

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/30 (2006.01)



[12] 发明专利说明书

专利号 ZL 03141220.3

[45] 授权公告日 2009 年 5 月 27 日

[11] 授权公告号 CN 100492277C

[22] 申请日 2003.6.5 [21] 申请号 03141220.3

[30] 优先权

[32] 2002.6.7 [33] US [31] 10/165,519

[73] 专利权人 微软公司

地址 美国华盛顿州

[72] 发明人 D·莫雷斯 J·兰格 D·西蒙

陈陵 J·D·贝纳勒

[56] 参考文献

US6185678B1 2001.2.6

审查员 王丹

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 刘佳

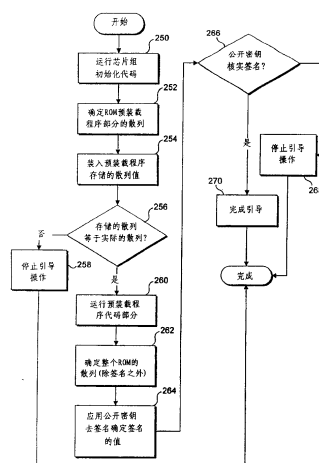
权利要求书 3 页 说明书 9 页 附图 3 页

[54] 发明名称

在安全的引导载入程序中使用散列法的方法和装置

[57] 摘要

由自举代码组成的机器指令隐藏在电子游戏控制台的一个重要组成部分里面，在那里它们不能容易的被存取或修正。在只读存储器 (ROM) 的预装载程序部分由引导代码散列和结果与一个期望的保持在引导代码散列值比较。起动过程的进一步确认由预装载程序执行，散列在 ROM 的代码为代码获得一个散列值。结果对照数字签名核实为这散列定义一期望的值。获得任何的预期结果的失败终止起动过程。当引导代码确认预装载程序，并且预装载程序证实在 ROM 里剩余的代码，这为保证用于引导设备的代码未被修改或未被替换的技术是有用的。



1. 一种确定在电子设备的起动期间被提供用于执行的代码是否被授权的方法，其特征在于，所述方法包括步骤：

- (a) 散列代码的预定义部分以产生第一散列值；
- (b) 比较第一散列值与保持在电子设备的电路部件的一个被存储的散列值，所述电路部件从存储代码的存储器分离，以核实所述代码的预定义部分是被授权的；
- (c) 如果第一散列值等于被存储的散列值，则执行被预定义的代码部分，并且如果不是，终止电子设备的起动；
- (d) 其中执行被授权的所述被预定义的代码部分包括执行以下步骤：
 - (i) 充分散列包括所述预定义部分的所有代码，以确定第二个散列值；并且
 - (ii) 核实包括在代码中的一个数字签名是否匹配于第二个散列值，如果那样，则执行所述代码，和如果不是，终止电子设备的起动。

2. 如权利要求 1 所述的方法，其特征在于，其中比较第一值与被存储的散列值的步骤包括执行被保持在电路组分的一个无挥发性的存贮器部分的一个初始代码，所述的初始代码包括被存储的散列值。

3. 如权利要求 2 所述的方法，其特征在于，其中初始代码被保持在一个附加的处理器。

4. 如权利要求 2 所述的方法，其特征在于，其中初始代码被保持在：

- (a) 一个图形处理器；
- (b) 一个声音处理器；
- (c) 一个输入处理器；
- (d) 一个输出处理器；
- (e) 一个通信处理器；和
- (f) 一个数字信号处理器。

5. 如权利要求 2 所述的方法，其特征在于，其中初始代码被保持在执行

初始代码的处理器。

6. 如权利要求 2 所述的方法, 其特征在于, 其中初始代码被运行以执行权利要求1的步骤(a)至(c)。

7. 如权利要求 2 所述的方法, 其特征在于, 其中初始代码以一个预定的字节数永久地被定义在固件中。

8. 如权利要求 1 所述的方法, 其特征在于, 其中代码的预定义部分包括预装载程序代码, 所述预装载程序代码具有被配置在所述代码的一个预定区域中的预定字节数。

9. 如权利要求 8 所述的方法, 其特征在于, 其中核实数字签名的步骤是执行包括在预装载程序代码的一个公开密钥。

10. 一种确定在电子设备的起动期间被提供用于执行的代码是否被授权的装置, 其特征在于, 所述装置包括:

(a) 散列代码的预定义部分以产生第一散列值的装置;

(b) 比较第一散列值与保持在电子设备的电路部件的一个被存储的散列值的装置, 所述电路部件从存储代码的存储器分离, 以核实所述代码的预定义部分是被授权的;

(c) 如果第一散列值等于被存储的散列值, 则执行被预定义的代码部分, 并且如果不是, 终止电子设备的起动的装置;

(d) 其中执行被授权的所述被预定义的代码部分的装置包括:

(i) 充分散列包括所述预定义部分的所有代码, 以确定第二个散列值的装置; 并且

(ii) 核实包括在代码中的一个数字签名是否匹配于第二个散列值, 如果那样, 则执行所述代码, 和如果不是, 终止电子设备的起动的装置。

11. 如权利要求 10 所述的装置, 其特征在于, 其中比较第一值与被存储的散列值的装置包括执行被保持在电路组分的一个无挥发性的存储器部分的

一个初始代码的装置，所述的初始代码包括被存储的散列值。

12. 如权利要求 11 所述的装置，其特征在于，其中初始代码被保持在一个附加的处理器。

13. 如权利要求 11 所述的装置，其特征在于，其中初始代码被保持在：

(a) 一个图形处理器；

(b) 一个声音处理器；

(c) 一个输入处理器；

(d) 一个输出处理器；

(e) 一个通信处理器；和

(f) 一个数字信号处理器。

14. 如权利要求 11 所述的装置，其特征在于，其中初始代码被保持在执行初始代码的处理器。

15. 如权利要求 11 所述的装置，其特征在于，其中初始代码被运行以实现如权利要求10的装置(a)至(c)。

16. 如权利要求 11 所述的装置，其特征在于，其中初始代码以一个预定的字节数永久地被定义在固件中。

17. 如权利要求 10 所述的装置，其特征在于，其中代码的预定义部分包括预装载程序代码，所述预装载程序代码具有被配置在所述代码的一个预定区域中的预定字节数。

18. 如权利要求 17 所述的装置，其特征在于，其中核实数字签名的装置是执行包括在预装载程序代码的一个公开密钥。

在安全的引导载入程序中使用散列法的方法和装置

技术领域

本发明通常涉及安全地启动（引导）包括一个处理器的电子装置，尤其涉及确定当启动这样的电子装置时只需要由处理器运行机器指令，以便防止在启动过程期间被执行的机器指令替代或取舍。

背景技术

有许多类型的电子装置在初始通电或者重新设定时必须接受引导处理。在启动过程时，控制电子装置基本操作特性的机器指令典型地从存储在只读存储器（ROM）中获取并且执行初始化设备和使能装载进一步的机器指令到随机存取存储器（RAM）它将被执行使电子设备实现更多的功能。举例来说，当一台个人计算机被启动时，由基本的输入-输出系统（BIOS）组成的指令被运行使操作系统被计算机的中央处理单元（CPU）从一个硬盘驱动器载入到RAM并且运行。术语“启动”是比较早的简易格式和也许更多的描述术语为“自举”。

必须被启动的其它类型电子设备包括游戏控制台、数字记录设备、个人数据系统，和包括某种形式的处理器的几乎任何其他电子产品必须执行一套最初的机器指令使能进一步的功能，如另外的机器指令装入到内存和被执行。由于启动过程确定一个电子设备的初始状态，它影响设备的重要操作参数，可能实际上影响在启动过程被完成后电子设备怎样被使用。对于出售电子设备的公司防止启动过程的修改可能是重要，避免由于装置的使用发生收入的损失。

例如，在电子游戏工业中，许多游戏控制台的市場价值由运行在游戏控制台的游戏软件产生许可证收入卖玩电子游戏获得。从而，在启动过程期间装载的机器指令实现功能防止运行在游戏控制台的软件无许可的拷贝和强制关于用游戏控制台玩电子游戏的制造商的政策。某些用户倾向于认为运行无许可的软件的拷贝的制约和强制执行在游戏控制台的这样政策的制约对游戏控制台的用途作为一个挑战和一个不受欢迎的限制。这些用户研究用程序“挖口”

（hacking）游戏控制台电路和软件克服这些制约。例如，单向的避免这些制约是根据运行在游戏控制台启动过程装载某些做了修改的改变软件内核。这些变动去除由游戏控制台的制造者强加的制约，如果软件游戏的无许可的副本因

此被能够运行在游戏控制台，能造成关于游戏控制台如何被使用的制造商的控制损失的结果，和能引起收入的损失。因此，通常游戏控制台制造者用大量的努力保证防止黑客使能一个修改过的软件内核在起动过程期间被使用。

一个相似的问题存在在使用电子设备必须起动处理的其它技术领域。例如，卫星电视接收器制造商根据由用户支付的月费限制频道接收必须保证他们的安全政策和关于他们的产品的使用政策被遵循以便消费者只能与它的许可一致的期限使用电子设备。黑客也许能修改根据在卫星接收器的处理器确定用户支付观看电视频道的代码，因此没有做适当的许可费付款使能所有频道被接受和被观看。

因此，保证唯一授权软件代码在电子设备的起动期间被执行是所希望的。用于防止修改的或取舍机器指令集替代在起动设备期间打算执行的授权软件的任何技术，因而保证电子设备实施制作并且/或者分发它给终端用户的功能和当事人的政策。已知的方法通常防止黑客击败关于对电子设备的用途制约和政策，它包括在起动电子设备代码的装载，是明显地不完全成功。通过使用包括供选择的软件代码的扩展程序电路卡，已知的安全方法能至少部份地由连接电路卡到电子设备的线路的黑客击败。明显地，一种更加安全和更加严谨的方法必需防止在电子设备的起动过程期间一个供选择的代码被插入和被执行。

发明内容

本发明通常可以应用在包括一个处理器和当初始加电或重新设置时必须起动的几乎任何的电子装置，使电子的装置其他的功能能够被运行。在这样设备，经常保护在设备操作期间被使用的私有的信息和防止在起动过程期间未授权的代码被执行、破坏与电子设备的操作和应用有关的政策将是重要的。

破坏一个电子设备的预期的政策和功能很可能被替换部件之一是存储定义电子设备怎么使用的非易失性存储器的机器指令。因此，本发明试图证实，由在这样的存储器的机器指令组成的代码是被授权的(也就是，没有由于机器指令被修正或替换以改变电子的装置期望的功能和政策)。本发明，授权代码包括一个被预定义的部份(也称为预引导程序代码)。既使当对授权代码的剩余物产生变动，这个被预定义的部份必须保持同样，或电子设备将不会起动。

程序初始执行确保被预先定义的代码部分是授权的。在这个过程中，被预先定义的部分被散列，产生第一散列值。接着，第一散列值从存储代码的存储

器分离，与保持在电子设备的电路部件的一个被存储的散列值比较，核实被预定义的部份的代码是被授权。如果第一散列值等于被存储的散列值，使能执行被预定义的代码部份，并且如果不是，电子设备的起动被终止。如果被预定义的代码部份是允许的，则充分地散列所有代码，确定第二散列值。与被预定的代码部分相比，数字签名包括在代码的不同部份。然后对照数字签名第二散列值被核实，确保署名的真实性。如果数字签名被核实是可信的，代码的执行是允许的，并且如果不是，电子设备的起动被终止。

为了要比较第一值和被储存的散列值，在电路部件的非挥发性存储器部分中被保持的初始代码被运行。这个初始的代码包括被存储的散列值和被保持在一个图形处理器，虽然，它也考虑被存储的散列值可能保持在其它辅助处理器，例如 一个音频处理器，一个输入处理器，一个输出处理器，一个通讯处理器或一个数字信号处理器。的确，它甚至是更好的保持初始的代码和期望的散列值在执行初始代码的处理器。初始代码被执行散列被预定义的部份，和执行比较第一散列值与被存储的散列值。以发明的较佳的形式，初始代码以预定的字节数永久地被定义在固件中。另外，被预定义的代码部份更好地包括被预定的字节数配置在一个预定的代码区域内。明显地，除非被存储的代码相应地被改变，被预定义的部份的散列值大小和内容无法被修改，因为被存储的散列值不会等于第一散列值。

被预定义的代码也包括被用于核实数字签名的一个公开密钥并且有使代码的一个被编码的内核部份被解码的机器指令。被解码的内核然后被执行完成电子设备的起动。被预定义的代码使用一个流密码实施代码的内核部份的解密。

本发明的另外一个方面指向在其中储存代码的存储媒介包含在一个电子设备起动期间确定代码是否被授权的存取的机器指令。记忆媒介包含内核部份、起动装载程序部份、预装载程序部份，和数字签名，通常如上所述。

本发明的另外方面指向必须被引导的电子设备操作。电子设备包括在非挥发性存储器中存储的多个机器指令。非挥发性存储器包括主要的部分和有被预定义内容，大小和位置的预装载程序部分。一个处理器被连接到非挥发性存储器在起动过程期间运行机器指令。引导代码固件元件指定机器指令定义散列算法和一个期望的散列值。在电子设备的起动期间引导代码固件的机器指令由处理器初始执行，导致处理器执行预装载程序部份的散列和对照期望的散列值的结果。电子设备和它的功能的其它细节通常与上面被讨论的方法步骤一致。

在一个电子设备使用本发明，譬如游戏控制台，企图在起动过程期间改变被执行的机器指令或用其它存储器不同的机器指令替代将防止设备成功地引导,它将是明显的。因此，本发明通常防止某人修改基本的功能或避免由电子装置实现需要的政策，确保在电子设备的起动期间唯一授权代码被执行。

附图说明

前述方面和许多本发明的伴随好处将变更容易评价当参考如下详细描述将同样更好的理解，当理解伴随的附图时，其中：

图1 是使用本发明游戏控制台的一个立体示意图；

图2A 是包括在游戏控制台图1的几个功能部件的结构图；

图2B 是一般电子设备起动和包括处理器和存储器的功能结构图；

图3 是被配置在本发明的举例说明存储器部份的概要图；和

图 4 是在本发明举例说明逻辑实施的流程图。

具体实施方式

典型系统

必须强调，本发明不打算被限制只用在游戏控制台，虽然本发明的最初的较佳的实施的确被使用在游戏控制台上。本发明被开发确保私有的信息不被透露给试图逆向工程代码的用户，并且防止用户消除许可制约和与关于用游戏控制台玩电子游戏的政策。

如图1所示，一个典型电子游戏系统100 包括游戏控制台102 和支持到四种用户输入装置，譬如控制器104.a 和104b 。游戏控制台102装备内部硬盘磁碟机（不在图中示出）和便携式媒体驱动器106以光盘存储器108 为代表的支持各种各样便携式的光存储器媒介. 适当的便携式的存储介质的例子，包括DVD 盘和CD-ROM 盘。在这个游戏系统，游戏程序在游戏控制台使用DVD 盘更好地被分配，但它也考虑其它存储介质替代使用或使用本发明其它类型系统执行数据保密政策和确保数字数据真实的被输入到系统。

在游戏控制台的前面板102 是四个槽孔110 为连接和支持控制器，虽然槽孔的数量和安排可能被修改。电源按钮112 和弹出按钮114 也被安置在游戏控制台102 的前面板。电源按钮112 控制游戏控制台的电能应用，和弹出按钮114

交替打开和关闭便携式的媒介驱动106的盘子(没被显示) 使能插入和取出存贮盘108 以便其上的数字数据能由游戏控制台读出供使用。

游戏控制台102通过音频/视频(A/V) 接口电缆120 连接到一台电视或其它监视器或屏幕(没被显示) 。电缆插座122 当连接到一条常规交流电线源(没被显示)传达电能到游戏控制台。游戏控制台102 进一步带有数据连接器124 在网络上传输数据譬如互联网, 例如, 通过一个常规电话调制解调器, 或更好, 由宽频连接。

每个控制器 104 和104b 通过导线(或选择通过一个无线接口)被连接到游戏控制台102。 在被说明的实施中, 控制器是通用串行总线(USB) 兼容和通过USB 缆绳130被连接到游戏控制台102。游戏控制台102 被装备以任何各种各样的交互用户设备和控制游戏软件。虽然控制器104.a的所有细节不显示在图1, 各个控制器104.a 和104b 被装备以二个拇指操纵钮132.a 和132b , D一垫(pad) 134 , 按钮136 , 和二切换开关138 。这些控制器仅仅是代表性的, 并且其它已知的游戏输入和控制机构可以被替代为或增加到那些显示在图1用于游戏控制台102 。

一个可移动或便携式的存储器单元(MU) 140 可能任意地被插入到控制器104 提供附加的可移动的存贮。便携式的MUs 通过插入便携式的MUs 到其它控制器使用户存放游戏参量和带它们在其它控制台玩。在被描述的实施中, 各个控制器被配置容纳2个MUs , 虽然比2个MUs更多或较少可以代替被使用。

游戏系统100 是能玩游戏、听音乐, 和看录影。考虑其它功能使用存放在硬盘驱动器数字资料或从驱动106的光存储器盘108 读, 从在线源, 或从MU 140 能被实施。游戏控制台被设计防止未许可的拷贝的电子游戏盘在游戏控制台上玩。并且, 某个政策由游戏控制台强制执行。例如, 软件被销售到一个地区可以阻止被销售一个另外地区的游戏控制台上执行。同样, 防止视频DVDs复制的业界标准计划(MACROVISIONTM)由游戏控制台软件实施。

某些用户会喜欢击败由游戏控制台实施的这些功能限制和政策。试图避免这些局限和政策的一个方法是由安装集成电路(IC) 或模块在游戏控制台, 以一个修改过的版本, 替换原始的ROM 和被存放在其中用于引导的游戏控制台代码。在这样的替换模块里修改机器指令打算在起动过程期间操作和消除或改变由游戏控制台制造者或设计师强加对未授权的拷贝的用途, 复制录影DVD, 和游戏控制台的其它功能方面和/或者政策的制约的限制。但是, 本发明使插入一

个未授权的替换ROM 模块改变起动过程和终止起动过程非常困难如果它查出在游戏控制台的起动期间企图使用供选择和未授权的代码。

为了防止关于起动过程的私有的信息被发现和在起动过程期间防止修改或供选择的代码被使用，至少在起动期间被执行的某一机器指令的部份必须与包括在游戏控制台或其它电子设备的ROM 之内多数的机器指令分开保留。通常，如果电子设备被打开，IC、跟踪、连接点，和通过电子设备的印制电路板是容易接近的，使能新连接和具体的修改破解设备。虽然防止某人访问印制电路板是困难的，本发明使访问被嵌入装配在印制电路板上的一个IC内作为固件的机器指令非常难。更好地，对供应商用作这用途的IC应该不容易能够公开，因为它是为电子设备的制造商定制的。并且，用作此用途的IC应该基本是对电子设备的操作，以便如果企图访问被嵌入在IC的固件，它是非常象IC 的操作，和因而，电子设备的操作将相反地影响。

图 2A 举例说明被包含在游戏控制台100一些IC部件。CPU 202 是主要处理器和用于执行游戏控制台的大多数处理功能的。CPU 202 必须初始引导，与多数处理器相同，使能执行游戏控制台被设计实施的各种各样的功能。CPU 202 是双向连接到一个定制的图形处理器，它也是由NVIDIA Corporation 生产的总线和记忆控制器芯片204和被称为NV2A 芯片。NV2A 芯片连接到RAM 206 和到另外的 NVIDIA 定制的媒体通讯处理器 (MCP) 208芯片，提供声频信号处理器能力，连接到系统存储器，和为数据通讯也连接到USB 口和以太网口。在MCP 208 内包括512 个字节的固件组成的引导代码212。引导代码212 实质上隐藏在MCP 208内的其它层之下和不打开该模块简单地接近。为了完全访问引导代码212，是必要去除其它叠加的层，那将有效地毁坏MCP模块，使它和游戏控制台无法使用。此外，因为MCP 208 是为游戏控制台的制造商定制的，在开放的市场上其他人不是可利用的。即使引导代码在某些方式下被获取使包括这个固件的机器指令"可见，" 本发明使起动序列不能改变。MCP 208 连接到ROM 210，在起动游戏控制台100期间包括大多机器指令被使用。

本发明的一种更加一般的应用其构成被显示在图2B。它设想定制CPU 220 能包括固件引导代码222 "隐藏" 在其中，在CPU 的其它层之下。如图 2B 所示，CPU 220 被连接到RAM 206 和ROM 210。因为引导代码222由CPU 220 内的固件组成，在CPU处理部份和引导代码222 之间的信号一般不能进入。因此，对于显示在图2B的实施例，它更加难访问引导代码222 和确定它的内容，

并且因而，相对图2.A的实施例，图2B的实施例在安全上提供进一步增加。

图 3 举例说明使用在本发明的ROM 210 的不同的部份。在使用在游戏控制台100中的更佳的实施例，ROM 210 包括一个256 个千字节存储器模块。包括在ROM 210 中的预装载程序230，不被编码。预装载程序 230 固定了大约11 个千字节的大小在较佳的实施例中，并且它的内容、大小，和地点在ROM 210 之内是全部被预定义的。注意预装载程序230 包括编码的公众钥匙 231是重要的。需要保持预装载程序230 的内容无变化也是重要的，除非对应的变化产生到固件引导代码 212，同样下列各项解释是显然的。ROM 210 也包括起动装载程序232，它被编码。另外，ROM 210 包括一个数字签名234 和一个对称密钥236。到目前为止 ROM 210 的较大部分致力于存储机器指令组成内核 238。内核238 被压缩和编码。包括在内核238 之内机器指令定义许多功能和建立相关游戏控制台100操作的政策。最后，芯片组初始化代码240 被包括和当初始供电给游戏控制台时被执行。

图4 举例说明当游戏控制台102 被初始加电或被重新设置时被实施的逻辑步骤。步骤250 提供运行在ROM 210 里的芯片组初始化代码。机器指令包括在芯片组初始化代码240 之内不被编码；他们定义具体配置信息和具体配置序列完全合乎游戏控制台体系结构。机器代码必需执行芯片组配置包括在引导代码；具体值和序列是芯片组初始化代码的一部分。并且，CPU的初始化序列包含在引导代码和在芯片组初始化代码的剩余物之前被执行。其次，在块252，机器指令包括在固件引导代码212之内，它隐藏在MCP 208 之内，为在ROM210 的预装载程序230运行单程散列算法确定一个散列值。如上所述，当出品时，原始的ROM 210被安装在游戏控制台100 之内，在ROM 210 之内预装载程序 230 将有一个具体内容、大小，和地点。因此，由散列获得散列值的机器指令包括在预装载程序230 之内总是保持同样的，只要预装载程序230不用未许可的代码修改或替换。在较佳的实施例，SHA-1 单程散列算法被应用散列预装载程序。作为选择，MD5 散列算法能替换使用，并且那些已知平常技术被意识到另外散列算法能被使用。使用的散列算法是包括的在引导代码212 的机器指令之内。

并且包括在引导代码212 之内是为预装载程序230的期望的散列值的一个被存储的散列值，和一个对称密钥。步骤254 从引导代码装载被存放的散列值。在引导代码212的机器指令比较从引导代码被存放的散列值与在步骤252 预装

载程序230刚才确定的散列值。比较决定步骤256 确定是否被存放的散列值与被确定的实际散列值是相等的。如果不是，在引导代码212机器指令实现步骤258，它停止游戏控制台102 的起动过程。因此，如果不同的ROM 替代原始的ROM它将是明显的，并且新替代的或未许可的ROM 不包括的一个相同的以单程散列算法生产期望的散列值的预装载程序部份，选择步骤256 将查出对预装载程序230 的修改和将终止起动过程。

假设被存放的期望的散列值与确定的实际散列值是相等的，步骤260 执行包括预装载程序代码部份ROM 210的机器指令。这步能被实施，因为预装载程序机器指令与最初包括在ROM由它的制造商被安装在游戏控制台之内预装载程序代码是相同的是明显的。

其次，步骤262 提供为整个ROM 210确定一个散列值，除了数字签名234。预装载程序也包括为确定一个单程散列值的机器指令和又更适于使用SHA-1 或MD5 散列算法(或其它已知的单程散列算法的当中一个) 确定大多数ROM 210内容的散列值 (数字签名不是包括在散列的ROM210的内容之中)。只要使用同样散列算法，结果应该总是相同除非机器指令被改变或用未授权的机器指令替换。改变甚至散列在ROM 210 里机器指令的个别位将极大地改变散列值的结果。

在ROM 210 里的公开密钥231被运用到数字签名234，在步骤264 产生对应的值为数字签名。(在公开密钥能应用之前，它用存放在MCP 的引导代码的对称密钥解码，但这步骤不是必需的如果公开密钥不用对称密钥编码。)其次，在预装载程序230的机器指令确定是否公开密钥能核实在图4选择步骤266的署名；这步骤确定是否步骤264的值等于在步骤262ROM 被确定的值。如果不，步骤268 停止起动操作因为当ROM 的原始的内容被产生，在ROM的签名被改变将是明显的。如众所周知的，如果签名值最初使用只有游戏控制台的制造商知道的私用密钥签字，署名的有效性能使用一个公开密钥被证实。如果某人破解游戏控制台100 和试图修改任一个ROM 210 的部份，在散列值上的变化将被查出在选择步骤266，导致在步骤268起动过程被终止。相反地，如果数字签名匹配ROM 的散列，ROM 内容与被授权的原始的内容是相同的将是明显的。

假设在步骤264从数字签名被确定值核实在选择步骤266ROM 的散列，步骤270 使能起动去完成，使能内核238 被复制入RAM 206 和然后被解压和未加密到RAM。预装载程序230 包括为解码起动装载程序的机器指令。在固

件引导代码的对称密钥被保持在 MCP 与在 ROM 210 里的对称密钥 236 结合产生用于为解码起动装载程序与在预装载程序机器指令一致的一个新对称代码。

起动装载程序包括为实施压缩和被编成密码的内核的流密码解密的机器指令，与RC4 流密码算法符合，如同已知的众所周知的平常技术。机器指令组成内核被解压并且解码到RAM 206然后 能由CPU 202执行实现游戏控制台的全功能，确保，举例来说，它唯一装载授权游戏软件，执行阻碍复制录影DVDs 的算法，并且确保，执行由游戏控制台的制造商渴望的所有其它政策和功能，如由授权起动代码定义。

虽然本发明被描述了与实践它的更佳的形式的关系，那些已知的普通的技巧可以明白在随后的要求的范围之内许多改动能做。因此，一般不打算以任何方式被上述的描述限制发明的范围，但是完全参考下述的权利要求替换决定。

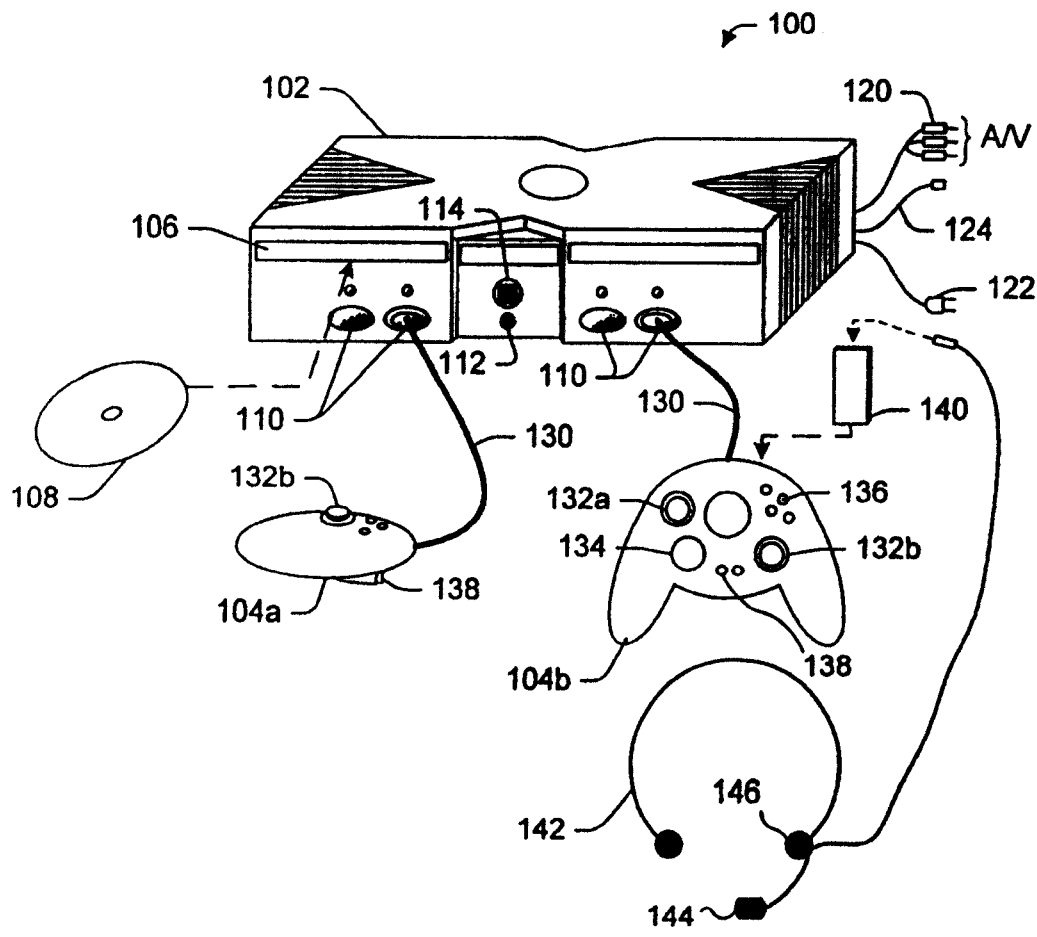


图 1

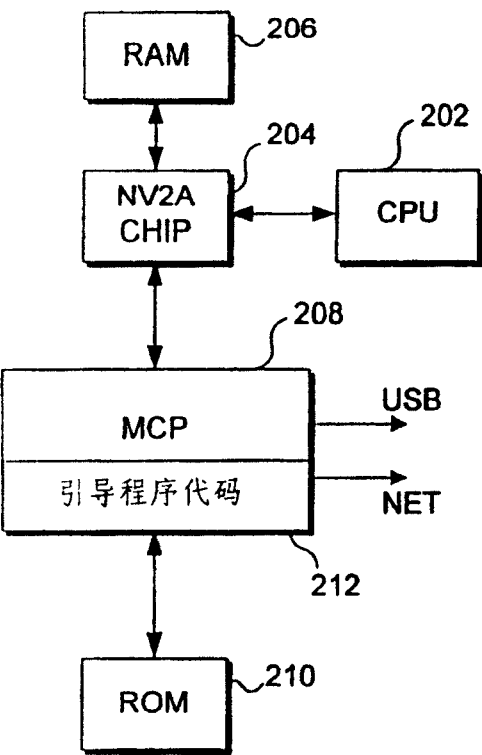


图 2A

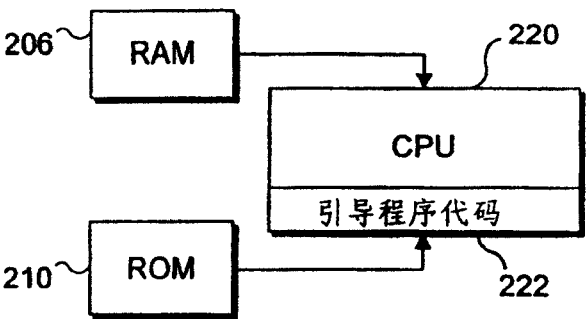


图 2B

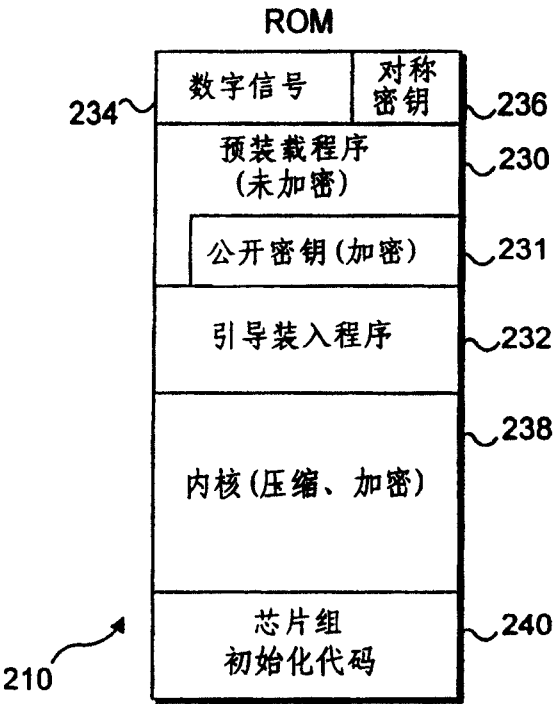


图 3

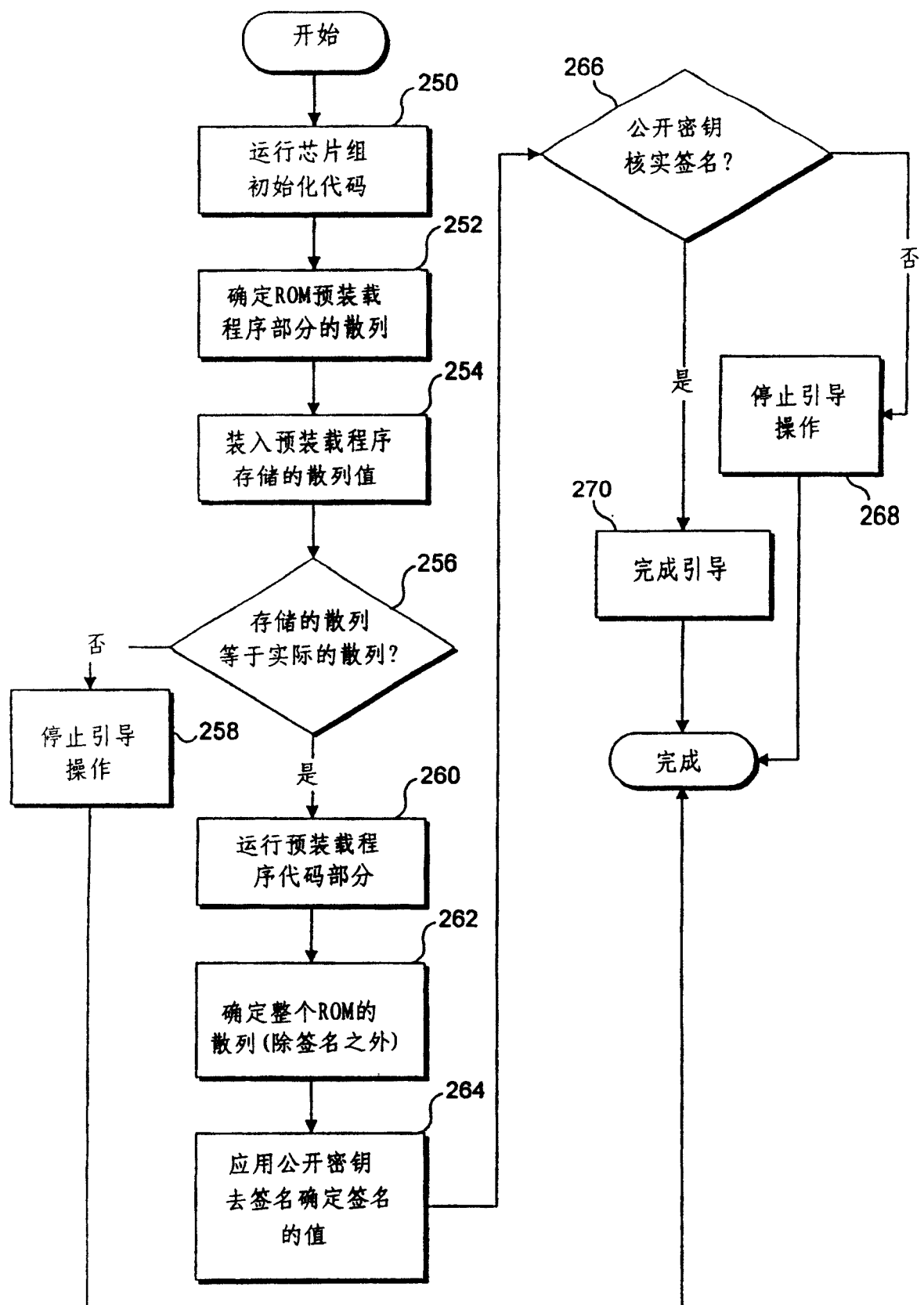


图 4