（暂时存储）
堆栈
MAC / 签名

除了明文表头外，密码内容是加密的。明文表头由下列字段组成：

序号号（S/N）：S/N 是在登录过程中为该安全小程序颁发给软件开发者的初

始序列号。

大小：对应于从密码单元卸载并存入硬盘驱动器的密码内容的字节数。

修订版本号：用于跟踪对初始登录的安全小程序的变化。

时间标记：对应于在卸载时间密码单元实时时钟的内容。

密码内容的另密部分由下列字段组成：

程序数据：包括任何在程序执行过程中作的修改的安全小程序。

堆（暂时存储）：表示在卸载以前密码的密码状态的参数。

堆栈：程序的堆栈存储，如对嵌套子程序的返回地址。

MAC / 签名：对整个密码内容计算的 MAC。

表 II－签名登录

板上 RAM 的签名登录 224 具有下述格式：

序列号（S/N）	MAC（签名）	标志
S/N 1	MAC 1	标志 1
S/N 2	MAC 2	标志 2
---	---	---
S/N 31	MAC 31	标志 3

S/N：小程序的序列号。

MAC：对储存在 PC 硬盘驱动器的小程序的密码内容的消息鉴别码。

标志：储存在签名登录中的标志包括一个小程序删除标志，它由 OPC 设置以防止被删除的小程序又一次的使用。

图 8A 的 ROM 加载控制 O/S－换出

在图 8A 中示出 ROM 加载控制程序（O/S）的换出部分的流程图。操作系统的换出部分的功能是卸载当前在密码单元运行的安全小程序到台式 PC 的硬盘驱动器，小程序包括其密码内容。例如，安全小程序可以具有内部寄存器存储，堆栈指针和其它程序，它们在执行时被修改，并组成它的密码内容的部分。

在图 8A 中，在步骤 810 若当前的安全小程序已经完成，在步骤 812 将密码单元的密码状态保存在板上 RAM 中。储存的密码状态包括 DES 引擎（图 2 中的 218）的状态和将密码恢复到它当前状态所需要的任何其他变量。然后，在步骤 814RAM 的内容（按照在图 9B 中示出的加密密码组）被加密。在步骤 816 对包括明文表头和 S/N 的加密 RAM 内容计算 MAC，且在步骤 818 将此 MAC 存入（或更新）RAM 签名登录 224。在步骤 820 组成安全页并在步骤 882 存在如式 PC 的硬盘驱动器。

图 8BROM 加载控制 O/S 0 换入

在图 8B 中示出 ROM 加载控制部分（O/S）的换入部分的流程图。操作系统的这部分的功能是将下一个安全小程序加载到板上 RAM 以便在密码单元运行，包括从台式 PC 的硬盘器恢复可能有的相应的以前的密码内容。

在图 8B 中，到了加载一个安全小程序到板上 RAM 的时信，ROM 另载控制程序首先在步骤 830 检查，S/N 是否在 RAM 的签名登录部分（图 2 中的 224）。S/N 是否在签名登录 224 决定了此密码单元以前是否运行过此特定的安全小程序。

如果该小程序的 S/N 未在登录处，密码单元未曾运行过此特定的安全小程序。然后程序在步骤 834 检查，以确定签名登录是否已满或者还有空间用于另外的存入内容。如果签名登录已满，返回一个错误消息“登录已满－REGISTRY FULL”。如果签名登录未满，ROM 加载控制程序在步骤 838 换入自然上程序，如上按照图 6 所述，它建立了一个与 OPC 的通讯。

如上结合图 6 指出，在步骤 838 自然形式安全小程序将提出的安全小程序的 S/N 送到 OPC，并在步骤 839 获得编码密钥 C。在上面还提出，密码单元使用接收的编码密钥 C 在步骤 837 提出的安全小程序并计算对该安全小程序的 MAC。对加载到给定的密码单元的安全小程序的解密密钥首先结合图 3B 在上面叙述。

如果密码单元以前已经运行过此特定的安全小程序，则在步骤 830 将在登录中找到此 S/N。在此情况，在步骤 832 从 RAM 的签名登录部分（图 2 中 224）取出 MAC。在步骤 836 解密此安全小程序（用其密码内容）并计算 MAC。用于解密存储的小程序并计算 MAC 的密钥组在下面结合图 9 描述。

在换入过程的这个阶段，有 3 个与该安全小程序相关的 MAC（带有它的密码内容），ROM 加载控制程序（O/S）试图将其加载到密码单元的板上 RAM。第一个 MAC 从签名登录取出，第二个 MAC 与储存的密码内容一起从台式 PC 接收到，第三个 MAC 根据输入的解密的小程序计算。如果在步骤 840 判断 3 个 MAC 互相相等，则解密的安全小程序被加载到 RAM 的密码程序控制部分，且在步骤 842 开始执行该安全小程序。否则，从步骤 840 返回给 PC 一个错误消息“访问被拒绝－ACCESS DENIDE”。

密码内容文件

图 9A（换入）和图 9B（换出）示出为了安全小程序（在对应的密码内容中）在 RAM222 的密码程序控制部分和台式 PC 的硬盘之间交换的相应的解密和加密密钥组。尤其是，图 9A 是一方块图，示出用于将对应于一个安全小程序的密码内容解密并从 PC 硬盘驱动器加载（换入）到密码单元 RAM 存储器的方法和装置。图 9B 是一个广场图，示出用于将对应于一个安全小程序的密码内容加密并从密码单元 RAM 存储器卸载（换出）到 PC 的硬盘驱动器的方法及装置。

密码内容换出－图 9B

在图 9B 中，RAM222 的密码程序控制部分的内容作为加密的文件 962A 被卸载到硬盘驱动器 26 中。RAM 存储器的签名登录部分未被卸载。所产生的各种加密密钥是基于第一个固定的字符串 A940，第二个固定的字符串 B956 和一个称为客户密钥 942 的秘密密钥。 客户密钥 942 被存入可编程存储器（图 2 中的 220）。客户密钥存储器通常是非易失的，可以由任何适合的非易失存储器实现，如可熔断的连结。EEPROM，电池供电的 RAM 等。对每个密码单元所存储的客户密钥 942 是唯一的，且在制造时安装。

第一个固定字符串 A940 是在加密器 944 中借助客户密钥加密的。加密器 944 的输出用作加密器 946 的密钥，加密将被卸载的小程序的 S/N（明文）。加密器 946 的输出用作为密钥在 3 密钥 CBC 加密器 948 中加密此安全小程序。注意，对换出的安全小程序的加密密钥（到加密器 948）与该安全小程序初始加载使用的不是同一密钥。对于安全小程序的初始加载，使用的密钥是开发者的编码密钥 A。在图 9B 中用于卸载的密钥是固定字符串 A940，S/N 和客户密钥 942 的函数。因为每个客户官衔每个密码单元是单独的，存在硬盘驱动器 26 的换出密码内容不能换回到另一个密码单元。即，一旦一个安全包使用一个客户密钥被换出密码单元到硬盘驱动器，换出的安全小程序（在其密码内容中）不能加载到具有不同客户密钥的不同的密码单元。

为了对密码内容（包括安全小程序）产生一个 MAC，组合一个安全包 950。安全包 950 包括明文的 S/N 和加密的安全小程序（带着它的密码内容）。MAC 通过借助由加密器 954 的输出导出的密钥的 3 密钥 CBC。加密安全包而产生。如从图 9B 所见，从加密器 954 输出的 MAC 密钥是固定字符串 B956，（通过加密器 944 和 946），S/N，客户密钥 942 和固定字符串 A940 的函数。

尤其是，加密器 946 的输出作为加密密钥是到加密器 954 的输入，后者加密固定字符串 B 成为到了密钥 CBC 回避顺 952 的 MAC 密钥。在加密器 952 的输出端的 MAC 与安全包组合形成一个安全页 958。安全页 958 是与另外的密码内容 962N 以及换出的自然形式小程序 960 一起存在硬盘中的 962A。

密码内容换入－图 9A

当密码单元在多个同时的安全应用程序之间切换时，在图 9A 中以前存入的密码内容 912，918A - 918N 从硬盘驱动器 26 加载到板上 RAM 的密码程序控制部分 222。密码单元使用签名登录的内容来确定每个以前储存的密码内容 912，918A - 918N 是否允许加载和运行。在密码内容 912 中的自然形式安全小程序与其他由密

码单元运行的多个同时的安全的小程序 918A - 918N 以同样的方式换入或换出密码单元。

图 9A 中的密钥组（换入）完成在图 9B（换出）中密钥组的逆向密码过程。尤其是，固定字符串 A910 在加密器 916 中借助于客户密钥被加密。加密器 916 的输出被用作加密器 920 中的密码来加密将被加载的安全小程序的 S/N 和密码内容 918A。加密器 920 的输出被用作小程序的解密密码，未在 3 密钥 CBC 解密器 922 中解密安全小程序密码内容。对安全小程序换入的小程序解密密钥（到解密器 922）是在换出过程中用来加密安全小程序的同一个密钥。

对密码内容 918A 的 MAC 密钥是通过在加密器 932 中借助于小程序解密密钥（加密器 920 的输出）的第一个加密固定字符串 B930 计算的。然后加密器 932 的输出被用作在加密器 926 的密钥，以形成有关密码内容 918A 的安全页部分的计算的 MAC，为检查此 MAC，从 RAM 的签名登录部分 224 取出储存的 MAC。然后在比较器 928 中比较从加密器 926 输出计算的 MAC，从签名登录 224 储存的 MAC 以及从密码内容 918A 接收的 MAC 等 3 个 MAC，在步骤 934 如果 3 个 MAC 相等，则与（AND）门 924 使能，将接收到的安全小程序加载到 RAM 的密码程序控制部分 222。若在步骤 936，3 个 MAC 中任何一个与另一个不等，则与门 924 不使能，不能将接收到的安全小程序加载到 RAM 的密码程序控制部分 222。

安全小程序交换

安全小程序可以通过一步过程或二步过程换入到密码单元。二步过程已在上面描述。即，在将加密的安全小程序加载到板上 RAM 的密码程序控制部分以前，ROM 加载控制程序对其审查。在二步实现过程中，如果所有 MAC 答名测试通过，该安全小程序然后在第二步被解密并加载到板上 RAM。如果在第一步不允许加载，在第二步没有任何安全小程序的部分被加载到板上的 RAM。

在一步实施过程中，ROM 加载控制程序审查一个加密的安全小程序，同时解密并将解密的安全小程序加载到板上 RAM 的密码程序控制部分。如果 MAC 签名测试失败（在图 8B 中步骤 840），密码单元的控制不转移到刚加载的安全小程序。而是，下一个安全小程序或自然形式安全小程序被加载到 RAM 的该密码程序控制部分，履盖以前加载的未允许的安全小程序。但是，如果 MAC 签名被通过，则 ROM 加载 密码单元的以刚加载的安全小程序。

二步实施例通常更安全，因为在所有 MAC 签名的测试完成以前没有任何部分的新安全小程序被加载到 RAM222 的密码程序控制部分，一步实施时通常导致更快的安全小程序交换，因为新的安全小程序在板上 RAM 开始执行而不必等待第二步。

由 OPC 监控密码单元

在图 1 中的密码单元 44 由 OPC21 周期地览监控。即，至少每月一次或隔选定的时间间隔一次密码单元 44 发起一次与 OPC21 的通信佳话。通信可以通过调制解调器 24 到拔号连结。或通过 TCP/IP 协议通过因特网连接。在两者情况，密码单元 44 的状态被报告到 OPC21。周期通信的目的是将密码单元 44 的内容与在 OPC21 所期望的内容相同步。

例如，在与 OPC21 周期通讯期间，消逝时间计数器 204（图 2）与它期望的值校验。若需要使其同步。消逝时间的较大差异可能是是搅乱的指示，并可能导致由 OPC 抑制密码单元。在访问寄存器 2120PC 可以设置一个或多个许可位 216，来抑制密码单元。一般被抑制，抑制制的密码单元可以不加载或运行任何的安全小程序。

而且在与 OPC21 周期性通讯期间，签名登录（图 2 中 224）被检查以回顾哪个安全小程序已被加载到该密码单元并在其中运行。如果一个安全小程序已被删除（即，运行那个安全小程序的系统的广泛的许可已被撤消），将在答名登录中设置对应于那个安全小程序的删除标志，与许可控制（图 2 中 226）相结合，密码单元 44 将不换入（加载）该被删除的安全小程序。

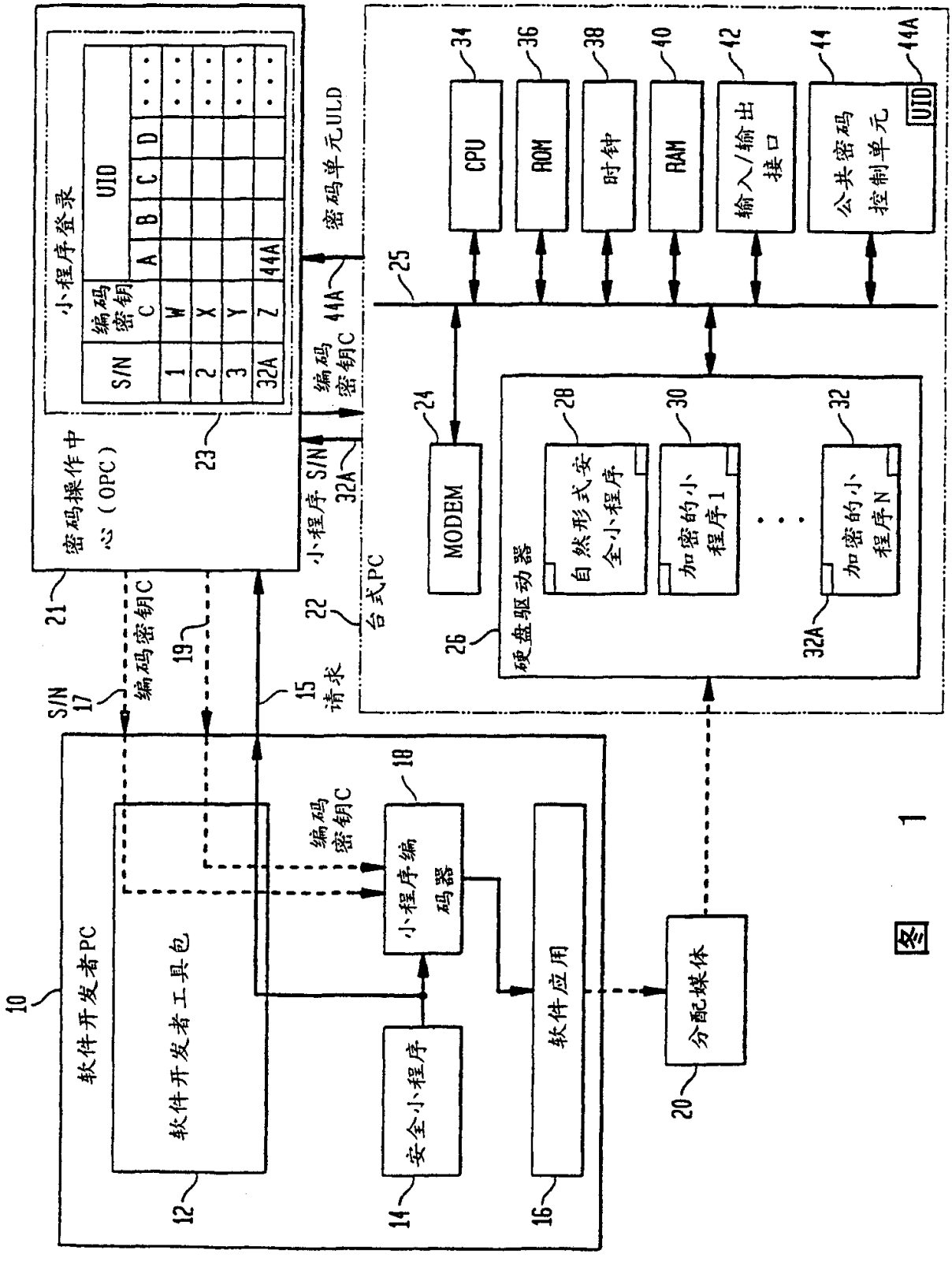

10
软件开发者PC
12
软件开发者工具包
14
安全小程序
16
软件应用
18
小程序编码器
20
分配媒体
21
密码操作中心（OPC）
S/N
编码密钥C
小程序登录
UID
A
B
C
D
1
2
3
32A
W
X
Y
Z
44A
23
密码单元ULD
44A
编码密钥C
小程序 S/N
32A
22
台式PC
24
MODEM
25
CPU
ROM
时钟
RAM
输入/输出接口
公共密码控制单元
UID
34
36
38
40
42
44
44A
硬盘驱动器
26
自然形式安全小程序
加密的小程序1
加密的小程序N
28
30
32
32A
15
请求
19
编码密钥C
17
S/N

图 1

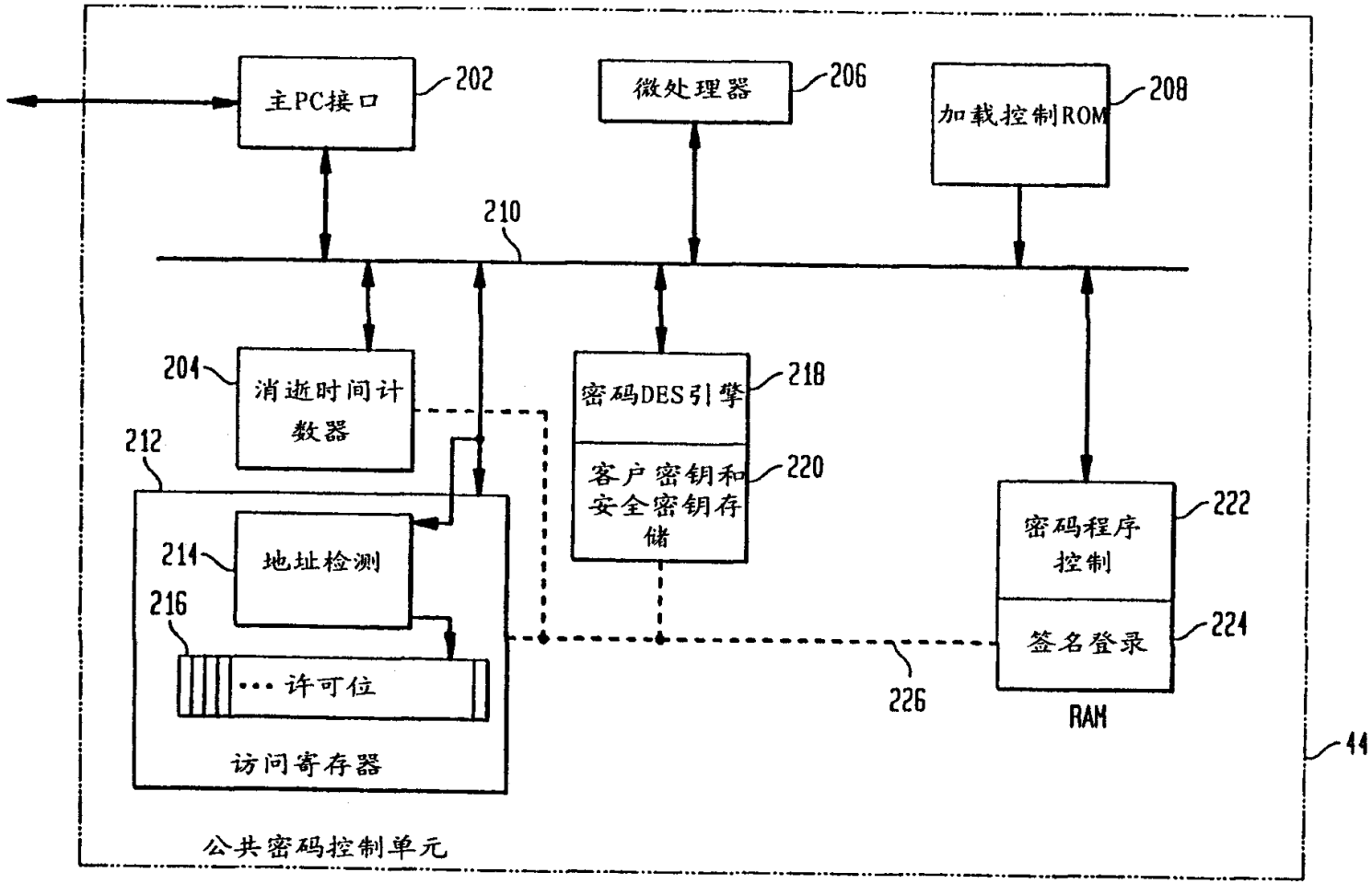

主PC接口
202
微处理器
206
加载控制ROM
208
210
204
消逝时间计数器
212
密码DES引擎
218
客户密钥和安全密钥存储
220
密码程序控制
222
214
地址检测
216
··· 许可位
访问寄存器
签名登录
224
226
RAM
44
公共密码控制单元

图 2

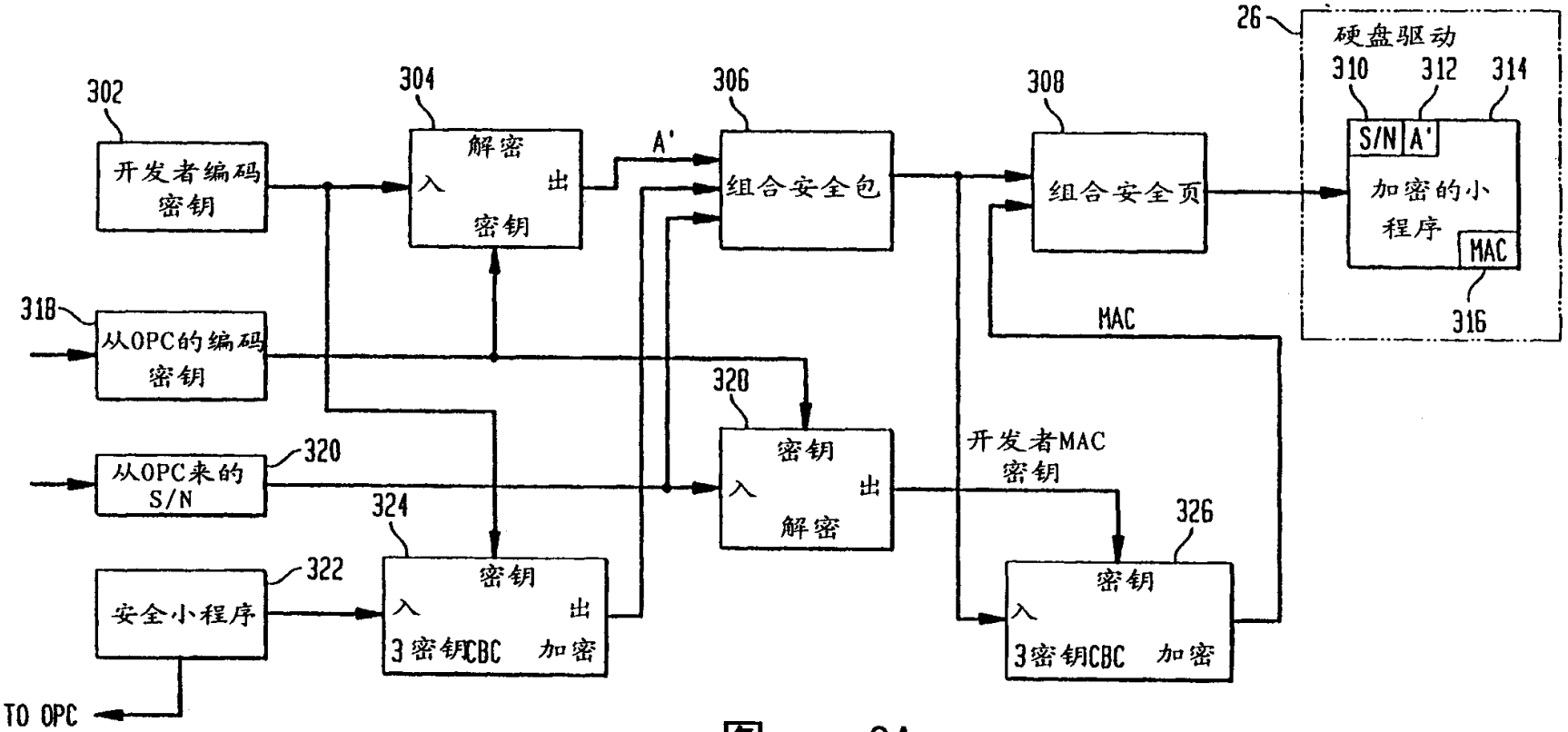

26
硬盘驱动
310
312
314
S/N
A'
加密的小程序
MAC
316
302
开发者编码密钥
304
解密
入
出
密钥
A'
306
组合安全包
308
组合安全页
MAC
318
从OPC的编码密钥
320
从OPC来的S/N
328
密钥
入
出
解密
开发者MAC密钥
324
密钥
入
出
3密钥CBC
加密
322
安全小程序
326
密钥
入
3密钥CBC
加密
TO OPC

图 3A

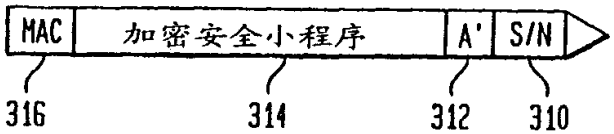

MAC
加密安全小程序
A'
S/N
316
314
312
310

图 4

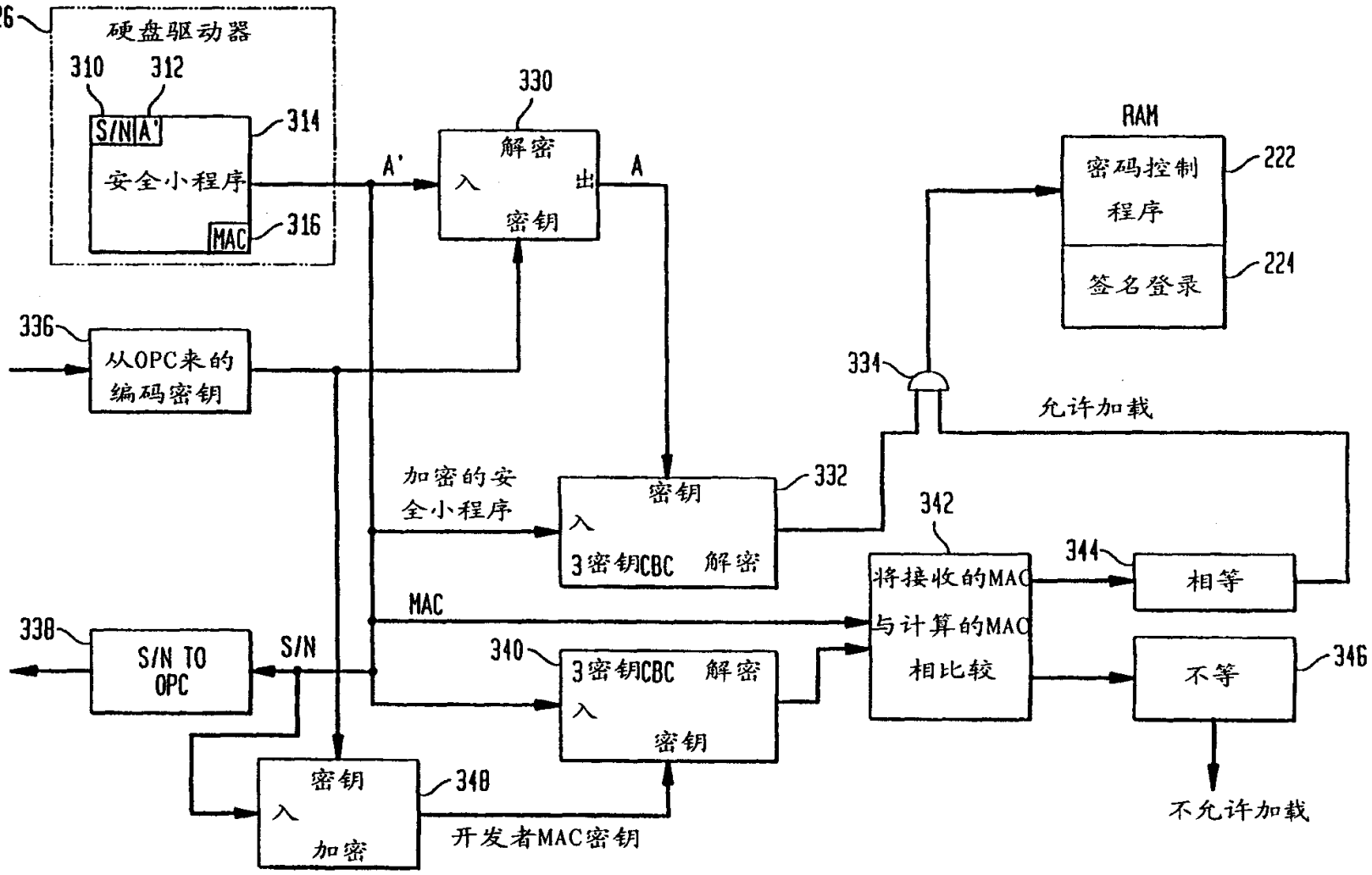

26
硬盘驱动器
310
312
S/N
A'
314
安全小程序
MAC
316
330
解密
入
出
密钥
A'
A
RAM
密码控制
程序
222
签名登录
224
336
从OPC来的
编码密钥
334
允许加载
加密的安
全小程序
密钥
入
3密钥CBC 解密
332
342
344
将接收的MAC
与计算的MAC
相比较
相等
MAC
338
S/N TO
OPC
S/N
340
3密钥CBC 解密
入
密钥
不等
346
密钥
入
加密
348
开发者MAC密钥
不允许加载

图 3B

当OPC处安全小程序的开发者登录

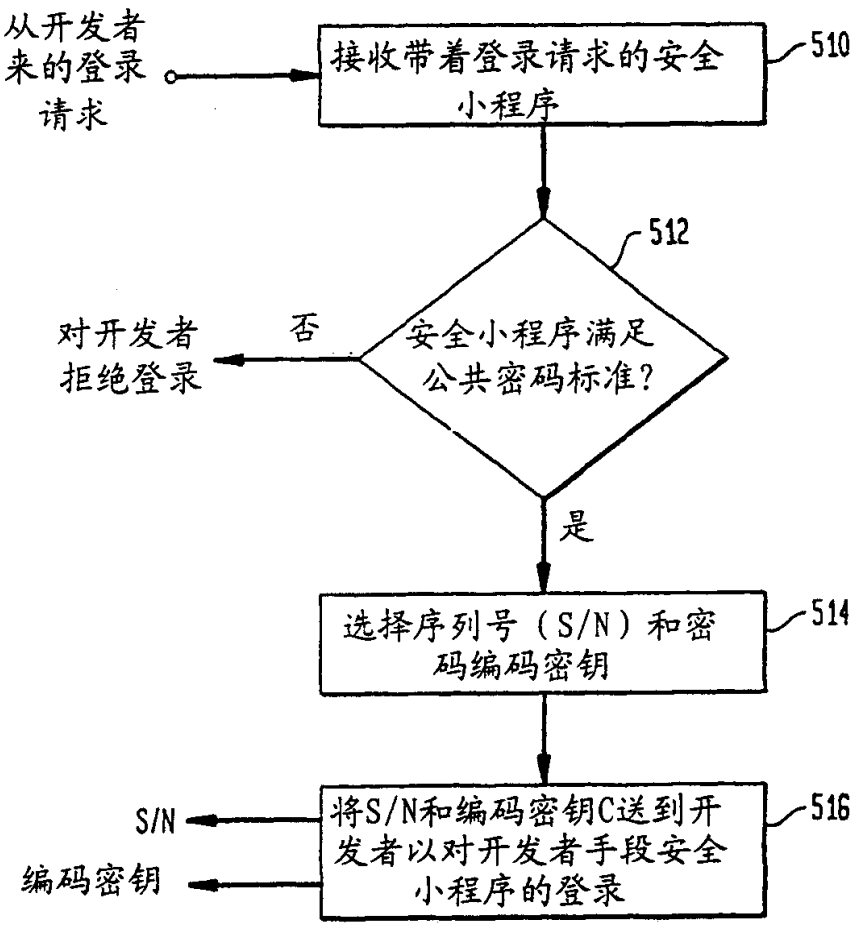


图 5

台式PC初始化在OPC
的安全小程序

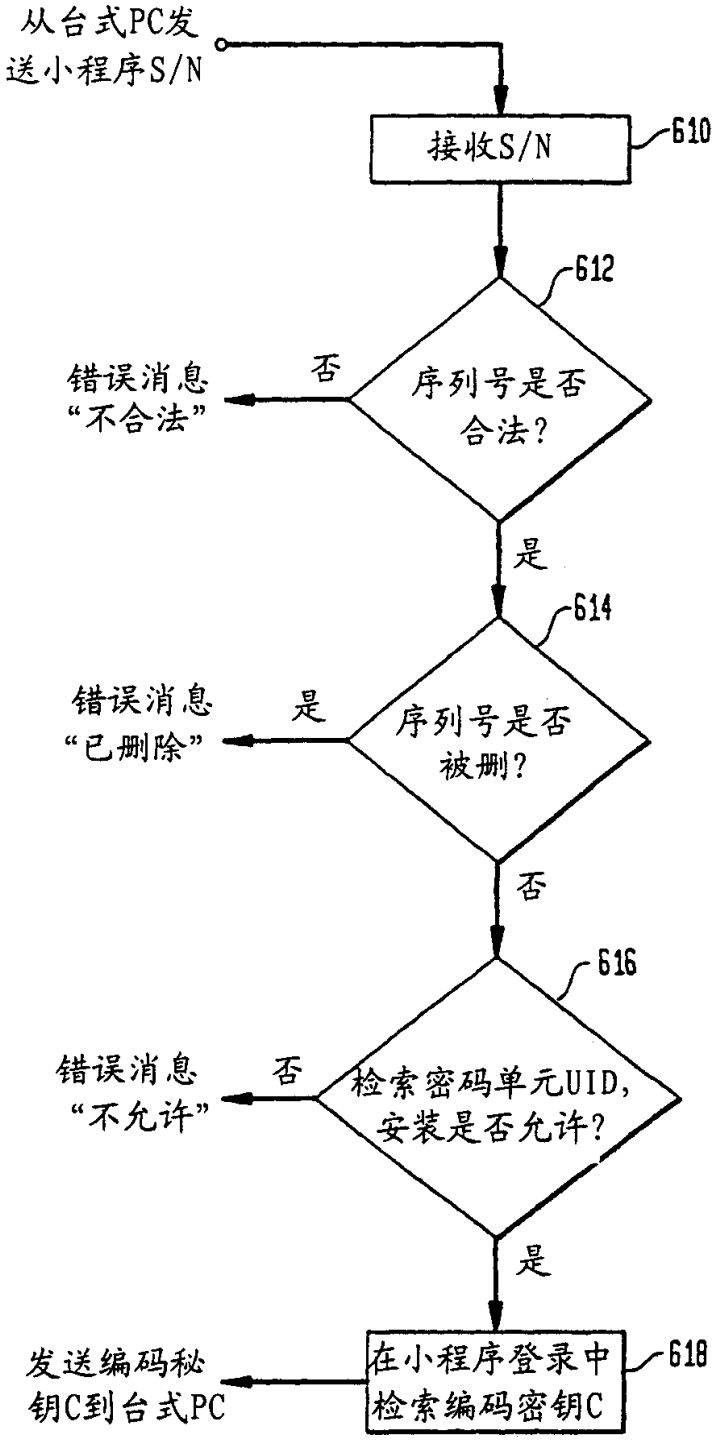


图 6

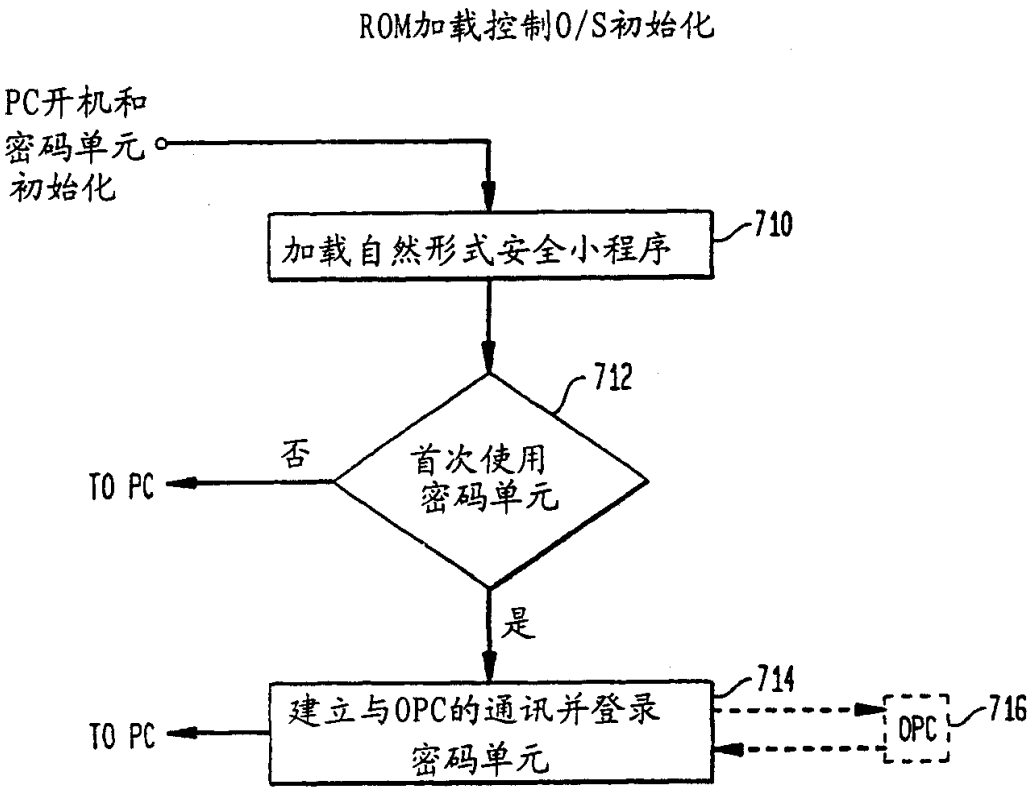

ROM加载控制O/S初始化
PC开机和
密码单元
初始化
加载自然形式安全小程序
710
712
首次使用
密码单元
否
TO PC
是
714
建立与OPC的通讯并登录
密码单元
TO PC
OPC
716

图 7

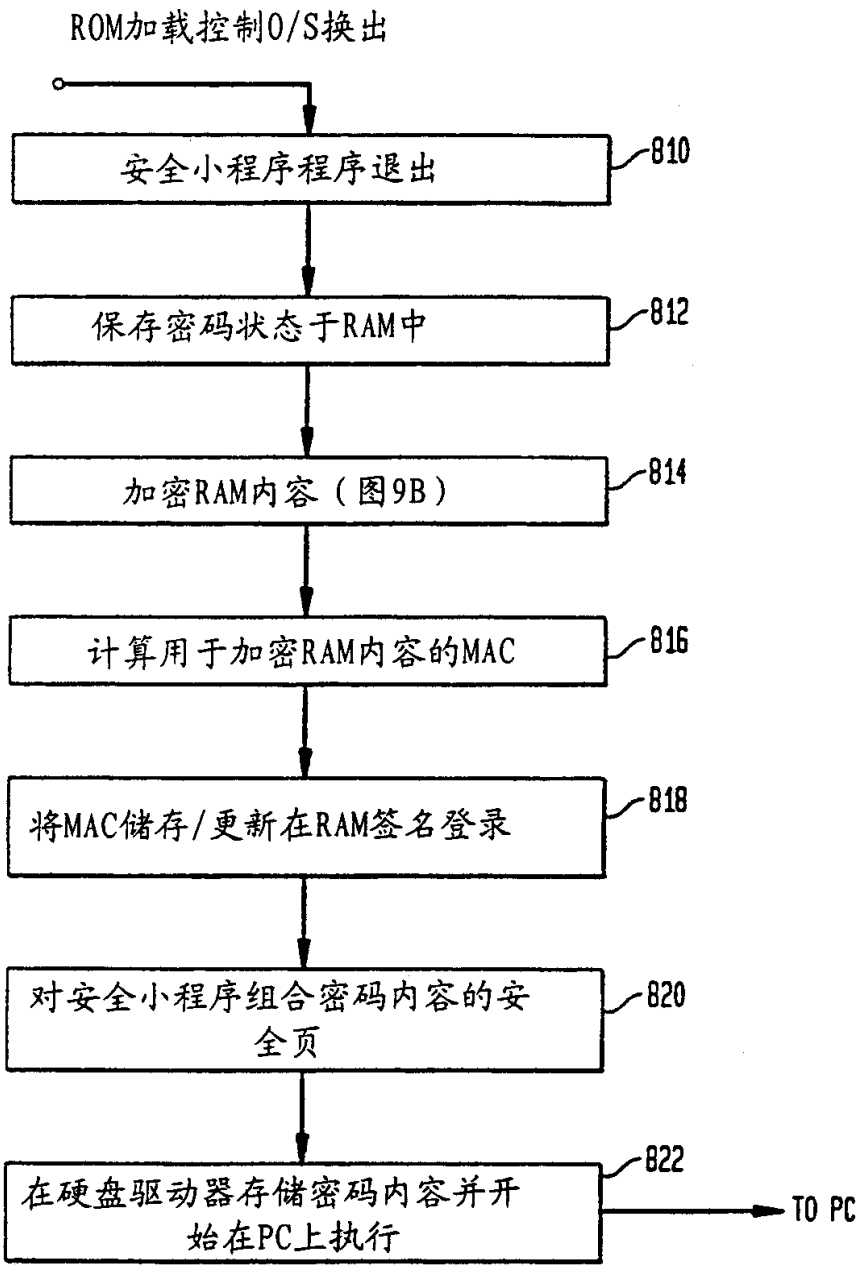

ROM加载控制O/S换出
安全小程序程序退出
810
保存密码状态于RAM中
812
加密RAM内容（图9B）
814
计算用于加密RAM内容的MAC
816
将MAC储存/更新在RAM签名登录
818
对安全小程序组合密码内容的安全页
820
在硬盘驱动器存储密码内容并开始在PC上执行
822
TO PC

图 8A

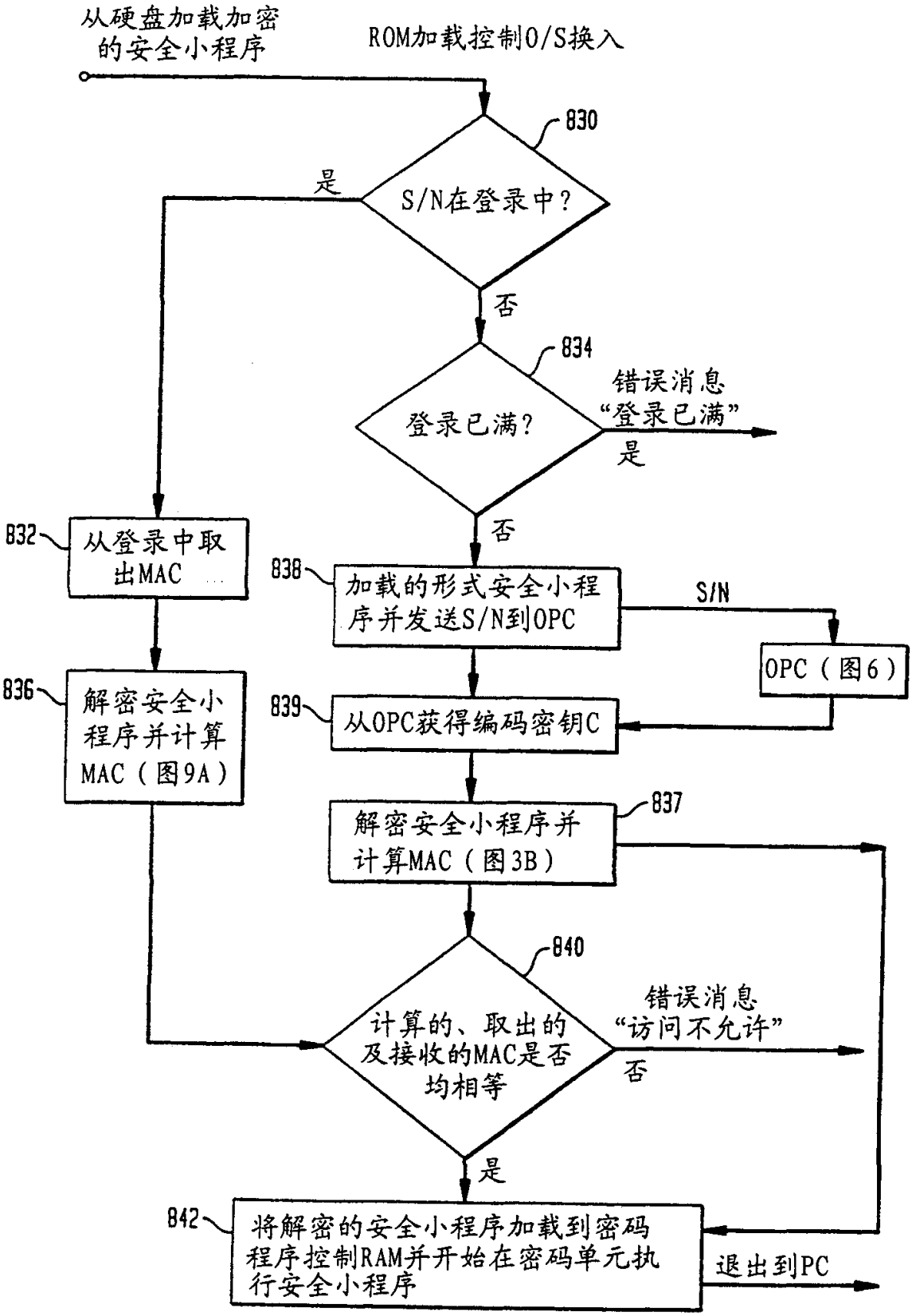

从硬盘加载加密的安全小程序
ROM加载控制O/S换入
830
S/N在登录中？
是
否
834
登录已满？
错误消息“登录已满”
是
否
832
从登录中取出MAC
838
加载的形式安全小程序并发送S/N到OPC
S/N
OPC（图6）
836
解密安全小程序并计算MAC（图9A）
839
从OPC获得编码密钥C
837
解密安全小程序并计算MAC（图3B）
840
计算的、取出的及接收的MAC是否均相等
错误消息“访问不允许”
否
是
842
将解密的安全小程序加载到密码程序控制RAM并开始在密码单元执行安全小程序
退出到PC

图 8B

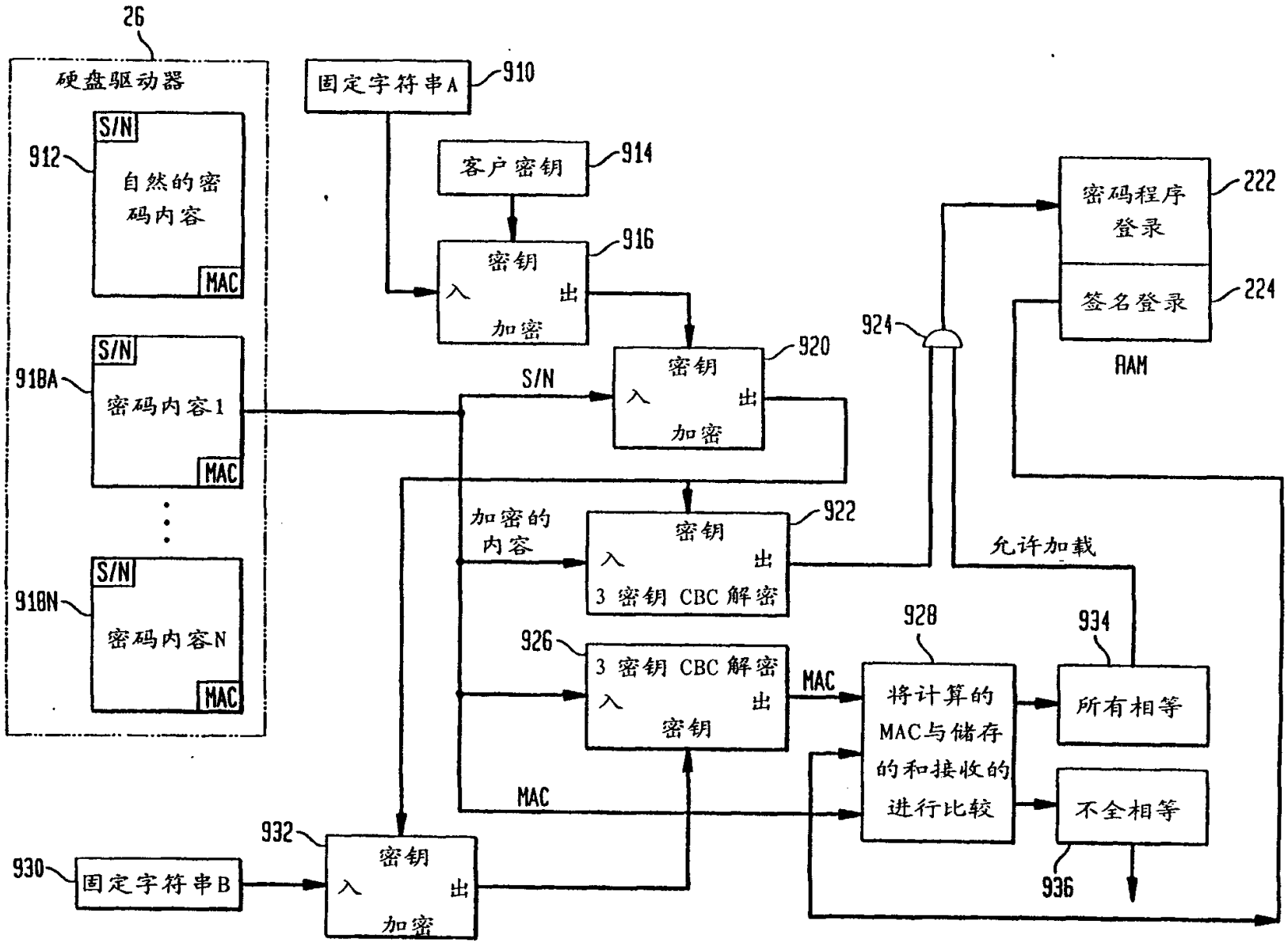

26
硬盘驱动器
S/N
912
自然的密码内容
MAC
S/N
918A
密码内容1
MAC
S/N
918N
密码内容N
MAC
固定字符串A
910
客户密钥
914
密钥
入
出
加密
916
密钥
入
出
加密
920
S/N
加密的内容
密钥
入
出
3 密钥 CBC 解密
922
密码程序登录
222
签名登录
224
RAM
924
允许加载
926
3 密钥 CBC 解密
入
出
密钥
MAC
928
将计算的MAC与储存的和接收的进行比较
934
所有相等
不全相等
936
MAC
932
密钥
入
出
加密
930
固定字符串B

图 9A

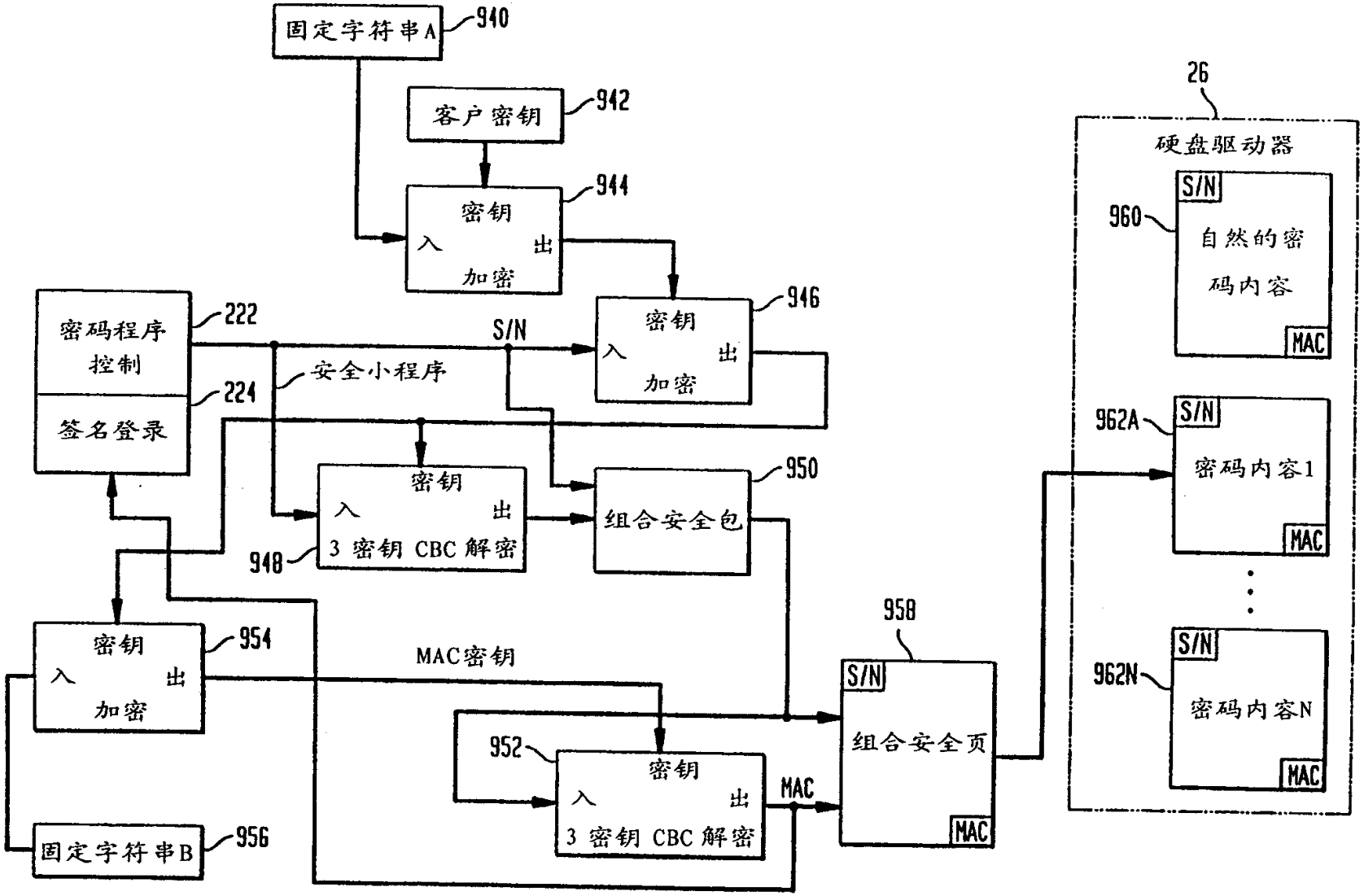

固定字符串A
940
客户密钥
942
密钥
入
出
加密
944
密码程序
控制
222
签名登录
224
S/N
安全小程序
密钥
入
出
加密
946
密钥
入
出
3 密钥 CBC 解密
948
组合安全包
950
密钥
入
出
加密
954
MAC密钥
固定字符串B
956
952
密钥
入
出
3 密钥 CBC 解密
MAC
958
S/N
组合安全页
MAC
26
硬盘驱动器
960
S/N
自然的密
码内容
MAC
962A
S/N
密码内容1
MAC
962N
S/N
密码内容N
MAC

图 9B