[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 98811411.9

[43]公开日 2001年7月11日

[11]公开号 CN 1303553A

[22]申请日 1998.6.24 [21]申请号 98811411.9

[30]优先权

[32]1997.9.30 [33]US [31]08/938,491

[86]国际申请 PCT/US98/13096 1998.6.24

[87]国际公布 WO99/17495 英 1999.4.8

[85]进入国家阶段日期 2000.5.22

[71]申请人 英特尔公司

地址 美国加利福尼亚州

[72]发明人 D·L·达维斯

[74]专利代理机构 中国专利代理(香港)有限公司

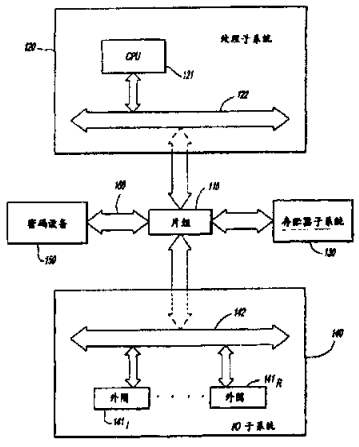
代理人 栾本生 张志醒

权利要求书3页 说明书5页 附图页数4页

[54]发明名称 配置与登记密码设备的电路和方法

[57]摘要

一种用于配置和登记密码设备(150)的系统和方法，配置状态包含将设备编号(DSER)和对称钥匙(SK)加载到密码设备(150)的非挥发性存贮器(215)中。非挥发性存贮器(215)被集成在密码设备(150)的处理逻辑内。DSER由外部源提供而SK在密码设备(150)内生成，登记状态包含提供DSER给数据库(415,420)，其中包含与每台所制造的密码设备(150)有关的密码信息。密码信息包括至少一个公共钥匙和一个用SK加密的私人钥匙。DSER用于安置相应的密码信息，以便将密码信息发送到具有密码设备(150)的一个电子系统。



ISSN1008-4274

权　利　要　求　书

1. 一种用于配置密码设备的方法包括以下步骤:

将设备串号加载到密码设备的非挥发性存贮器中;

在密码设备内生成对称钥匙; 和

将对称钥匙加载到密码设备的非挥发性存贮器中。

2. 如权利要求 1 的方法还包括以下步骤:

在设备串号和对称钥匙已被加载以后，在密码设备的非挥发性存贮器内停止任何进一步的信息加载。

3. 如权利要求 1 的方法还包括以下步骤:

将设备串号从密码设备加载到位于远处的数据库中。

4. 如权利要求 3 的方法还包括以下步骤:

在密码设备内生成至少一个公共钥匙和一个私人钥匙;

发送公共钥匙到数据库;

用此钥匙将私人钥匙加密，产生加密的私人钥匙; 和

发送加密的私人钥匙到数据库。

5. 如权利要求 4 的方法还包括以下步骤:

提供公共钥匙给证明授权者; 和

用证明授权者的私人钥匙将公共钥匙加密产生数字证书; 和

将数字证书发送到数据库伴随公共钥匙和加密的私人钥匙。

6. 如权利要求 1 的方法，其中设备编号是唯一的并与其它密码设备的设备串号不同。

7. 如权利要求 1 的方法，其中钥匙是对称钥匙。

8. 如权利要求 7 的方法，其中对称钥匙是唯一的并与其它密码设备有关的其它对称钥匙不同。

9. 如权利要求 1 的方法，其中非挥发性存贮器被集成在密码设备的处理逻辑内。

10. 一种用于登记密码设备的方法包括以下步骤:

在数据库和用密码设备实现的电子系统之间建立通信信道，密码设备包括存贮钥匙和设备串号的非挥发存贮器;

将消息发送到数据库，消息包括包含在密码设备中的设备串号; 和

接收公共钥匙和用与密码设备有关的钥匙加密的私人钥匙。

11. 如权利要求 10 的方法还包括以下步骤:

将公共钥匙和用此钥匙加密的私人钥匙加载到电子系统的非挥发性存贮器部件中.

12. 如权利要求 10 的方法，其中通信信道不是安全的.

13. 如权利要求 10 的方法，其中钥匙是对称钥匙.

14. 如权利要求 10 的方法，其中在接收步骤以前，本方法还包括以下步骤.

数据库接收包括设备串号的消息;

利用设备串号作为查看索引; 和

发送公共钥匙和用此钥匙加密的私人钥匙到电子系统.

15. 如权利要求 10 的方法还包括以下步骤:

接收成为用证明授权者的私人钥匙加密的公共钥匙的数字证书.

16. 一种系统包括:

一个片组;

一个连到片组的非挥发性存贮器; 和

一个连到片组的密码设备，密码设备包括具有少量设备非挥发性存贮器的处理逻辑，非挥发性存贮器包含设备串号和对称钥匙.

17. 如权利要求 16 的系统，其中非挥发性存贮器包括至少一个与密码设备有关的公共钥匙和用对称钥匙加密的私人钥匙.

18. 如权利要求 16 的系统，其中本系统能建立与数据库的通信，以便将公共钥匙和加密的私人钥匙加载到非挥发性存贮器中.

19. 一种处理子系统包括:

一个基板;

一个连到基板的处理器;

一个连到基板的密码设备; 和

一个将处理器和密码设备互连的总线.

20. 如权利要求 19 的处理子系统，其中密码设备包括:

一个处理单元;

一个集成在处理单元中的非挥发性存贮器，非挥发性存贮器包括一个钥匙和设备串号; 和

一个随机数发生器.

21. 如权利要求 19 的处理子系统，其中密码设备的随机数发生器

被集成在处理单元内.

22. 如权利要求 19 的处理子系统，其中总线是后部总线.

23. 如权利要求 19 的处理子系统还包括一个塑料盒，通常装入基板而连接器位于基板的边缘.

5

00·05·22

说　明　书

配置与登记密码设备的电路和方法

发明背景

1.发明领域

本发明涉及密码领域．更具体而言，本发明涉及用于配置与登记密码设备的电路和方法．

2.与本发明有关的现有技术的描述

当前，许多个人正在利用个人计算机用数字格式存贮和发送敏感信息（例如，机密的、专有的，等），例如，信用卡帐户信息有时可在互联网上被传送供购物和/或服务．同样，利用在线银行传送银行帐号和银行帐户馀额．由于这种信息的敏感性质，已经采取措施在计算机的物理边界外部保护该信息的“完整性”；也就是，保证没有授权的情况下不变更信息．然而，这样的措施不能保护计算机内的信息．

正如在转让给 Intel 公司，本发明的受让人的美国专利 NO.5,539,828 中所描述的那样，可通过利用保密硬件来保护计算机内的信息．该保密硬件包括一个集成电路（IC）包，含有处理逻辑和专用的，在 IC 包中的非挥发性（NV）存贮器（称为“设备 NV 存贮器”）．典型情况下，该密码硬件在制造设备上经受一种穷举的配置阶段，其中设备 NV 存贮器被配置成包含为密码设备的安全功能必要的唯一的密码信息，例如，公共/私人钥匙对和数字证书．

当密码技术更加先进时，这种类型的结构将会觉得有些不足．一个缺点是需要较大，较贵的包，因为为了存贮较大数量的密码信息需要较大数量的设备 NV 存贮器．因此，支持位于系统其它地方，在此称为“系统 NV 存贮器的 NV 存贮器，大大减少位于密码设备中的 NV 存贮器数量是有成本效率的．系统 NV 存贮器的例子包括硬盘，位于母板或子卡上的 NV 存贮器，等．

当前，不可能使用系统 NV 存贮器．原因是为保证用对某个密码硬件唯一的密码信息配置与编程的系统 NV 存贮器将在具有密码硬件的电子系统内实现，一种可靠的，有成本效率的技术还未开发出来。

发明概述

一种用于配置和/或登记密码设备的方法，关于配置设计的一种实

施方案，设备编号被装入该密码设备的非挥发性存贮器．该密码设备的内部，生成一种钥匙并被加载到密码设备的非挥发性存贮器中．

附图简述

通过以下的本发明详述将使本发明的特征与优点变得更明显，其中：

图 1 是用作说明的一个电子系统的方框图，包括作为一个桥路部件应用的多片模块；

图 2 是最适合作为图 1 的桥路部件示出的多片模块最佳实施方案的方框图；

图 3 是用作说明的一个包括密码设备的图 1 中的处理子系统实施方案；

图 4 是用作说明的一种图 3 基板的实施方案；

图 5 是由图 2 的密码设备执行的配置方案流程图；

图 6 是由图 2 的密码设备执行的登记方案流程图．

最佳实施方案描述

本发明涉及用于利用非常驻，非挥发性（NV）存贮器配置密码设备和从远处登记密码设备的系统与技术，在以下的描述中，某些术语通常被用来描述本发明的某些特性．例如，“电子系统”通常被定义为具有信息处理功能的任何硬件产品，例如，计算机，传真机和打印机．“信息”通常被定义为一位或多位数据，地址，和/或控制信息．

另外，以下的术语被用于识别不同类型的密码信息．“钥匙”是一种由常规的密码功能使用的编码和/或解码参数，例如对称钥匙密码功能（例如，基于数据密码标准“DES”的功能）或公共钥匙密码功能（例如，基于 Rivest，Shamir 和 Adleman（RSA）的功能）．“数字证书”通常被定义为用于用户证明的任何信息（例如，公共钥匙）．用证明授权的私人钥匙（PRKCA）对信息编码，授权者也就是任何个人或者处于信托地位担保或保证数字证明的任何实体，例如银行，政府部门，贸易社团，原始设备制造商，等．

参考图 1，示出一个用作说明的应用本发明的电子系统 100 的实施方案．在此实施方案中，电子系统 100 包括将许多子系统互连的片组 110．这些子系统的例子可以包括，但并不限于，处理子系统 120，存贮器子系统 130，输入/输出（I/O）子系统 140．这些子系统 120，130

和 140 合起来控制电子子系统 100 的功能.

更具体而言，作为一个用作说明的实施方案，处理子系统 120 包括至少一个中央处理单元（CPU）121. CPU121 通过主总线 122 连到片组 110. 存贮器子系统 130 通常包括一个或多个挥发性存贮器组（未示出），例如任何类型的动态随机存取存贮器（DRAM），和/或静态随机存取存贮器（SRAM）. 然而，打算，系统 NV 存贮器可被用于存贮器子系统 130 替代或补充挥发性存贮器.

而且，I/O 子系统 140 包括“n”个连到 I/O 总线 142 的外围设备 141_1 - 141n（n 是一个正整数），外围设备的例子包括大容量存贮设备 141_1（例如，硬盘驱动器，数字带驱动器，软盘驱动器，和数字多用途盘“DVD”播放器）.

为了提供保密功能，保密设备 150 可通过专用总线 160 连到片组 110. 当然，作为一种替代的系统实施方案，密码设备 150 可被放置为与计算机 100 中任何总线通信，例如主总线 121 或另一个基于处理器的总线，如后部总线（未示出），或也许是 I/O 总线 142.

参考图 2，示出一种用作说明的图 1 中的密码设备 150 的实施方案，密码设备 150 包括一个集成电路（IC）设备 200，包含在一个保护 IC 设备 200 免受危险和有害污染的封套 205 内. IC 设备 200 包括与少量设备 NV 存贮器 215 集成在一起的处理单元 210，作为选项，随机数发生器 220 可被制作在封套 205 内作为一个分离设备通过内部总线 225（如图所示）连到处理单元 210 或者集成在处理单元 210 内. 当密码设备 150 在配置模式中工作时，随机数发生器 220 被用于产生一个或多个钥匙.

虽然示于图 2 中的密码设备 150 的实施方案可作为一个协处理器来实现，然而可以选择各种各样的不同实施方案. 例如，密码设备 150 可被实现在一个盘控制器内，在一个“智能”卡上（部分像信用卡形状但具有微控制器的形式），或者在包括 CPU121 的盒式处理器封套内，如以下图 3 - 4 中所示. 其它的替代实施方案可以包括将密码设备的功能并入片组或 CPU121 内.

参考图 3，示出将密码设备 150 实现在处理子系统 120 内的一种替代的系统实施方案的透视图. IC 部件（包括密码设备 150）被安放在由任何类型的材料组成的处理器基板 300 上，IC 部件（未示出）可通过熟知的技术（例如焊接，等）贴附在上面. 处理器基板 300 大部分

由一个矩形封套 310 盖住，以便保护 IC 部件免受危险或有害污染，处理器基板 300 包括连接器 320，最好适合于例如，建立与母板的机械和电气连接。正如所示，连接器 320 可以包括一个标准的公的边缘连接器（如图所示）或也许是一个母的边缘连接器。

如图 4 中所示，处理器基板 300 中的 IC 部件包括，但并不限于，CPU121，存贮器 330 和密码器 150. 为了与 CPU121 通信，密码设备 150 可以放在（i）后部总线上，通常与存贮器 330 相连，（ii）前部总线上，通常与外部连接器 320 相连，或者（iii）专用内部总线上. 当然，只要执行时间和其它必不可少的条件被保持，这种密码设备 150 的安放是随意的. 虽然未示出，分立元件（例如，电容，振荡器，电阻，电感，等）以一种有选择的方式贴附在处理器基板 300 上，特别是要最大限度地提高路由能力并减少这些 IC 部件之间的通信线路的长度.

现在参考图 5，示出一种由密码设备使用的配置方案的最佳实施方案. 在制造时，密码设备经受一种配置状态，以便仅将有限数量的密码信息加载到它的集成化的设备 NV 存贮器中，对于这种配置状态的一种实施方案包括使用一种证明系统，包括（i）具有一种尺寸容纳下密码设备的设备载体的编程机构，和（ii）从编程机构接收密码信息的数据库（例如，服务器，个人计算机，主帧，等）. 为了避免使本发明含糊不清，将只描述编程机构的功能操作.

当接通时，编程机构开始供电并通过设备载体将预定的控制信息提供给密码设备的相应引线. 这种控制信息将密码设备放入配置模式（步骤 400）. 在放入配置模式以后，密码设备开始从编程机构接收唯一的设备串号（DSER）（步骤 405）. 通常利用足够数量的位以避免重复（例如，32 或 64 位），DSER 被存贮在密码设备的集成化设备 NV 存贮器中并提供给数据库（步骤 410）. DSER 被数据库用作指针表的索引. 每个指针负责对存贮器中一个或多个位置寻址，包含与由它的 DSER 识别的密码设备唯一有关的密码信息.

此外，通过对密码设备供电，随机数发生器被供电，产生随机数用于生成唯一的对称钥匙（SK）和公共/私人钥匙对（步骤 415）. 公共钥匙（PUK）被输出到数据库未经受任何修改（步骤 420）. 然而，私人钥匙（PRK）被利用密码算法加密（例如，预加载在密码设备的存贮器中的 DES），然后，输出到数据库（步骤 425）. 更具体而言，PRK

在输出到数据库以前用 SK 加密（产生 E_{SK}（PRK））。结果，密码设备包含最少数量的密码信息，也就是 SK 和 DSER，而数据库中被检索的位置包括大多数的密码信息。

有时，如虚线所示，可以设想，与 PUK 和 DSER 有关的数字证书可在稍后的时间里装入数据库，甚至在密码设备已被送到原始设备制造商（OEM）以供放入电子系统（步骤 430）以后。数字证书包括至少用在本实施方案中的制造商的私人钥匙加密的 PUK，可用作密码设备的后续授权。然而，可以设想，DSER 可被包括在数字证书中。

在密码设备已经装入具有足够系统 NV 存贮器的电子系统以后，可为登记的目的建立到制造商数据库的通信。这种登记方案不需要安全的通信信道，因为 PRK 已被加密。可由任何下游用户执行登记，包括装运电子系统到最终用户以前的 OEM，或者最终用户，对于后一种情况，电子系统可用具有登记子程序的系统软件来加载。在由系统软件对电子系统初始化期间，登记子程序可帮助建立与数据库的通信，以便恢复和下载对电子系统唯一的密码信息。这种登记方案对于最终用户可以是透明的或者在与某些项目和条件的符合方面要求最终用户有效参与（例如，解除制造商的责任，等）。

现在参考图 6，示出一种在制造商的数据库与下游用户（OEM，最终用户，等）之间登记方案的实施方案。首先，在数据库与用密码设备实现的电子系统之间必须建立通信信道（步骤 600）。这可以通过专用电话线路在互联网或者在任何其它的通信链路上实现。接着，电子系统将包括从它的密码设备得到的 DSER 的消息在通信信道上发送到数据库（步骤 605）。数据库接收此消息并利用 DSER 作为索引，搜索与由 DSER 识别的密码设备有关的密码信息（步骤 610）。这种密码信息（PUK，E_{SK}（PRK），和数字证书）被在通信信道上发送到电子系统并加载到电子系统的系统 NV 存贮器中（步骤 615－620）。因此，现在密码设备完全有功能去支持公共钥匙加密，因为它具有对它的 PUK 和 PRK 的入口，E_{SK}（PRK）可利用已经在它的设备 NV 存贮器中集成的 SK 来解密。

虽然已描述了某些示范性实施方案并示于附图中，但应该理解，这样的一些实施方案仅仅是用作说明而并不是对本发明的限制，本发明并不限于所示的和所描述的具体结构和安排，因为对于本领域的技术人员来说，可能有各种各样的其它的修改方案。

说 明 书 附 图

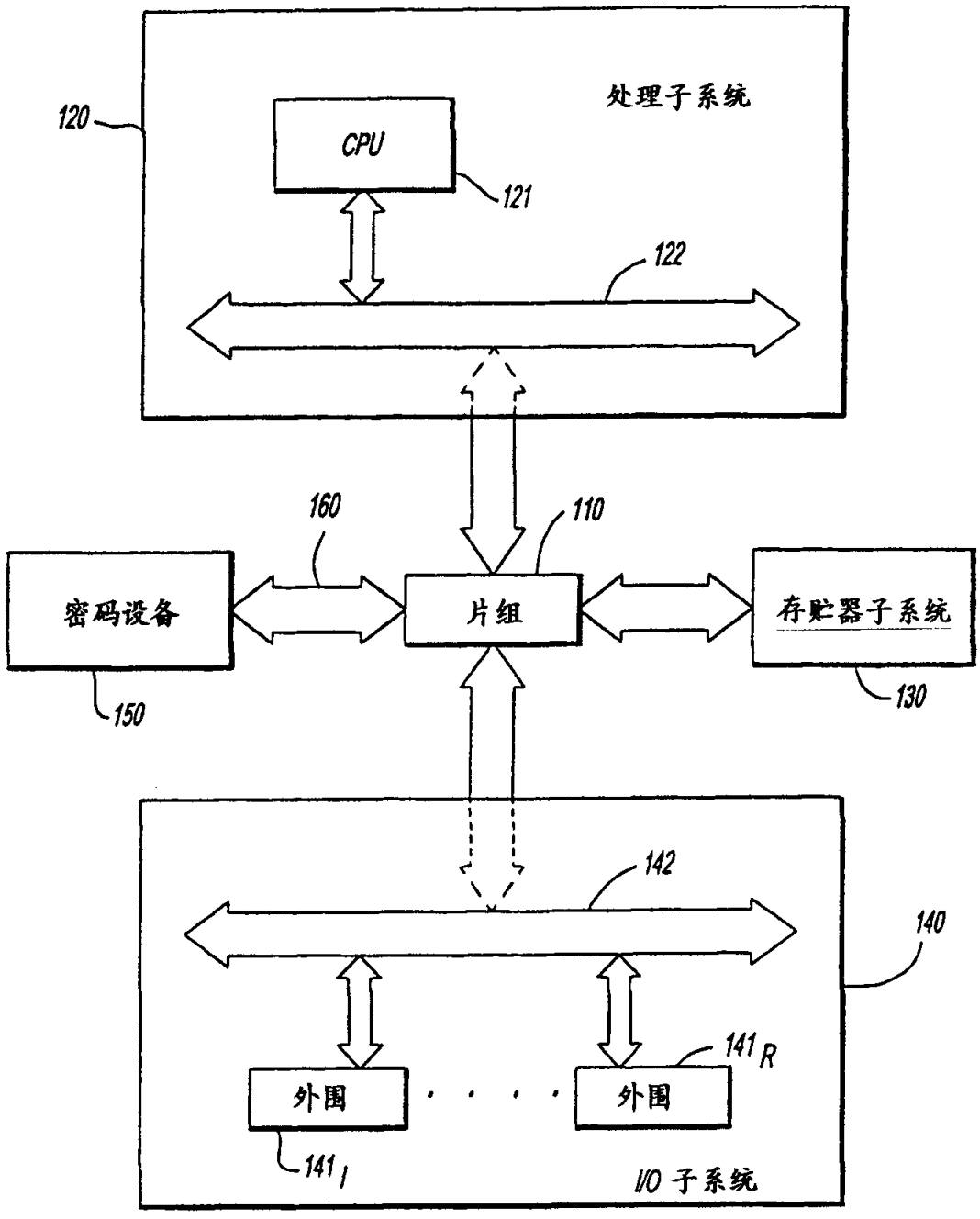

处理子系统
120
CPU
121
122
160
110
密码设备
片组
存贮器子系统
150
130
142
140
141R
外围
外围
141I
I/O 子系统

图 1

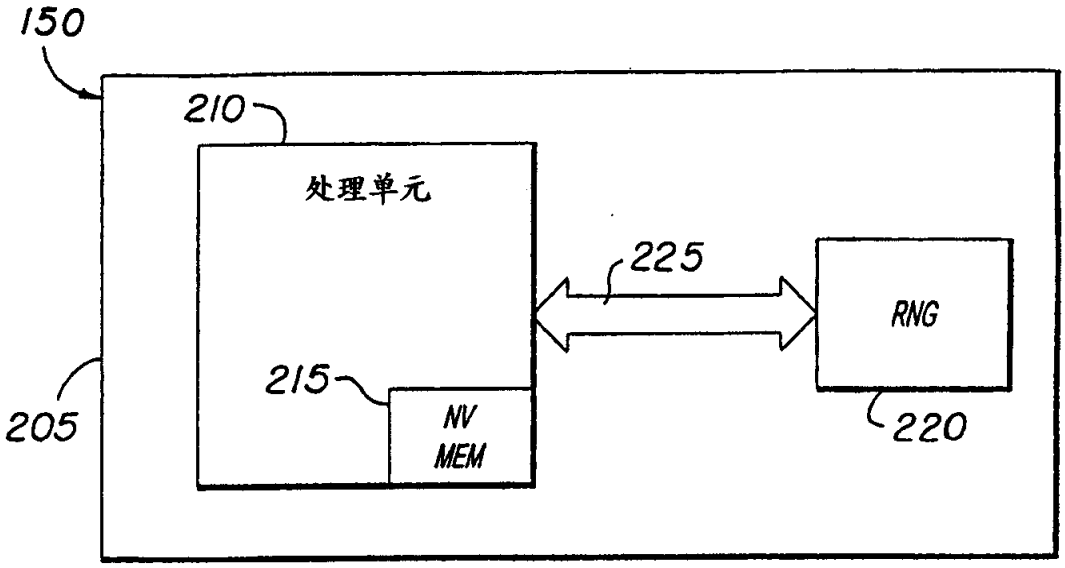

150
210
处理单元
225
RNG
215
NV
MEM
205
220

图 2

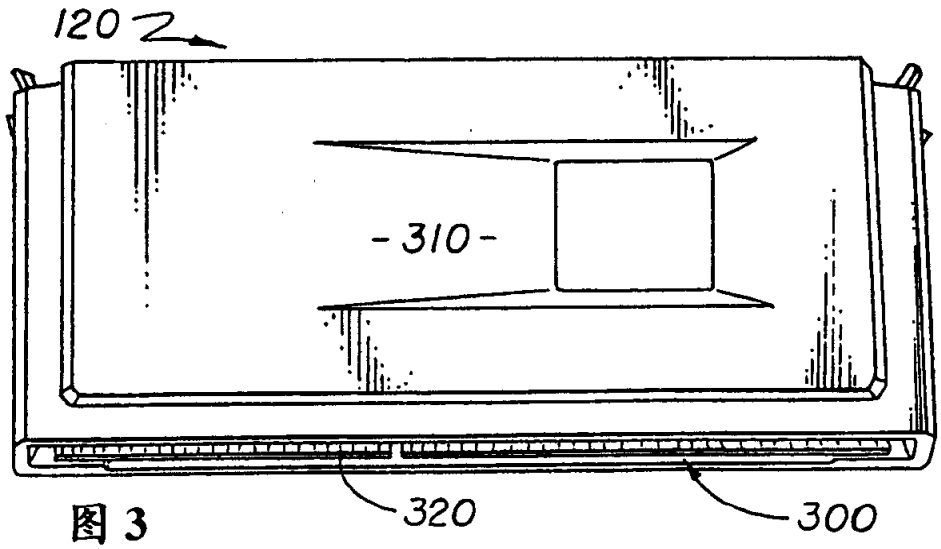

120
-310-
320
300

图 3

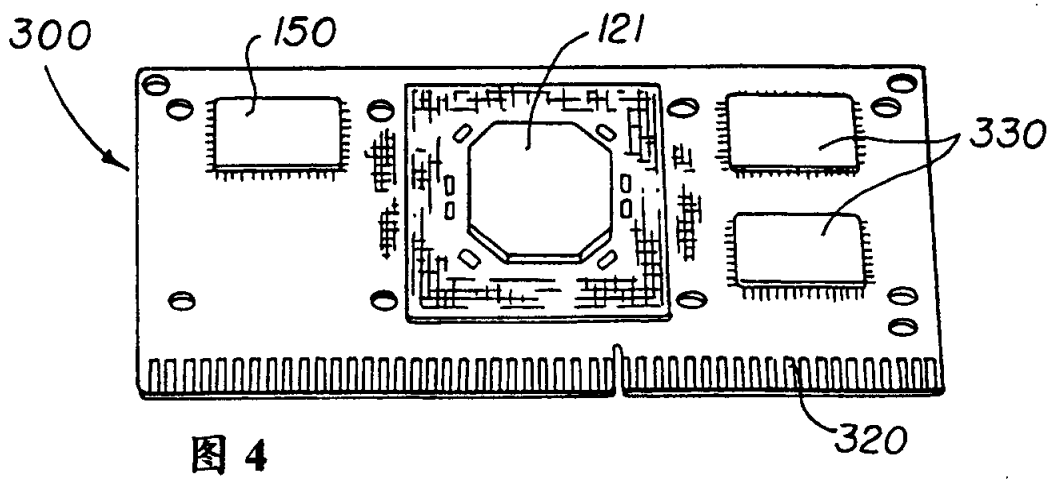

300
150
121
330
320

图 4

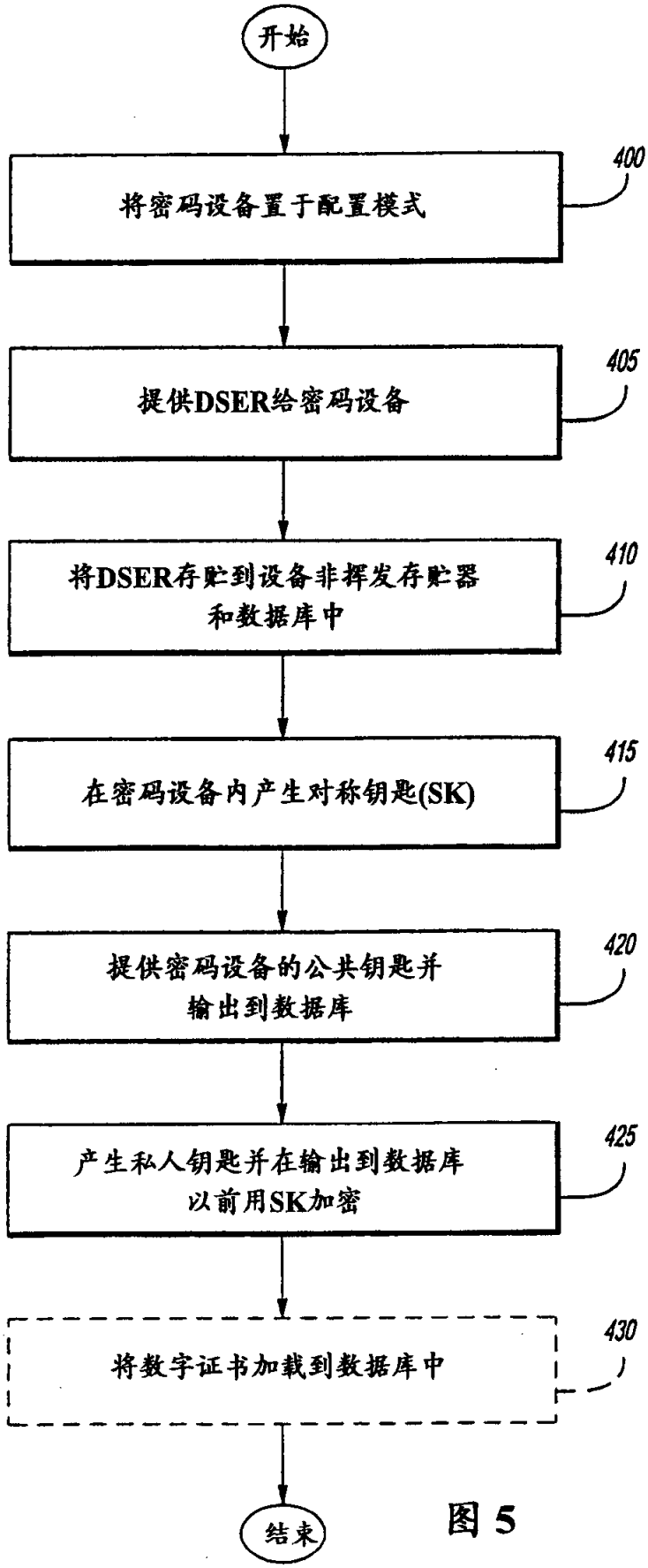

开始
400
将密码设备置于配置模式
405
提供DSER给密码设备
410
将DSER存贮到设备非挥发存贮器
和数据库中
415
在密码设备内产生对称钥匙(SK)
420
提供密码设备的公共钥匙并
输出到数据库
425
产生私人钥匙并在输出到数据库
以前用SK加密
430
将数字证书加载到数据库中
结束

图 5

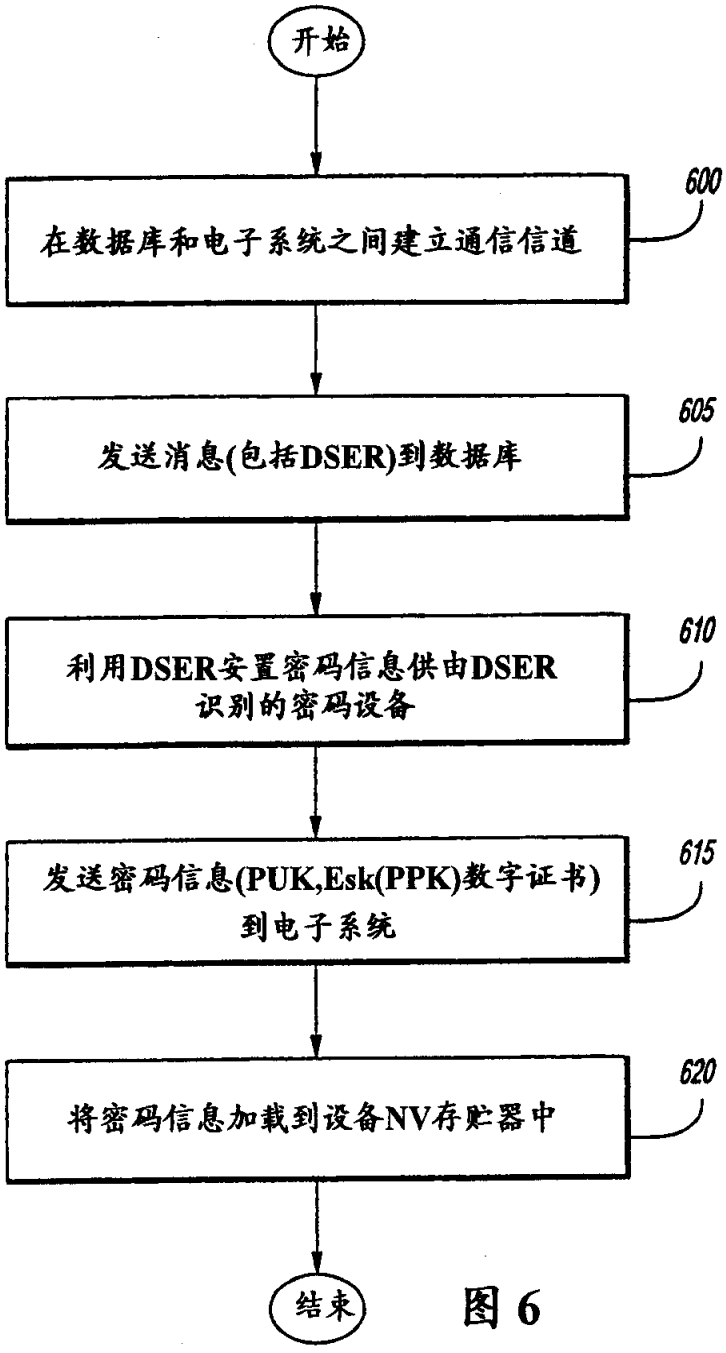

开始
600
在数据库和电子系统之间建立通信信道
605
发送消息(包括DSER)到数据库
610
利用DSER安置密码信息供由DSER
识别的密码设备
615
发送密码信息(PUK,Esk(PPK)数字证书)
到电子系统
620
将密码信息加载到设备NV存贮器中
结束

图 6