



(12) 发明专利

(10) 授权公告号 CN 1647444 B

(45) 授权公告日 2012.03.21

(21) 申请号 03808452.X

(51) Int. Cl.

(22) 申请日 2003.03.31

H04L 9/00 (2006.01)

G06F 11/30 (2006.01)

(30) 优先权数据

10/123,923 2002.04.16 US

(56) 对比文件

(85) PCT申请进入国家阶段日

2004.10.15

CN 1309487 A, 2001.08.22, 全文.

CN 1249589 A, 2000.04.05, 全文.

(86) PCT申请的申请数据

PCT/US2003/009935 2003.03.31

US 6292569 B1, 2001.09.18, 摘要、说明书第6栏第37-44行、第11栏第53-67行、第12栏第43-54行、第14栏第57-65行、第16栏第63-65行、图10C、图13.

(87) PCT申请的公布数据

W02003/090404 EN 2003.10.30

US 5956408 A, 1999.09.21, 摘要、说明书第6栏第24行 - 第7栏第36行、图1-5.

(73) 专利权人 美国索尼电脑娱乐公司

审查员 陈昇

地址 美国加利福尼亚州

(72) 发明人 W·M·麦卡罗尔

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 徐谦 刘杰

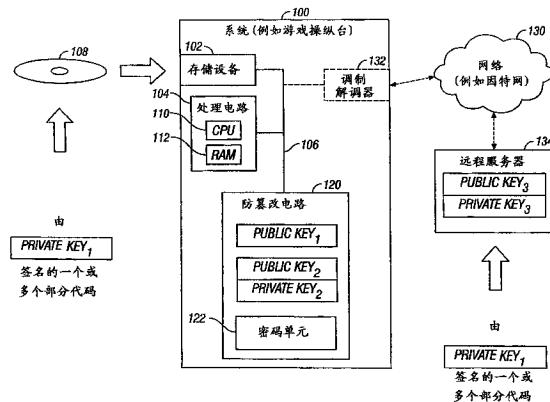
权利要求书 2 页 说明书 8 页 附图 8 页

(54) 发明名称

用于使用防止篡改硬件以提供复制保护和在线安全的方法和系统

(57) 摘要

系统(100)包括相关的防篡改电路(120)，该电路包含密码单元(122)和一个或多个密钥。该系统接收具有一个或多个部分代码的软件(108)，在由系统(202)接收该代码之前已经对代码进行数字签名。包含在防篡改电路中的密码单元和密钥之一被用于解密一部分代码的签名文件。通过使用解密的签名文件来确定这一部分代码的有效性，并且如果由系统接收的这一部分代码、如通信协议，也可在系统接收代码之前被加密。该系统通过安全的通信信道从远程服务器(134)获得密钥，并使用该密钥和包含在防篡改电路中的密码单元来解密该通信协议。然后该系统使用通信协议通过网络(130)与其他客户机通信，如玩在线游戏。



1. 一种操作系统的方法,包括以下步骤 :

从系统中的存储设备读取一部分软件代码,其中这一部分软件代码在输入系统之前已经用第一密钥进行了数字签名;

将这一部分软件代码发送给包含在与系统有关的防篡改电路中的密码单元;

利用密码单元使用在防篡改电路中存储的第二密钥来解密对应于这一部分软件代码的签名文件,以形成解密的签名文件;

通过使用解密的签名文件确定这一部分软件代码是否有效;

如果这一部分软件代码无效,则阻止系统的操作;

通过网络从服务器接收第三密钥;

从系统中的存储设备读取一部分加密的代码;

利用密码单元使用第三密钥解密这一部分加密的代码。

2. 根据权利要求 1 的方法,其中防篡改电路包括在系统中硬布线的内部防篡改电路。

3. 根据权利要求 1 的方法,其中防篡改电路包括外部防篡改电路。

4. 根据权利要求 1 的方法,其中防篡改电路包括类卡式可移动防篡改电路,所述类卡式可移动防篡改电路包括单板闪存 (170)。

5. 根据权利要求 4 的方法,其中确定这一部分软件代码是否有效的步骤包括以下步骤:

将这一部分软件代码哈希计算为第一消息摘要;

用解密的签名文件形成第二消息摘要;

比较第一消息摘要和第二消息摘要;和

如果第一消息摘要和第二消息摘要不匹配,则指示这一部分软件代码是无效的。

6. 根据权利要求 4 的方法,其中存储设备包括在其中存储有软件代码的可移动计算机可读介质。

7. 根据权利要求 4 的方法,其中存储设备包括在其中存储有软件代码的硬盘驱动器。

8. 根据权利要求 4 的方法,还包括步骤:

在系统接收该软件代码之前,用第一密钥至少对这一部分软件代码进行数字签名。

9. 根据权利要求 4 的方法,还包括以下步骤:

从系统中的存储设备读取一个或多个附加的软件代码部分,每个附加的软件代码部分在输入到系统之前已经使用第一密钥进行了数字签名;

利用密码单元使用第二密钥解密对应于一个或多个附加的软件代码部分的签名文件;和

如果任何一个或多个附加的软件代码部分是无效的,则阻止系统的操作。

10. 根据权利要求 4 的方法,其中这一部分加密的代码包括设置成用于通过网络进行通信的通信协议。

11. 根据权利要求 10 的方法,还包括步骤:

使用通信协议通过网络进行通信。

12. 根据权利要求 4 的方法,还包括以下步骤:

在接收第三密钥的步骤之前通过网络与服务器建立安全的通信信道;和

通过该安全的通信信道从服务器接收第三密钥。

13. 一种基于处理器的系统,包括:

用于从系统中的存储设备读取一部分软件代码的装置,其中这一部分软件代码在输入系统之前已经用第一密钥进行了数字签名;

用于将这一部分软件代码发送给包含在与系统有关的防篡改电路中的密码单元的装置;

用于利用密码单元使用在防篡改电路中存储的第二密钥来解密对应于这一部分软件代码的签名文件,以形成解密的签名文件的装置;

用于通过使用解密的签名文件确定这一部分软件代码是否有效的装置;

用于如果这一部分软件代码无效,则阻止系统的操作的装置;

用于通过网络从服务器接收第三密钥的装置;

用于从系统中的存储设备读取一部分加密的代码的装置;

用于利用密码单元使用第三密钥解密这一部分加密的代码的装置。

14. 根据权利要求 13 的基于处理器的系统,其中防篡改电路包括在系统中硬布线的内部防篡改电路。

15. 根据权利要求 13 的基于处理器的系统,其中防篡改电路包括外部防篡改电路。

16. 根据权利要求 13 的基于处理器的系统,其中防篡改电路包括类卡式可移动防篡改电路,所述类卡式可移动防篡改电路包括单板闪存 (170)。

17. 根据权利要求 16 的基于处理器的系统,其中用于确定这一部分软件代码是否有效的装置包括:

用于将这一部分软件代码哈希计算为第一消息摘要的装置;

用于用解密的签名文件形成第二消息摘要的装置;

用于比较第一消息摘要和第二消息摘要的装置;和

用于如果第一消息摘要和第二消息摘要不匹配,则指示这一部分软件代码是无效的的装置。

18. 根据权利要求 16 的基于处理器的系统,其中存储设备包括在其中存储有软件代码的可移动计算机可读介质。

19. 根据权利要求 16 的基于处理器的系统,其中存储设备包括在其中存储有软件代码的硬盘驱动器。

20. 根据权利要求 16 的基于处理器的系统,还包括:

用于从系统中的存储设备读取一个或多个附加的软件代码部分的装置,每个附加的软件代码部分在输入到系统之前已经使用第一密钥进行了数字签名;

用于利用密码单元使用第二密钥解密对应于一个或多个附加的软件代码部分的签名文件的装置;和

用于如果任何一个或多个附加的软件代码部分是无效的,则阻止系统的操作的装置。

21. 根据权利要求 16 的基于处理器的系统,其中这一部分加密的代码包括设置用于通过网络进行通信的通信协议。

22. 根据权利要求 21 的基于处理器的系统,还包括:

用于使用通信协议通过网络进行通信的装置。

用于使用防止篡改硬件以提供 复制保护和在线安全的方 法和系统

[0001] 发明背景

[0002] 1. 发明领域

[0003] 本发明总体上涉及软件复制保护和用于保护通信协议的方案,尤其涉及防篡改硬件密码电路的使用以确保复制保护的完整性并保护在在线通信使用的通信协议消息和结构、如在线游戏中。

[0004] 2. 相关技术的讨论

[0005] 计算机娱乐游戏系统,如 Sony 的 PlayStation® 和 PlayStation 2 在最近几年已经变成最成功的消费者电子产品中的一部分占满了货架。不幸的是,伴随着这些成功,潜在的增加了希望不适当篡改系统和相关软件的用户的滥用。一些人的以特定方式修改特定游戏以实现特殊或不平常的结果,甚至可能从该修改软件的销售和 / 或分发中非法获益的歪曲思想驱使了该滥用。明显的,游戏出版者主要关心的一个问题是他们软件的盗版,因为这种修改可以导致在公众中软件版本不相容的循环,这能引起混乱并甚至损害游戏出版者的信誉和诚信。

[0006] 同样潜在地存在有关在线或网络启动游戏系统的滥用。例如,电脑黑客或恶作剧者可以执行所谓的“中间人 (man in the middle)”攻击,借此黑客试图截取在两个游戏系统之间通过网络 (例如因特网) 传输的消息。黑客的动机可能是希望欺骗或破坏两个合法用户的游戏。再者,该滥用能不利地引起混乱和无辜用户中的严重破坏,最终导致公众对系统和游戏本身产生不合理的不信任。

[0007] 本发明涉及有关这些和其他背景信息因素。

[0008] 发明概述

[0009] 本发明通过提出一种操作系统的办法,有利地处理了上述需要和其他需要。该方法包括以下步骤:从系统的存储设备中读取一部分软件代码,其中这一部分软件代码在输入系统之前已经用第一密钥进行数字签名;将这一部分软件代码发送给包含在与系统有关的防篡改电路中的密码单元;使用在防篡改电路中存储的第二密钥,利用密码单元解密对应于这一部分软件代码的签名文件以形成解密的签名文件;通过使用解密的签名文件,确定这一部分软件代码是否有效;并且如果这一部分软件代码无效则阻止系统操作。

[0010] 在另一实施例中,本发明被特征化为基于处理器的系统,该系统包括存储设备、防篡改电路、包含在防篡改电路中的密码单元和处理电路。配置该处理电路以从存储设备中读取一部分软件代码,这一部分软件代码在输入系统之前已经用第一密钥进行数字签名,并且发送这一部分软件代码给密码单元。配置该密码单元以使用在防篡改电路中存储的第二密钥来解密对应于这一部分软件代码的签名文件,并且确定这一部分软件代码是否有效。进一步配置该处理电路以在这一部分软件代码无效时,阻止系统的操作。

[0011] 在另一实施例中,操作系统的方法包括以下步骤:通过网络从服务器接收系统中的第一密钥;从系统中的存储设备中读取一部分加密的代码;将这一部分加密的代码发送

给包含在与系统有关的防篡改电路中的密码单元；利用密码单元使用第一密钥解密这一部分加密的代码以形成解密的代码；并且使用解密的代码通过网络进行通信。

[0012] 在另一实施例中，基于处理器的系统包括存储设备、防篡改电路、包含在防篡改电路中的密码单元和处理电路。配置该处理电路以通过网络从服务器接收第一密钥，从存储设备中读取一部分加密代码，发送这一部分加密代码给密码单元。配置该密码单元以使用第一密钥来解密这一部分加密的代码以形成解密的代码，并且进一步配置该处理电路使用该解密的代码通过网络进行通信。

[0013] 通过参考下面的本发明的详细描述和附图能更好的理解本发明的优点和特征，该附图阐明了其中使用本发明原理的说明性实施例。

[0014] 附图概述

[0015] 从下面更加详细的描述并结合下列附图，本发明的上述和其他方面、特征和优点将更加明显，其中：

[0016] 图 1 是描述根据本发明的一个实施例的系统的框图；

[0017] 图 2A 和 2B 是描述可用于操作图 1 所示的系统的根据本发明实施例的典型方法的流程图；

[0018] 图 3 是描述根据本发明另一实施例的系统的框图；

[0019] 图 4A 和 4B 是描述可用于操作图 3 所示的系统的根据本发明实施例的典型方法的流程图；

[0020] 图 5A、5B 和 5C 是描述图 1 和 3 所示的系统的替换配置的框图；和

[0021] 图 6 是描述根据本发明实施例的掌控过程的流程图。

[0022] 相应的参考字符表示贯穿若干视图的相应部分。

[0023] 本发明的详细描述

[0024] 参考图 1，描述了根据本发明实施例的系统 100。该系统 100 可以包括游戏系统或操纵台，如过去、现在或将来版本的流行的 Sony PlayStation[®]，或其他类型的计算机系统、处理系统、游戏系统以及包括一个或多个在此描述的特征的系统等。该系统 100 能使用当前可用的商业密码算法以减少盗版或逆向操作 (reverse engineering) 的威胁。以这样的方式使用当前的复制保护技术，以便通过使用数字签名核查软件的完整性。

[0025] 该系统 100 典型地包括存储设备 102 和通过主要系统总线 106 互连的处理电路 104。该存储设备 102 可包括任何类型的存储设备，该存储设备具有可移动计算机可读介质 108，如数字通用盘 (DVD) 驱动器、光盘 (CD) 驱动器，任何其它类型的光盘驱动器、任何类型的高容量磁盘驱动器，如 Iomega 公司的 Zip[®] 驱动器，等等。该存储设备 102 可选择地包括具有可移动计算机可读介质 108 的 SonyMagicGate[™] 或 Memory Stick[®] 介质插槽，该计算机可读介质包括 MagicGate[™] 或 Memory Stick[®] 介质。如下面将要讨论，该存储设备 102 可选择地包括硬盘驱动器。该处理电路 104 可包括中央处理单元 (CPU) 110 和随机存取存储器 (RAM) 112。

[0026] 根据本发明，该系统 100 也包括防篡改电路 120。防篡改电路是一种典型的电路，当一些人试图修改或篡改它时，其摧毁自身。典型地耦合到系统总线 106 的防篡改电路 120

可包括任何类型的防篡改电路，如那些在智能卡技术中 用于数字现金交易的当前可利用的防篡改电路。在系统 100 的该实施例中，该防篡改电路 120 包括在系统 100 操纵台自身内硬布线的内部防篡改电路。然而，如下所讨论，该防篡改电路 120 能选择地作为外部或“附加”部件实现，如存储卡或 PCMCIA 卡，并且甚至可包括附加功能。

[0027] 该防篡改电路 120 优选地包括密码单元 122。该密码（或“保密”）单元 122 可包括专用于加密和解密的处理器或其它电路。通过使保密单元 122 包含在防篡改外壳 120 中，用于实际解密的算法十分安全地被保存。

[0028] 该系统 100 使用在防篡改电路 120 中的密码单元 122 以通过使用利用公共 / 私有密钥加密技术的数字签名，来确保复制保护的完整性和系统软件的机器代码的完整性。公共 / 私有密钥加密技术是公知的使用一对密钥（号码串）进行加密的非对称方案。即，该公共密钥加密数据，并且对应的私有或“秘密”密钥解密它。对于数字签名，该过程相反。即，发送者使用私钥以产生能被拥有对应的公钥的任何人读取的唯一电子数，该公钥校验来自发送者的信息是正确的。因此，该用户发布公钥给公众，公众能使用它加密将发送给用户的消息并用于解密用户的数字签名。该用户秘密地保存私钥，并使用它加密数字签名和解密接收的消息。该数字签名方案是优选地用在本发明的第一方面中的技术。

[0029] 因此，根据本发明的一个实施例，公钥 PUBLIC KEY₁ 和公共 / 私有密钥对 PUBLIC KEY₂/PRIVATE KEY₂ 也被包含于或存储在防篡改电路 120 中。该密钥 PUBLIC KEY₁ 必须是用于所有系统单元的相同密钥，该系统单元由意图使用由密钥 PRIVATE KEY₁ 掌控的介质的任何特定生产商分配（下面描述）。该密钥对 PUBLIC KEY₂/PRIVATE KEY₂ 最好是用于每个系统单元的唯一密钥对，但这仍旧不是必须的。因为这些密钥被封装在防篡改外壳 120 中，对于每个人，包括用户和游戏开发者本人是看不见的。这减小了在游戏开发公司内部人员泄露密钥给外部的可能性。而且，该防篡改电路 120 可包括附加密钥或密钥对，以防一个密钥的安全性被破坏。

[0030] 图 2A 描述了用于操作系统 100 的根据本发明的一个实施例的方法 200。该方法 200 对于校验在系统 100 中使用的软件的复制保护是有用的。在介质（例如，磁盘）108 被插入到系统 100 中之前，用密钥、如 PRIVATE KEY₁ 对用于游戏的至少一部分软件代码进行数字签名（图 1）。例如，当游戏由生产商掌控时，可以使用仅仅生产商知道的密钥 PRIVATE KEY₁ 对软件代码的关键部分进 行数字签名。通过范例，可以被签名的一部分代码是：磁盘的内容表、应用本身、可执行的文件、引导基本输入输出系统（boot bios）和任何其他不应当被第三方修改的敏感数据。

[0031] 尽管也可以使用唯一的密钥对磁盘 108 的内容进行加密，但签名应用能校验签名数据的完整性。即使黑客改变了磁盘 108 本身的内容，黑客也不能正确地产生用于新代码的有效签名，因为需要生产商私钥来做这些。

[0032] 在步骤 202，包括数字签名部分代码的软件代码由系统 100 接收。通过范例，通过用户将磁盘 108 插入到存储设备 102 中，或通过从网络下载该代码并将代码存储在存储设备上，可以由系统 100 接收软件代码（下面描述）。在系统 100 接收代码后，控制进行到步骤 204，在此处理电路 104 从存储设备 102 读取一部分软件代码。被读取的这一部分软件代码最好是在代码输入到系统 100 之前已经用 PRIVATE KEY₁ 进行数字签名的一部分代码。在步骤 206 中，该处理电路 104 发送这一部分软件代码给包含在防篡改电路 120 中的密码

单元 122。例如,如果这一部分软件代码是内容表,则该系统 100 从磁盘 108 中读取内容表并将它发送给密码单元 122。

[0033] 在步骤 208,该密码单元 122 使用在防篡改电路 120 中存储的 PUBLIC KEY₁ 来解密对应于这一部分软件代码的签名文件。该密钥 PUBLIC KEY₁ 典型地是生产商公钥,并如上所述,它可以与系统单元的实际数量相同。在步骤 210,该密码单元 122 使用解密的签名文件以确定这一部分软件代码是否有效。如步骤 212 所示,如果这一部分软件代码有效,则系统 100 的操作如步骤 214 所示那样正常继续。另一方面,如果这一部分软件代码无效,如步骤 216 所示,阻止系统 100 的操作。通过范例,通过阻止系统 100 的引导处理可以阻止系统 100 的操作。因此,在代码是无效的情况下,该系统 100 操纵台将试图加载修改的磁盘 108,发现签名是无效的,并拒绝引导该磁盘 108。这样,如果一些人试图修改磁盘 108 上的软件,该软件将不在系统 100 中运行。

[0034] 图 2B 描述了根据本发明的一个实施例用于执行步骤 210(图 2A)、即确定这一部分软件代码是否是有效的典型方法。尤其是,在步骤 220,该密码单元 122 将这一部分软件代码哈希计算(hash)为第一消息摘要。即,如果这一部分软件代码包括内容表,则该密码单元 122 将内容表哈希计算为第一消息摘要。在步骤 222,该密码单元 122 使用来自这一部分软件代码中的解密的签名文件来形成第二消息摘要。在步骤 224,该密码单元 122 比较第一消息摘要和第二消息摘要。如步骤 226 所示,如果第一消息摘要与第二消息摘要匹配,则在步骤 228,密码单元 122 表示这一部分代码是有效的。另一方面,如果两个摘要不匹配,则在步骤 230 该密码单元 122 表示这一部分代码是无效的。换句话说,如果两个摘要匹配,则能证实这一部分代码,如内容表,自从被生产者数字签名后没有被修改,并且因此允许继续该引导过程。

[0035] 对于一个或多个软件代码的附加部分,可以重复上述过程。即,从存储设备 102 中读取一个或多个软件代码的附加部分,每个部分代码在输入到存储设备 102 之前已经用密钥 PRIVATE KEY₁ 进行过数字签名。利用密码单元 122 使用该密钥 PUBLIC KEY₁ 解密对应于一个或多个软件代码的附加部分的签名文件,并且如果任何一个或多个软件代码的附加部分是无效的,则阻止系统 100 的操作。

[0036] 例如,无论何时从磁盘 108 中加载可执行文件,在处理电路 104 中的加载器发送可执行文件给密码单元 122 以校验该文件是否有效。该密码单元 122 将可执行文件哈希计算为消息摘要并使用生产商的公共密钥、如 PUBLIC KEY₁ 来解密对应的签名文件。该密码单元 122 比较产生的消息摘要与解密的摘要,并且如果摘要匹配,则能证实该可执行文件自从被生产者签名以来没有被修改,并且允许引导过程继续。如果摘要不匹配,则该可执行文件自从被生产者签名以来已经被修改,并且阻止系统 100 的操作,如通过阻止引导过程继续。每次可执行部分代码被加载时比较签名文件有助于保护“交换手段(swaptrick)”类型的复制保护失败。这是由于为了真实性,已经被数字签名的可执行代码的每个比特必须被检查。

[0037] 因此,上述过程与基于传统软件的密码系统相比具有显著优点。即,如果用于解密加密的数据的密钥存储在磁盘上,这意味着它能被一些人利用工具对在磁盘上发现的源代码进行反汇编而发现。然而,由于密钥安全的藏在防篡改硬件 120 中,这大大地减小了密钥被偷取的可能性。

[0038] 再次参考图 1, 上面已经描述了该存储设备 102 可选择地包括硬盘驱动器。在该情况下, 用于游戏或其他应用的软件代码可以从网络 130、如因特网或 America Online[®] 网络下载到系统 100 中。下载的软件将存储在硬盘驱动器 102 上。通过在系统 100 中包括耦合到系统总线 106 的调制解调器 132, 可以执行该下载。因为调制解调器 132 以及产生的到网络 130 的连接是本发明实施例中的可选特征, 它们用虚线示出。

[0039] 如果使用到系统 100 的软件下载, 则已经用密钥 PRIVATE KEY₁ 进行数字签名的一个或多个软件部分代码能被加载到远程服务器 134 上。或者, 该远程服务器 134 能实际执行该代码的数字签名过程。可以以与上面关于磁盘 108 所描述的相同的方式对该软件进行数字签名。然后该软件从远程服务器 134, 经过网络 130, 通过调制解调器 132 传送到系统 100, 它被存储在硬盘驱动器 102 中。如果希望, 可在下载软件之前建立系统 100 和远程服务器 134 之间的安全的通信信道。如本领域中公知的那样, 通过交换系统 100 的 PUBLIC KEY₂ 和远程服务器 134 的 PUBLIC KEY₃ 可建立安全的通信信道。而且, 通过使用数字证书, 该安全的通信信道能被进一步强化, 该数字证书对从因特网下载的软件来自正规源来说是一种担保。数字证书提供有关软件的信息, 诸如作者的身份和带有证书授权 (CA, Certificate Authority) 的软件的日期, 同时也是防篡改的措施。然而, 数字证书的使用不是必需的。

[0040] 图 3 描述了根据本发明另一个实施例的系统 100 的操作。通过使用调制解调器 132 和用于存储设备 102 的硬盘驱动器, 该系统 100 能保持宽带连接, 允许系统 100 充当用于电子商务应用和网络游戏能力的平台的网络连接。这允许系统 100 的用户通过网络 130 与其他客户系统、如客户系统 140、142、144 的用户玩游戏。

[0041] 然而, 如上所述, 存在有关在线或网络激活的游戏系统的潜在滥用, 如所谓的“中间人”攻击。例如, 如果用于在线游戏的通信协议的格式包含在游戏盘 108 本身中, 没有什么能阻止黑客逆向操纵来自机器代码的格式。一旦黑客获得通信协议, 他或她将能够截取在玩游戏的两个系统之间的消息, 这能够误导或破坏玩游戏。

[0042] 图 3 中描述的本发明的实施例利用远程服务器 134 的存在。即, 为了协调在客户机之间的网络游戏, 服务器, 如远程服务器 134, 将典型地被用于处理客户机的注册 / 仲裁。根据本发明, 游戏软件中机器代码的敏感部分, 如定义通信协议的代码被加密。一旦与远程服务器 134 连接, 就通过优选地加密的信道将密钥从远程服务器 134 发送给系统 100。然后系统 100 使用该密钥以解码通信协议格式。这意味着在任何时候通信协议在它的未加密格式中对终端用户来说都无法得到, 这阻止了黑客获得它。因此, 该实施例, 系统 100 通过使用加密提供保护代码的敏感部分, 如在客户机 / 服务器在线游戏中使用的通信协议消息和结构。

[0043] 图 4A 描述了操作根据图 3 描述的本发明实施例的系统 100 的方法 400。在介质 (如, 磁盘) 108 插入到系统 100 中之前, 存储在磁盘 108 上的至少一部分代码被加密。被加密的部分代码最好包括用于发生在在线游戏中的通信的通信协议。使用的加密类型可以包括任何类型的加密, 如, 例如公共 / 私有密钥加密技术的非对称方案, 或对称方案。

[0044] 在步骤 402, 系统 100 接收包括加密部分的代码。可以通过在存储设备中接收磁盘 108 来接收代码, 或通过调制解调器 132 接收代码并将其存储在硬盘驱动器中。在步骤 404, 该系统 100 通过网络 130 建立与远程服务器 134 的通信。该远程服务器 134 典型地包括处理网络游戏用户机的注册 / 仲裁的服务器。在步骤 406 中, 该系统 100 通过网络 130

从远程服务器 134 中接收密钥,例如 KEY₄。通过图 3 中的箭头 136 表示该接收。密钥 KEY₄ 可以包括任何类型的密钥。例如,如果非对称方案用于加密通信协议,则密钥 KEY₄ 可以包括公钥,或如果对称方案用于加密通信协议,则 KEY₄ 可以包括简单的对称密钥。

[0045] 在步骤 408,该处理电路 104 从存储设备 102 中读取一部分加密代码,并且在步骤 410 中,该处理电路 104 发送这一部分加密代码给包含在防篡改电路 120 中的密码单元 122。在步骤 412,该密码单元 122 使用从远程服务器 134 接收的密钥、在该情况下是 KEY₄ 来解密这一部分加密的代码。解密的通信协议消息格式被存储在存储器、如 RAM112 中。最后,在步骤 414,该系统 100 使用解密的通信协议开始安全通信。即,系统 100 使用解密的通信协议用于通过网络 130 进行通信,从而与其它系统、如图 3 中通过箭头 138 所示的系统 140 一起玩游戏。

[0046] 图 4B 描述了根据本发明的一个实施例的用于执行步骤 404、即建立与远程服务器 134 的通信的步骤的典型方法。该方法使用存储在系统 100 的防篡改电路 120 中的公共 / 私有密钥对 PUBLIC KEY₂/PRIVATE KEY₂ 和存储在远程服务器 134 中的公共 / 私有密钥对 PUBLIC KEY₃/PRIVATE KEY₃ 来建立在系统 100 和远程服务器 134 之间的安全的通信信道。尤其是,在步骤 420,系统 100 发送它的 PUBLIC KEY₂ 给远程服务器 134,并且在步骤 422,该系统 100 从远程 服务器 134 接收 PUBLIC KEY₃。该系统 100 和该服务器 134 使用这些密钥协商安全信道,这在本领域中是公知的。在步骤 424,该系统 100 和远程服务器 134 实施安全通信,并根据上述步骤 406,系统 100 通过安全的通信信道从远程服务器 134 接收密钥 KEY₄。

[0047] 作为本发明的选择性特征,该远程眼务器 134,或一些其他服务器,可以充当认证中心 (CA)。该认证中心具有每个系统、如系统 100、140、142、144 的序列号的列表,该序列号常常由生产商产生。该认证中心也可存储用于所有系统的唯一的公钥。当一个系统连接到该认证中心时,该认证中心可请求系统的序列号,并通过它的序列号肯定地识别出该系统以证实它是合法系统。在产生该肯定识别后,如果合适,该认证中心然后可以将正确的公钥发送给系统。接收到它的公钥后,于是该系统将具有与另一个系统玩在线游戏的能力。即,在两个系统玩在线游戏之前将会要求他们必须交换他们的公钥。这类可选的硬件标识 (“硬件 ID”) 将进一步阻止黑客具有干扰在线通信、如在线游戏的能力。

[0048] 因此,通过使用该方法 400(图 4A),代码的敏感部分、如通信协议消息格式对于终端用户来说是无法以它们未加密格式得到的。这意味着截取正在两个系统之间通信的消息的黑客将不能够解密它并不能用不同的消息替换该消息。理论上,如果黑客能够获得上述的数字签名,或具有直接访问运行的系统 100 上的 RAM112 的工具,他或她能够从 RAM112 中得到密钥 KEY₄。然而,与对来自在个人计算机上能被读取的磁盘的源代码进行反汇编相比,这更是相当困难的。

[0049] 上面已提到防篡改电路 120 可替换地作为外部或“附加”部件、如存储卡或 PCMCIA 卡实现。参考图 5A,描述了根据本发明另一实施例的系统 100 的一个版本,其中该防篡改电路 120 被实现为可移动的类似卡的设备,如 PC 卡或 PCMCIA 卡。在该实施例中,该防篡改电路 120 能容易地插入和移出系统 100 中的接口槽 160。该接口槽 160 将典型地耦合到系统总线 106。

[0050] 参考图 5B,描述了根据本发明另一个实施例的系统 100 的一个版本,其中该防篡

改电路 120 被实现为外部部件。该防篡改电路 120 通过电缆 164 和接口 166 耦合到系统 100。耦合到系统总线 106 的接口 166 可包括许多不同类型的接口,如通用串行总线 (USB) 或 i.LINK® (IEEE1394)。

[0051] 参考图 5C,描述了根据本发明另一个实施例的系统 100 的一个版本,其中该防篡改电路 120 被实现在如使用 Sony MagicGate™Memory Stick® 技术的小型类卡介质上。

MagicGate™Memory Stick® 介质结合 MagicGate 技术,它是创新的音乐版权保护技术。该 MagicGate™Memory Stick® 介质包括单板闪存 170 和包括加密电路 174 的 MagicGate™ 电路 172。该 MagicGate™Memory Stick® 介质通过介质槽 176 与系统 100 连接,该介质槽 176 将典型地耦合到系统总线 106。作为选择性特征,该系统 100 也可包括它自己的 MagicGate™ 电路 178,意味着根据 MagicGate 技术,系统 100 可起 MG 应用的作用。

[0052] 根据本发明的一个实施例,在 MagicGate™Memory Stick® 介质中的加密电路 174 可提供如上所述的密码单元 122 的功能。而且,在 MagicGate™Memory Stick® 介质中的单板闪存 170 可用于存储上述的密钥,即,PUBLIC KEY₁ 和 PUBLIC KEY₂/PRIVATE KEY₂。这样,该 MagicGate™Memory Stick® 介质能提供与上述防篡改电路 120 基本上相同的功能。

[0053] 该 MagicGate™Memory Stick® 介质被认为包括某个等级的防篡改保护,并且如果需要,该等级的防篡改保护可被加强用于额外的保护。而且,在系统 100 中的 MagicGate™ 电路 178,如果被包括,可根据 MagicGate 技术来使用以证明一个有效的 MagicGate™Memory Stick® 介质已经被插入到介质槽 176 中。因此,MagicGate™ 电路 178 可检测到对介质的任何篡改,这可阻止具有特殊介质的系统 100 的操作。

[0054] 应当理解该 MagicGate™Memory Stick® 介质仅仅是外部、可移动类卡式设备的一个范例,该类卡式设备可用于实现这里所述的防篡改电路 120。通过另一个范例,该防篡改电路 120 也可以实现在用于 Sony PlayStation® 2 的存储卡中。

[0055] 参考图 6,描述了根据本发明的一个实施例的掌控过程 600。该掌控过程 600 可用于产生能够利用上述方法的计算机可读介质,如 DVD 或 CD。尤其是,在步骤 602,游戏开发者产生未签名的代码并将代码刻在磁盘、例如 DVD 或 CD 上。在步骤 604,该磁盘被发送给生产商。在步骤 606,该生产商加密代码的敏感部分,如通信协议。该代码的敏感部分可由游戏开发者指定。在步骤 608,该生产商使用私钥为特定部分的代码产生数字签名。可以被数字签名的部分代码包括内容表、一个或多个可执行文件等。最后,在步骤 610,该生产商产生具有修改的数据的新的主盘。

[0056] 如上所述,系统 100 通过使用有关的防篡改电路能减小盗版和逆向操作的威胁,该防篡改电路包含密码单元和一个或多个密钥。通过使用包含在防篡改电路中的密码单元和一个或多个密钥来解密用于一部分接收的软件代码的签名文件,对于已经被不正确地修改或篡改的代码,该系统 100 的操作可被阻止。该防篡改电路显著地阻碍黑客获得用于实

际解码的密钥或算法的能力。而且，该防篡改电路可被用于阻碍黑客干扰在线通信、如在线游戏的能力。即，系统 100 接收的一个或多个部分代码、如通信协议可以在系统 100 接收代码之前被加密。该系统 100 能连接用于协调在线游戏的远程服务器，并获得由被包含在防篡改电路中的密码单元使用的密钥，以解密该通信协议。然后该系统使用通信协议通过网络与其他客户机通信，如玩在线游戏。因为黑客不能访问未加密的通信协议，黑客干扰在线游戏的能力被大大地减小。

[0057] 尽管在此公开的本发明已通过特定实施例及其应用进行描述，然而对于本领域技术人员来说在不脱离权利要求中描述的本发明范围的情况下，本发明可进行大量的修改和变化。

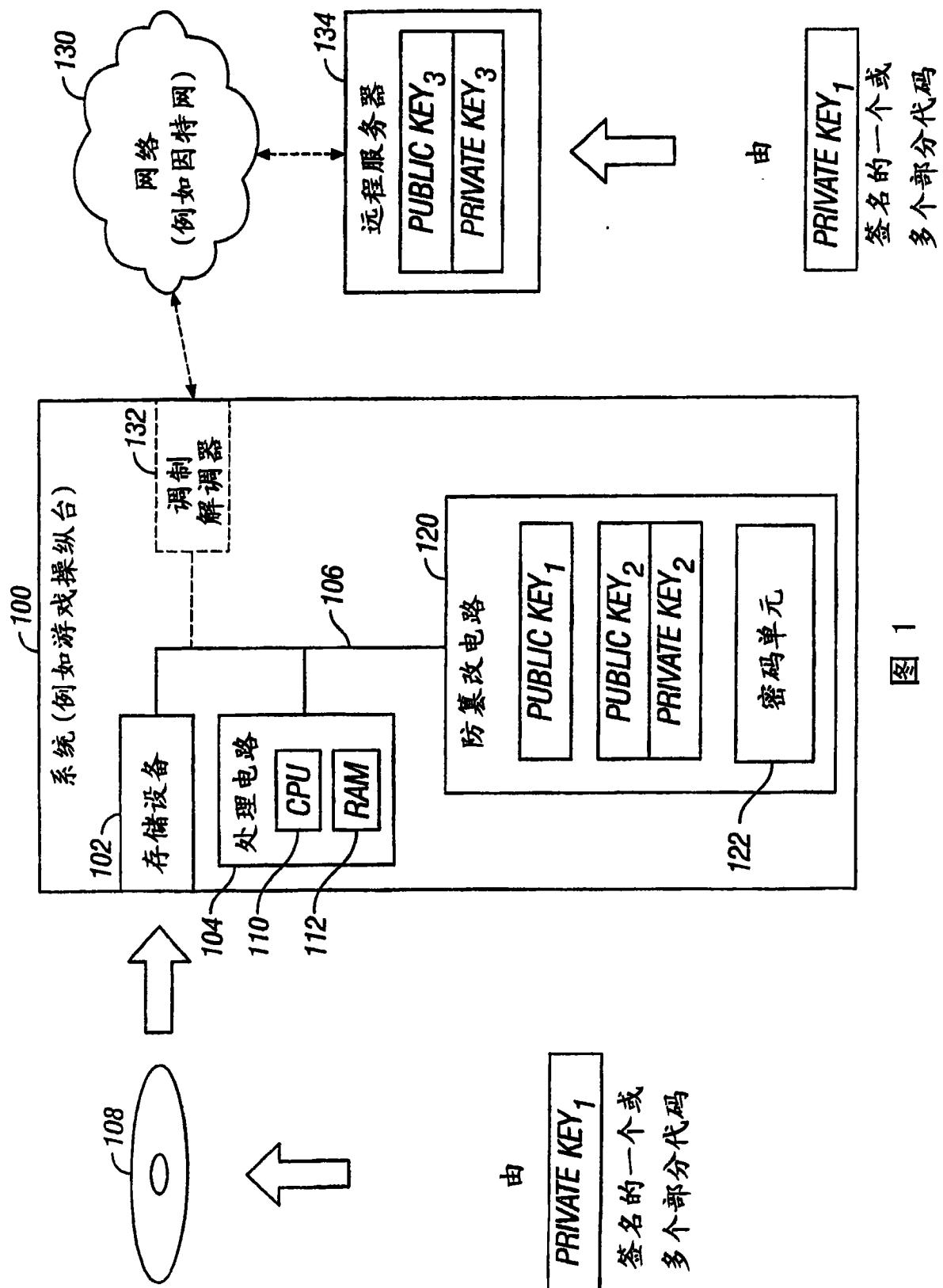


图 1

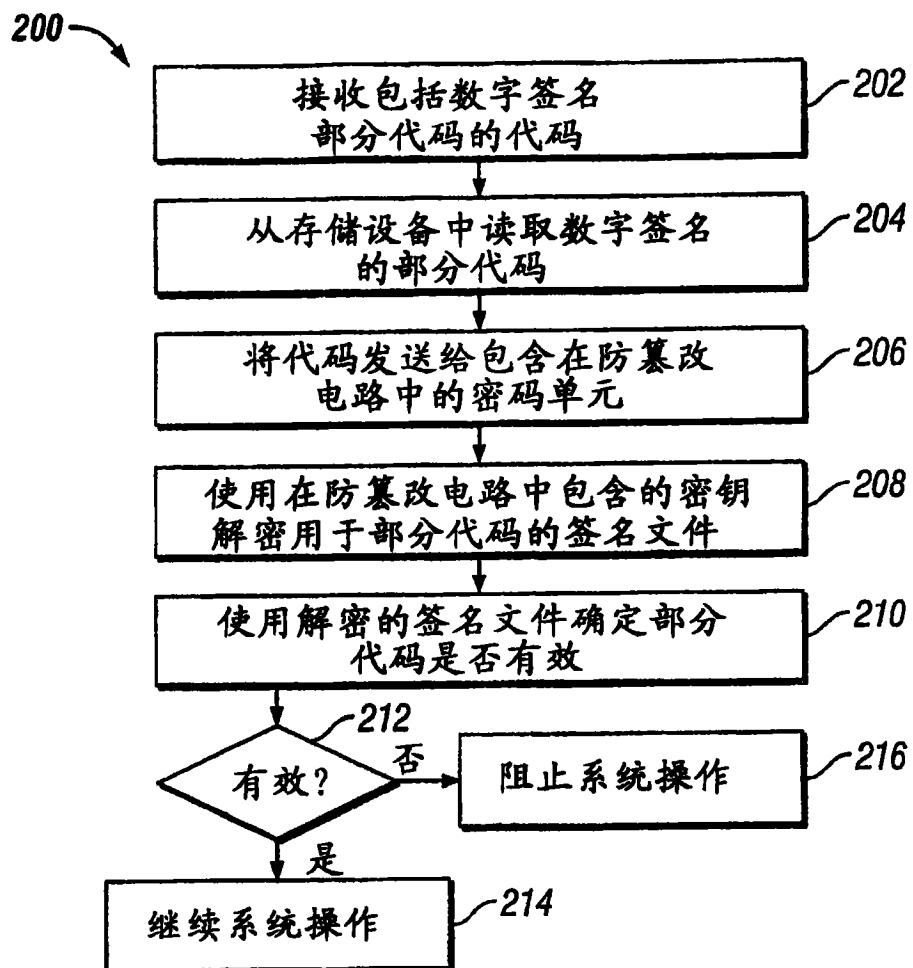


图 2A

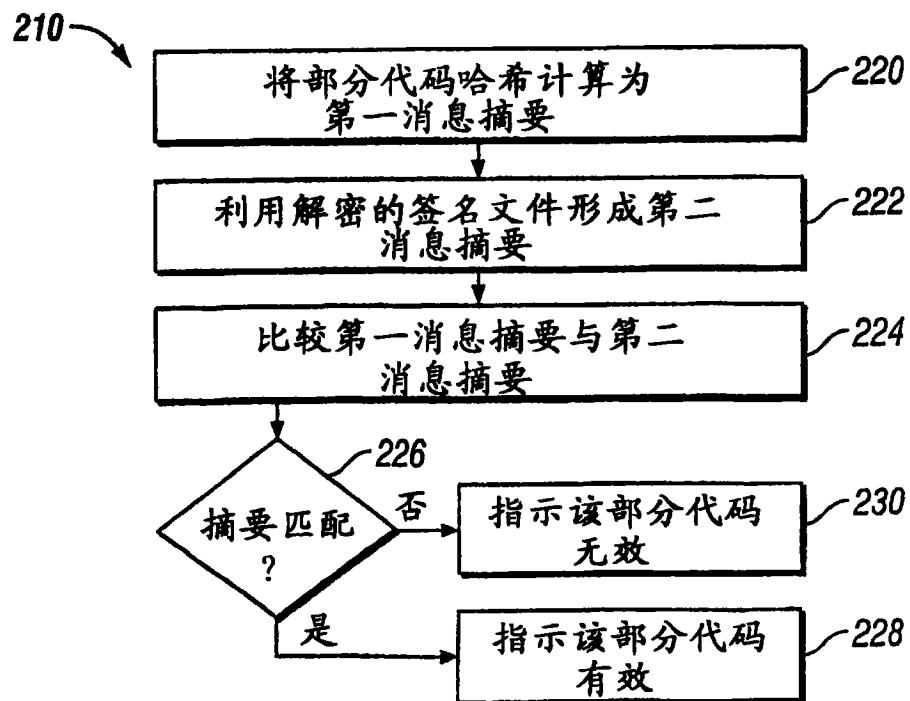


图 2B

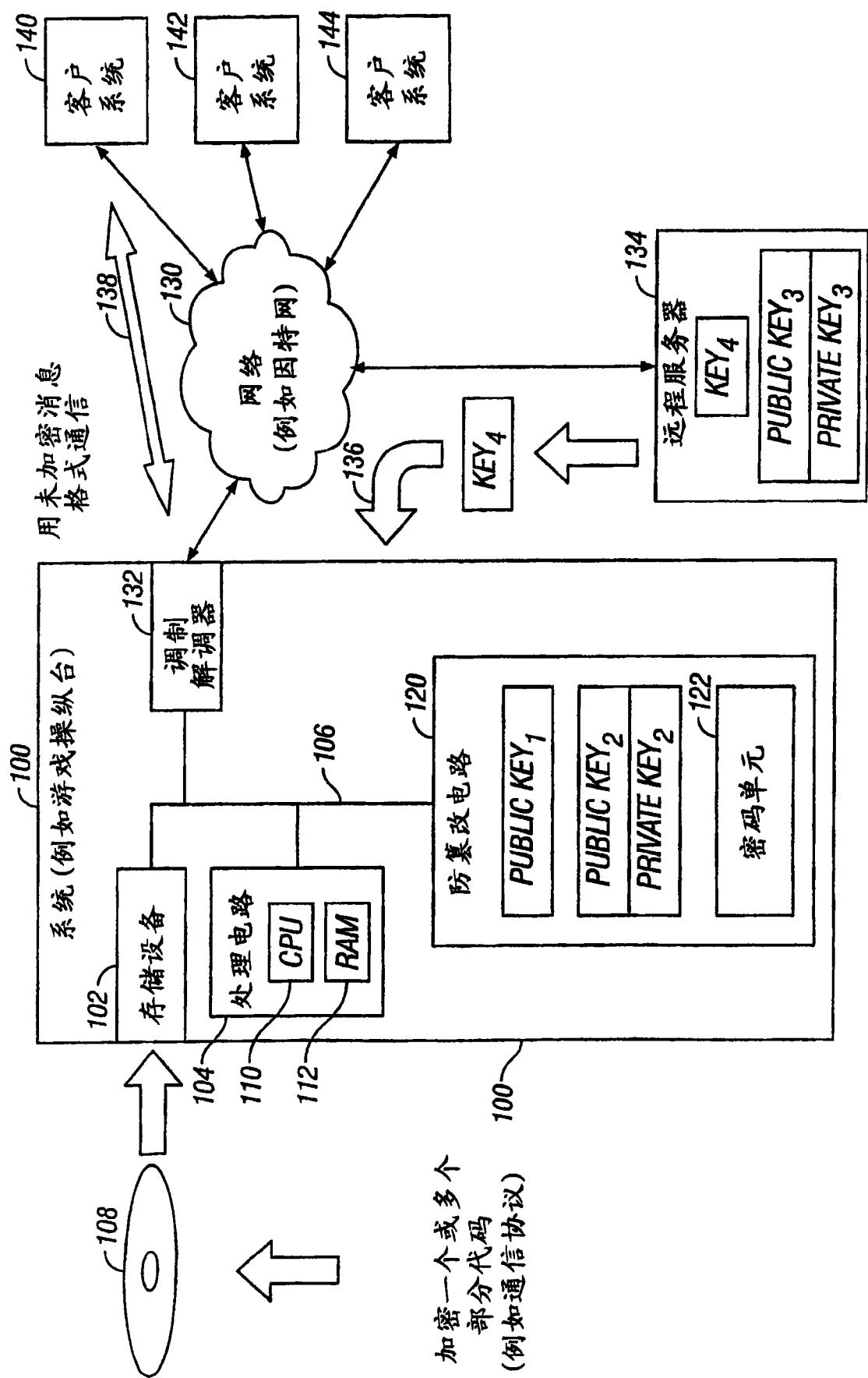


图 3

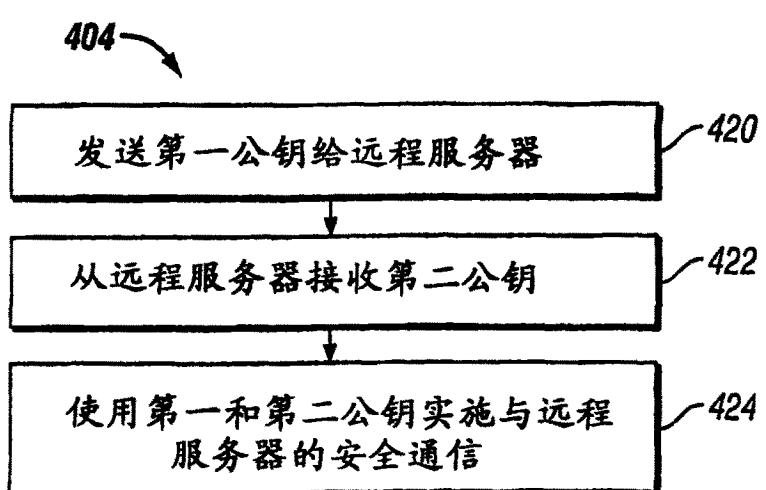
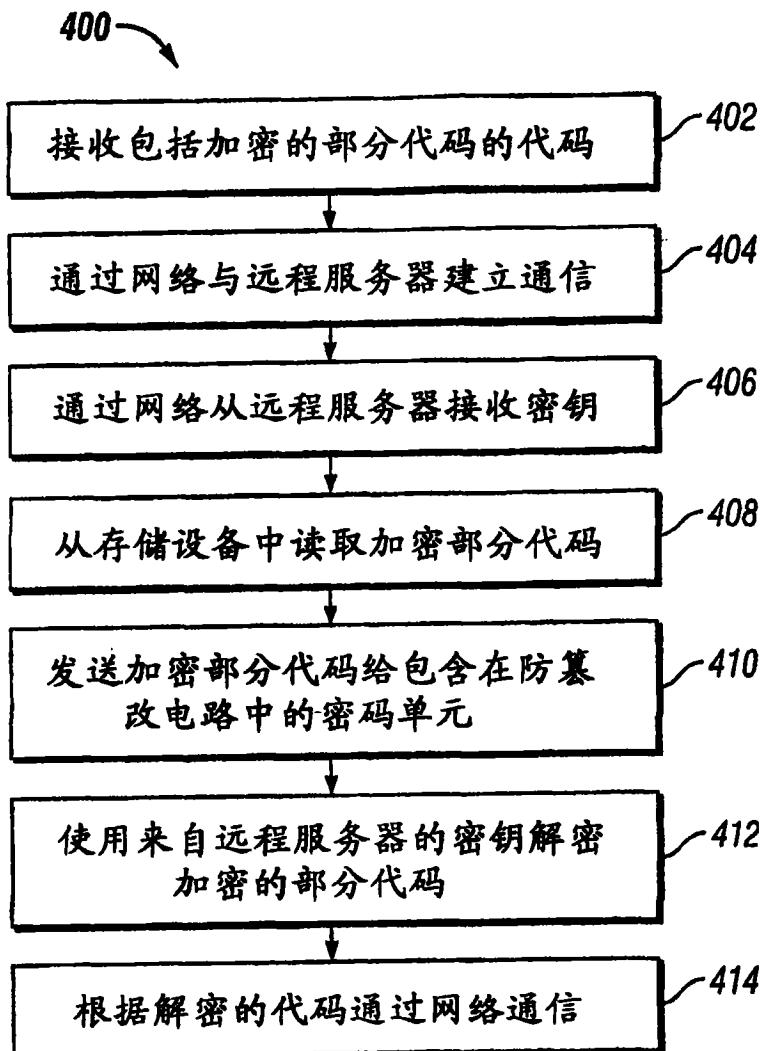


图 4B

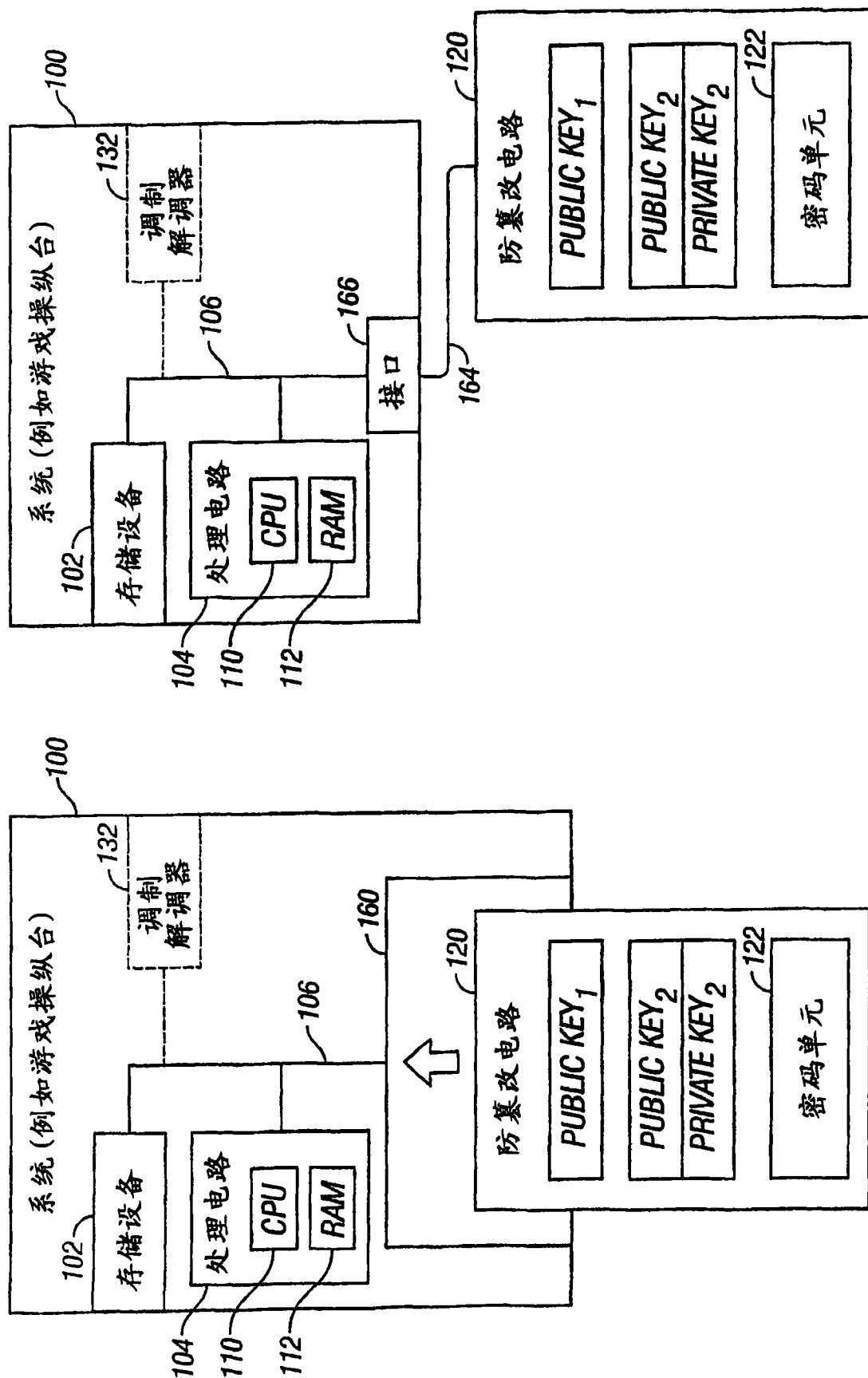


图 5A

图 5B

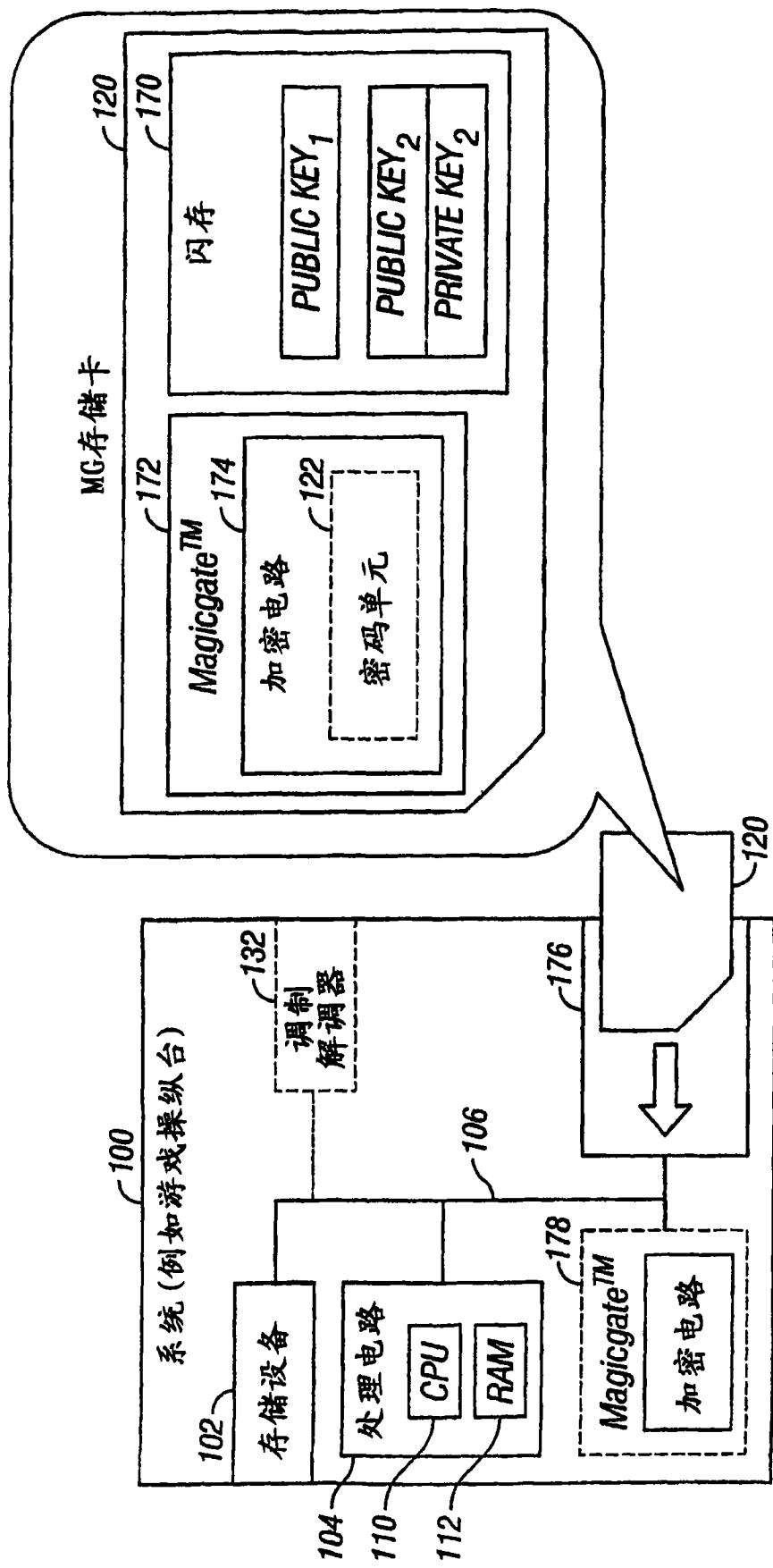


图 5C

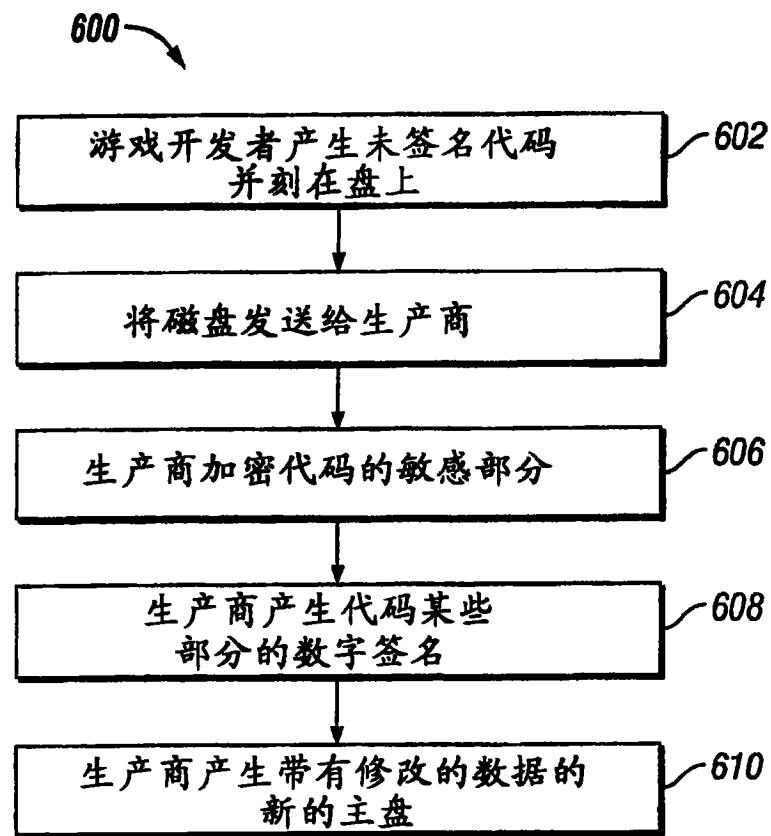


图 6