



(12) 发明专利

(10) 授权公告号 CN 101578608 B

(45) 授权公告日 2011.05.04

(21) 申请号 200780048917.7

代理人 刘国伟

(22) 申请日 2007.11.09

(51) Int. Cl.

(30) 优先权数据

G06F 21/00 (2006.01)

11/600, 273 2006.11.14 US

G11B 20/00 (2006.01)

11/600, 263 2006.11.14 US

(85) PCT申请进入国家阶段日

2009.06.30

(56) 对比文件

CN 1518825 A, 2004.08.04, 全文.

(86) PCT申请的申请数据

EP 1598822 A2, 2005.11.23, 全文.

PCT/US2007/023617 2007.11.09

US 2002/0126846 A1, 2002.09.12, 说明书第  
24-83段, 附图1-5.

(87) PCT申请的公布数据

US 2002/0126846 A1, 2002.09.12, 全文.

WO2008/069888 EN 2008.07.31

审查员 武文琛

(73) 专利权人 桑迪士克股份有限公司

地址 美国加利福尼亚州

(72) 发明人 法布里斯·约刚·库仑

阿吕·肯特·塔尼克

奥克塔伊·拉西扎德

(74) 专利代理机构 北京律盟知识产权代理有限

责任公司 11287

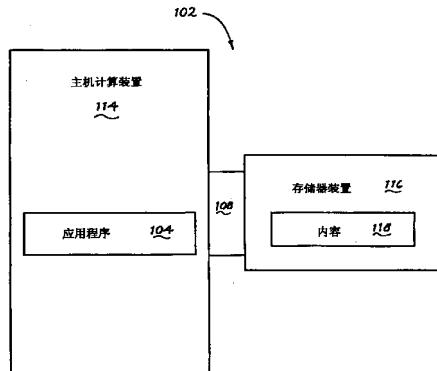
权利要求书 2 页 说明书 9 页 附图 11 页

(54) 发明名称

用于基于会话票证存取内容的方法及设备

(57) 摘要

本发明提供一种用于存取存储在存储器装置上的内容的方法。在此方法中，传输存取所述内容的请求且接收会话票证。所述会话票证包括用于解密所述内容的参数且所述会话票证基于经配置以在会话时改变的变量产生。可基于所述会话票证存取所述内容。还提供一种包含存储器及与所述存储器进行通信的处理器的设备。所述处理器经配置以：将存取存储在存储器装置中的内容的请求传输到所述存储器装置；接收会话票证；及基于所述会话票证存取所述内容。所述会话票证包括用于解密所述内容的参数且所述会话票证基于经配置以在会话时改变的数字产生。



1. 一种用于存取存储在存储器装置上的内容的方法,所述方法包含 :

在存储用密码密钥加密的内容的存储器装置中执行下述步骤 :

接收会话票证和请求,以从主机计算装置存取所述内容,其中所述会话票证先前被提供至所述主机计算装置,并且所述会话票证由所述存储器装置用变量加密与所述密码密钥相关联的参数而产生,所述变量具有与会话相关联的值并且所述变量在不同会话时改变值;

尝试经用所述变量解密所述会话票证来从所述会话票证抽取与所述密码密钥相关联的所述参数,其中如果所述会话没有改变,则所述变量的所述值没有改变,并且与所述密码密钥相关联的所述参数被从所述会话票证中抽取;以及

如果与所述密码密钥相关联的所述参数被从所述会话票证中抽取:

基于所述参数得到所述密码密钥,

用所述密码密钥解密所述内容,及

发送所述内容至主机计算装置。

2. 如权利要求 1 所述的方法,其中所述参数是对所述密码密钥的参考。

3. 如权利要求 1 所述的方法,其中所述参数是密码临时数,所述密码临时数用于产生所述密码密钥。

4. 如权利要求 1 所述的方法,其中所述变量是数字。

5. 如权利要求 4 所述的方法,其中所述数字经配置以在不同会话时随机改变。

6. 如权利要求 1 所述的方法,其中所述会话跨越一时间周期。

7. 如权利要求 1 所述的方法,其中所述会话在所述主机计算装置被重新起动时期满。

8. 如权利要求 1 所述的方法,其中所述会话在所述存储器装置从所述主机计算装置解耦时期满。

9. 一种存储器装置,其包含:

存储器,其存储用密码密钥加密的内容;及

存储器控制器,其与所述存储器进行通信,所述存储器控制器经配置以:

检索与所述密码密钥相关联的参数,

通过用变量加密与所述密码密钥相关联的参数而产生会话票证,所述变量具有

与会话相关联的值并且所述变量在不同会话时改变值;

将所述会话票证传输到计算装置,所述计算装置经配置以耦合到所述存储器装置,

从所述计算装置接收所述会话票证和存取所述内容的请求,及

尝试经用所述变量解密所述会话票证来从所述会话票证抽取与所述密码密钥相关联的所述参数,其中如果所述会话没有改变,则所述变量的所述值没有改变,并且与所述密码密钥相关联的所述参数被从所述会话票证中抽取;以及

如果与所述密码密钥相关联的所述参数被从所述会话票证中抽取:

基于所述参数得到所述密码密钥,

用所述密码密钥解密所述内容,及

发送所述内容至主机计算装置。

10. 如权利要求 9 所述的存储器装置,其中所述存储器控制器进一步经配置以:基于所  
述数字解密所述会话票证以抽取所述参数;及

基于所述参数存取所述内容。

11. 如权利要求 9 所述的存储器装置, 其中所述参数是对密码密钥的参考, 所述内容是用所述密码密钥加密的。

12. 如权利要求 9 所述的存储器装置, 其中所述参数是密码临时数, 所述密码临时数用于产生密码密钥。

13. 如权利要求 9 所述的存储器装置, 其中所述会话跨越一时间周期。

14. 如权利要求 9 所述的存储器装置, 其中所述会话在所述计算装置被重新起动时期满。

15. 如权利要求 9 所述的存储器装置, 其中所述会话在所述存储器装置从所述计算装置解耦时期满。

16. 一种存储器装置包括 :

存储器, 其可执行以存储用密码密钥加密的内容; 以及

与所述存储器进行通信的控制器, 其可执行 :

接收会话票证和请求, 以从主机计算装置存取所述内容, 其中所述会话票证先前被提供至所述主机计算装置, 并且所述会话票证由所述存储器装置用变量加密与所述密码密钥相关联的参数而产生, 所述变量具有与会话相关联的值并且所述变量在不同会话时改变值;

尝试经用所述变量解密所述会话票证来从所述会话票证抽取与所述密码密钥相关联的所述参数, 其中如果所述会话没有改变, 则所述变量的所述值没有改变, 并且与所述密码密钥相关联的所述参数被从所述会话票证中抽取; 以及

如果与所述密码密钥相关联的所述参数被从所述会话票证中抽取 :

基于所述参数得到所述密码密钥,

用所述密码密钥解密所述内容, 及

发送所述内容至主机计算装置。

17. 如权利要求 16 所述的存储器装置, 其中所述参数是对所述密码密钥的参考。

18. 如权利要求 16 所述的存储器装置, 其中所述参数是密码临时数, 所述密码临时数用于产生所述密码密钥。

19. 如权利要求 16 所述的存储器装置, 其中所述变量是数字。

20. 如权利要求 19 所述的存储器装置, 其中所述数字经配置以在不同会话时随机改变。

21. 如权利要求 16 所述的存储器装置, 其中所述会话跨越一时间周期。

22. 如权利要求 16 所述的存储器装置, 其中所述会话在所述主机计算装置被重新起动时期满。

23. 如权利要求 16 所述的存储器装置, 其中所述会话在所述存储器装置从所述主机计算装置解耦时期满。

## 用于基于会话票证存取内容的方法及设备

### 技术领域

[0001] 本发明的实施例大体来说涉及内容存取,且更特定来说涉及将内容与许可证链接及基于会话票证来存取所述内容。

### 背景技术

[0002] 数字权利管理 (DRM) 是用于保护并控制例如音乐文件、视频文件等內容及其它內容的分配的技术。在 DRM 中,用密码密钥加密內容,所述密码密钥从而也可用于解密所述內容。为使用户解密并存取所述內容,所述用户必须存取与所述內容相关联的许可证。通常,许可证可依据由许可证提供者定义的许可而准予对內容的不同存取权利。举例来说,所述许可证可将所述內容(例如,音乐文件)限制为播放有限的次数。

[0003] 在传统 DRM 技术中,用于解密所述內容的密码密钥仅存储在所述许可证中。所述许可证可被窃取且所述密码密钥可容易地被从所述许可证中抽取。如果危及所述密码密钥的安全,那么未经授权的用户可在没有所述许可证的情况下解密所述內容且从而在没有限制的情况下存取所述內容。因此,需要进一步改善对所述內容的保护。

### 发明内容

[0004] 本发明的各种实施例提供用于将许可证与內容链接且基于会话票证存取內容的方法、系统及 / 或设备。应了解,可以多种方式实施所述实施例,包括实施为方法、电路、系統或装置。下文将说明本发明的若干实施例。

[0005] 在一个实施例中,提供一种用于存取存储在存储器装置上的內容的方法。在此方法中,传输存取所述內容的请求且接收会话票证。所述会话票证包括用于解密所述內容的参数且所述会话票证基于经配置以在会话时改变的变量产生。可基于所述会话票证存取所述內容。

[0006] 在另一实施例中,提供一种设备。所述设备包括存储器及与所述存储器进行通信的处理器。所述处理器经配置以:将存取存储在存储器装置中的內容的请求传输到所述存储器装置;接收会话票证;及基于所述会话票证存取所述內容。所述会话票证包括用于解密所述內容的参数且所述会话票证基于经配置以在会话时改变的变量产生。

[0007] 结合以实例方式图解说明本发明的原理的附图根据以下详细说明,将易知本发明的其它实施例及优点。

### 附图说明

[0008] 结合附图阅读以下详细说明将易于理解本发明,且相同的参考编号指示相同的结构元件。

[0009] 图 1 是根据本发明实施例的设备的系统的简化框图。

[0010] 图 2 是描绘根据本发明实施例的用于解密內容的参数的产生的框图。

[0011] 图 3 是根据本发明实施例的用于存取存储器装置的系统的简化框图。

- [0012] 图 4 是描绘根据本发明实施例的从存储器装置存取内容的流程图。
- [0013] 图 5 是描绘根据本发明实施例的会话票证的产生的框图。
- [0014] 图 6 是根据本发明实施例的用于使用会话票证来存取存储器装置的系统的简化框图。
- [0015] 图 7 是描绘根据本发明实施例的基于会话票证从存储器装置存取内容的流程图。
- [0016] 图 8 是根据本发明实施例的可托管在主机计算装置上的用于存取内容的程序应用程序的简化框图。
- [0017] 图 9 是根据本发明实施例的可包括在存储器装置中的程序应用程序的简化框图。
- [0018] 图 10 是根据本发明实施例的适合于托管内容保护平台及其它程序应用程序的主机计算装置的总览的简化框图。
- [0019] 图 11 是根据本发明实施例的存储器装置的简化框图。

## 具体实施方式

[0020] 下文随同附图一起提供对一个或一个以上实施例的详细说明。结合所述实施例提供所述详细说明，但所述说明并不限于任一特定实施例。所述范围仅由权利要求书限制且涵盖许多替代方案、修改及等效物。以下说明中列出大量具体细节，以便提供透彻的理解。提供这些细节是出于举例目的，且可在没有这些具体细节中的某些或全部的情况下根据权利要求书来实施所说明的实施例。为清楚起见，没有详细说明在与所述实施例相关的技术领域中已知的技术材料以避免不必要地模糊本发明。

[0021] 本文中所说明的实施例提供许可证与内容的链接及基于会话票证对所述内容的存取。使用密码密钥来解密并存取经加密的内容。如下文将更加详细地解释，使用与所述许可证及所述内容两者相关联的参数来导出所述密码密钥。在某些实施例中，用以导出所述密码密钥的参数可进一步用变量加密，以便将对所述内容的存取限定到会话。

[0022] 图 1 是根据本发明实施例的设备的系统的简化框图。如图 1 中所示，系统 102 包括主机计算装置 114 及存储器装置 116。主机计算装置 114 可包括各种能够存取存储器装置 116 以将内容 118 存储在所述存储器装置上或检索存储在所述存储器装置上的内容 118 的电子装置。存储器装置 116 可通过机械接口 108（例如，引脚及 / 或插座连接器）以可抽换方式耦合到主机计算装置 114。存储器装置 116 是存储器存储装置。如下文将解释，存储器装置 116 的实例是使用非易失性存储器的存储器卡。

[0023] 主机计算装置 114 托管应用程序 104。应用程序 104 可包括各种程序应用程序。举例来说，应用程序 104 可以是管理主机计算装置 114 上的硬件及软件资源的操作系统。在一实例中，应用程序 104 可以是经配置以播放音频及视频文件的多媒体播放器。另外，举例来说，应用程序 104 可以是视频游戏。应用程序 104 可存取存储在存储器装置 116 中的内容 118。内容 118 可包括各种数据。内容 118 的实例包括编码为音频文件格式（例如，WAVE、MPEG-1、音频播放器 3 (MP3)、先进音频编码 (AAC) 及其它音频文件格式）的音频文件。内容 118 还可包括编码为视频文件格式（例如，音频视频交错 (AVI)、移动图片专家组 (MPEG) 及其它视频文件格式）的视频文件。内容 118 的其它实例包括文档文件、图像文件、应用文件及其它数据。

[0024] 将许可证与内容链接

[0025] 图 2 是描绘根据本发明实施例的用于解密内容的参数的产生的框图。图 2 显示内容 118 及相关联的许可证 204。内容 118 经加密，使得所述内容不可理解。一般来说，许可证 204 是使内容 118 能够被存取的数据（例如，串、文件及其它数据）。许可证 204 可包括对存取内容 118 的许可或规则，例如，存取的持续时间，将对所述内容的存取限制到特定的计算装置、日期、时间，可存取所述内容的次数及其它许可。许可证 204 因此可经配置以定义对存取内容 118 的所述许可。因此基于许可证 204 中所包括的许可用户被允许存取内容 118。举例来说，许可证 204 可允许呈音乐文件形式的内容 118 在特定计算装置上播放三次。在另一实例中，许可证 204 可允许内容 118 被存取但不允许将其拷贝到另一计算装置。

[0026] 内容 118 经加密且第三参数 210 经配置以用于解密所述内容。第三参数 210 包括可与内容 118 的解密相关联的各种数据。举例来说，第三参数 210 可以是用于内容 118 的加密及解密的密码密钥。代替所述密码密钥，第三参数 210 还可包括对所述密码密钥的参考。举例来说，所述参考可以是识别所述密码密钥的数字或串。第三参数 210 还可包括验证密钥。所述验证密钥是用于主机计算装置与存储器装置之间的验证会话的密码密钥。在另一实例中，第三参数 210 可以是密码临时数。密码临时数是可用于产生所述密码密钥的数字。

[0027] 基于第一参数 202 及第二参数 206 产生第三参数 210。换句话说，第三参数 210 可表达为

$$\text{[0028] 第三参数} = F(\text{第一参数}, \text{第二参数}) \quad (1.0)$$

[0029] 其中所述第三参数是第一及第二参数 202 及 206 的函数。所述函数可包括各种函数，例如散列函数，因此第三参数 210 可以是所述散列函数的散列值。第一参数 202 与许可证 204 相关联且第二参数 206 与内容 118 相关联。第一及第二参数 202 及 206 可包括各种数据。举例来说，第一参数 202 可以是数字。在一个实施例中，可随机产生所述数字。在另一实施例中，所述数字是预定义的。第二参数 206 可取决于第一参数 202 或反之亦然。举例来说，第二参数 206 可以是从对密码密钥的参考及第一参数 202 两者中导出的数字或串。所述数字或串可表达为

$$\text{[0030] 第二参数} = F(\text{密钥参考}, \text{第一参数}) \quad (1.2)$$

[0031] 其中第二参数 206 是对密码密钥的参考及第一参数 202 两者的函数。应了解，第二参数 206 也可从验证密钥及第一参数 202 两者中导出。在另一实例中，第二参数 206 可从密码临时数及第一参数 202 中导出。相反，第一参数 202 可从第二参数 206 及验证密钥、对密码密钥的参考、密码临时数或其它参数中导出。

[0032] 第一及第二参数 202 及 206 分别与许可证 204 及内容 118 相关联。为与许可证 204 或内容 118 相关联，第一及第二参数 202 及 206 可分别位于或包括在所述许可证及所述内容中。举例来说，第二参数 206 可位于内容 118 的标头或页脚中。另一选择为，第一参数 202 及 / 或第二参数 206 可与许可证 204 及 / 或内容 118 分开定位。如果分开定位，那么许可证 204 可与第一参数 202 相关联，其中包括指向所述第一参数的指针。如果所述第二参数与内容分开定位，那么内容 118 也可包括指向第二参数 206 的指针。

[0033] 图 3 是根据本发明实施例的用于存取存储器装置的系统的简化框图。如图所示，系统 302 包括耦合到存储器装置 116 的主机计算装置 114。主机计算装置 114 可包括应用程序 104 及第一内容保护平台 304。存储器装置 116 包括第二内容保护平台 306、内容 118

及许可证 204。在一个实施例中，许可证 204 可存储在存储器装置 116 的隐藏分区中，其中所述许可证对于许多应用程序不可见或不可存取。除存储在存储器装置 116 中以外，许可证 204 也可存储在主机计算装置 114 中。第一及第二内容保护平台 304 及 306 是用于将内容 118 保护到存储器装置 116 的技术平台。通过第一内容保护平台 304 及 / 或第二内容保护平台 306，用户可在不折衷内容保护的情况下转移存储器装置 116 及其内容 118。存在可用于保护数据的各种内容保护平台，实例以商标 TrustedFlash™ 及 Gruvi™(如由晟碟公司制造)出售。

[0034] 如图 3 中所示，作为第一内容保护平台 304 的应用程序 104 传输对存储在存储器装置 116 中的内容 118 的请求。在此，内容 118 经加密。为解密内容 118，检索与许可证 204 相关联的第一参数 202 及与内容 118 相关联的第二参数 206。第一参数 202 及第二参数 206 可分别包括在许可证 204 及内容 118 中，或可以是与所述许可证及所述内容分开定位的文件。如方程式 1.0 所定义，第三参数基于第一参数 202 及第二参数 206 产生。换句话说，所述第三参数可从第一及第二参数 202 及 206 中导出。所述第三参数可以是用于解密内容 118 的密码密钥、对所述密码密钥的参考、验证密钥、临时数或其它参数。使用所述第三参数，应用程序 104 可解密并存取内容 118。为存取内容 118，第一内容保护平台 304 可将所述第三参数及对内容 118 的请求传输到存储器装置 116。第二内容保护平台 306 可基于所述第三参数解密内容 118 且可将经解密的内容传输到作为第一内容保护平台 304 的应用程序 104。

[0035] 在图 3 的实施例中，主机计算装置 114 上所托管的第一内容保护平台 304 检索第一及第二参数 202 及 206 且基于所述第一及第二参数产生所述第三参数。在另一实施例中，存储器装置 116 中所包括的第二内容保护平台 306 也可检索第一及第二参数 202 及 206 且基于所述第一及第二参数产生所述第三参数。

[0036] 图 4 是描绘根据本发明实施例的从存储器装置存取内容的流程图。在 402 处开始，分析所述内容以确定所述内容是否受保护（即，经加密）。与所述内容相关联的各种信息可指示所述内容是否经加密。举例来说，所述内容的标头可指示所述内容经加密。另一选择为，所述内容的文件名扩展名也可指示所述内容经加密。如果所述内容不受保护，那么在 410 中可直接存取所述内容。如果所述内容受保护，那么在 404 处从所述许可证检索第一参数。在此实施例中，所述第一参数是数字。可随机产生或预定义所述数字。在 406 处，从所述内容中检索第二参数。在一个实施例中，如方程式 1.2 中所表达，所述第二参数可从对所述密码密钥的参考及所述第一参数中导出。所述密码密钥用于加密或解密所述内容。因此，所述第二参数与所述内容及所述许可证两者相关联，因为所述第二参数从对用于解密所述内容的密码密钥的参考及所述许可证中所包括的数字中导出或计算。应注意，在另一实施例中，所述第一参数（例如，数字）可与所述内容相关联且所述第二参数可与所述许可证相关联。

[0037] 使用所述第一参数及所述第二参数，在 408 处可产生或计算对所述密码密钥的参考。如以上方程式 1.0 中所表达，对所述密码密钥的参考可基于所述第一参数及所述第二参数产生。此后，在 410 处，可基于所述第三参数解密并存取所述内容。举例来说，在一个实施例中，呈对所述密码密钥的参考形式的第三参数可被传输到所述存储器装置。所述存储器装置可包括存储所述密码密钥的安全存储器件。所述存储器装置可使用对所述密码密

钥的参考从所述安全存储器件检索所述密码密钥。使用所述密码密钥，所述存储器装置可解密所述内容且将经解密的内容传输到主机计算装置。

[0038] 基于会话票证存取内容

[0039] 图 5 是描绘根据本发明实施例的会话票证的产生的框图。起初提供参数 502 且所述参数包括各种可与内容的解密相关联的数据。参数 502 可基于如上所述与许可证及内容相关联的参数产生。参数 502 的实例包括对用于所述内容的解密的密码密钥的参考、密码临时数或其它参数。

[0040] 会话票证 506 的产生涉及使用变量 504。变量 504 包括各种数据。举例来说，所述数据可以是数字。可预定义或随机产生所述数字。在另一实施例中，所述数据可以是字符串。不同于上文所论述的参数，变量 504 可不与所述许可证及内容相关联。换句话说，变量 504 可独立于所述许可证及内容。变量 504 经配置以在会话时改变。会话可跨越一时间周期。举例来说，所述会话可持续一小时、一天、一星期或其它时间单位。另外，会话可在耦合到所述存储器装置的主机计算装置被起始或重新起动时期满。会话也可在所述存储器装置从所述主机计算装置解耦时期满。此外，举例来说，会话可跨越对所述内容的有限数目的存取（例如，可存取所述内容的有限次数）。

[0041] 会话票证 506 基于参数 502 及变量 504 产生，借此基于所述变量来加密参数以定义会话票证 506。会话票证 506 因此可表达为

[0042] 会话票证 = F(参数, 变量) (2.0)

[0043] 其中会话票证是参数 502 及变量 504 的函数。使用会话票证 506，可基于所述会话票证来存取所述内容。举例来说，主机计算装置可将会话票证 506 传输到所述存储器装置。所述存储器装置可基于会话票证 506 导出用于解密所述内容的参数。参数 502 可从以下方程式中导出

[0044] 参数 = F<sup>-1</sup>(会话票证, 变量) (2.2)

[0045] 其中所述参数是会话票证 506 及变量 504 的反函数。

[0046] 应了解，会话票证 506 与特定内容相关联，因为所述会话票证用于解密所述内容。因此，不能够通过会话票证 506 来使用或存取存储在所述存储器装置中的另一内容，除非所述会话票证包括用以解密所述其它内容的参数，例如参数 502。作为实例，如果存储在存储器装置中的两个单独内容用不同的密码密钥加密，那么主机计算装置或存储器装置产生两个不同的会话票证以存取所述两个单独内容。在此，一个会话票证不能够用于存取所述两个用不同的密码密钥加密的单独内容。

[0047] 图 6 是根据本发明实施例的用于使用会话票证来存取存储器装置的系统的简化框图。系统 602 包括耦合到存储器装置 116 的主机计算装置 114。主机计算装置 114 可包括应用程序 104 及第一内容保护平台 304。存储器装置 116 包括第二内容保护平台 306、内容 118 及许可证 204。如上文所论述，第一及第二内容保护平台 304 及 306 可经配置以管理存储在存储器装置 116 中的内容 118 的数字权利。

[0048] 如图 6 中所示，应用程序 104 通过第一内容保护平台 304 传输对存储在存储器装置 116 中的内容 118 的请求。内容 118 用密码密钥加密。将与所述密码密钥相关联的参数（例如，对所述密码密钥的参考、临时数或其它参数）提供到第二内容保护平台 306。响应于存取内容 118 的请求，第二内容保护平台 306 基于变量 604 加密所述参数以定义会话票

证,其表达于方程式 2.0 中。第二内容保护平台 306 可产生变量 604(例如,数字、串或其它参数)。变量 604 经配置以在会话时改变。举例来说,第二内容保护平台 306 可针对每一会话产生不同的变量 604。可随机产生或预定义变量 604。

[0049] 在产生会话票证之后,第二内容保护平台 306 将所述会话票证传输到主机计算装置 114。使用所述会话票证,主机计算装置 114 可基于所述会话票证存取内容 118。为存取内容 118,主机计算装置 114 随后将所述会话票证传输回存储器装置 116。通过接收会话票证,第二内容保护平台 306 解密所述会话票证以抽取用于解密内容 118 的参数,其表达于方程式 2.2 中。如果变量 604 未改变,那么可抽取所述参数,因为所述解密基于与用于加密所述参数的变量相同的变量。变量 604 可在不同的会话时改变。因此,如果变量在同一会话内产生,那么变量 604 与用于加密所述参数的变量相同。然而,如果变量 604 已改变,那么不能够抽取所述参数,因为所述解密基于与用于加密所述参数的变量不同的变量。如果变量在不同的会话内产生,那么变量 604 不同于用于加密所述参数的变量。通过在会话时改变变量 604,所述会话票证持续或有效达一个会话。如果可抽取所述参数,那么第二内容保护平台 306 可基于所述参数解密内容 118 且将所述经解密的内容传输到主机计算装置 114。

[0050] 在另一实施例中,第一内容保护平台 304 也可通过对用于解密内容 118 的参数加密来产生所述会话票证。在此,响应于应用程序 104 存取内容 118 的请求,第一内容保护平台 304 可产生所述会话票证且将所述会话票证传输到应用程序 104。应用程序 104 随后可将所述会话票证传输回第一内容保护平台 304 以存取内容 118。

[0051] 图 7 是描绘根据本发明实施例的基于会话票从存储器装置存取内容的流程图。在 702 处开始,检索对密码密钥的参考。可从主机计算装置或存储器装置检索所述参考。存储在所述存储器装置中的内容经加密且可使用所述密码密钥解密。使用对所述密码密钥的参考,在 704 处基于数字加密对所述密码密钥的参考以定义会话票证。所述数字经配置以在会话时改变且可随机产生。在 706 处,所述会话票证随后可被传输到(举例来说)主机计算装置。

[0052] 当所述主机计算装置存取存储在存储器装置上的内容时,所述主机计算装置可在 706 处将所接收的会话票证传输到所述存储器装置。所述存储器装置在 708 处接收所述会话票证且在 710 处基于数字解密所述会话票证。如果所述数字与用以产生所述会话票证的数字相匹配,那么可从所述解密操作中抽取对密码密钥的参考。然而,如果所述会话已改变且所述存储器装置保存有不同的数字,那么不能够从所述解密操作中抽取对所述密码密钥的参考,因为所述数字不匹配。如果可从所述会话票证抽取对所述密码密钥的参考,那么在 712 处基于所述参考检索所述密码密钥。举例来说,可从安全存储器件中检索所述密码密钥。随后在 714 处使用所述密码密钥解密所述内容且随后在 716 处将其传输到(举例来说)所述主机计算装置。

[0053] 图 8 是根据本发明实施例的可托管在主机计算装置上的用于存取内容的程序应用程序的简化框图。主机计算装置 114 可托管应用程序 104、数字权利管理(DRM)模块 806、内容保护平台 304、文件系统管理器 808 及装置驱动器 810。如上文所论述,应用程序 104 可包括各种程序应用程序,例如多媒体播放器、视频游戏及其它应用程序。与应用程序 104 进行通信的是 DRM 模块 806 及内容保护平台 304。DRM 模块 806 允许主机计算装置 114 管理存储在存储器装置或其它位置中的内容的数字权利。举例来说,DRM 模块 806 可保护内容

且控制其分配。如上文所论述,内容保护平台 304 是用于保证存储器装置上的内容的技术平台。内容保护平台 304 可包括安全性管理器 802 及主机密码引擎 804。一般来说,安全性管理器 802 管理对存储在存储器装置中的内容的存取。管理包括(举例来说)检查所述内容是否受保护,基于与许可证及所述内容相关联的参数产生对密码密钥的参考,基于参数及变量产生会话票证,产生所述变量及其它操作。主机密码引擎 804 包括密码库以处置密码操作。内容保护平台 304 及 DRM 模块 806 一同为主机计算装置 114(及存储器装置) 提供安全存储及内容管理能力。举例来说,内容保护平台 304 及 DRM 模块 806 允许安全存储存储在所述存储器装置中的内容(例如,音乐文件、电影文件、软件及其它数据)及强制执行用于控制对所述内容的存取的预定义政策。

[0054] 与内容保护平台 304 进行通信的是文件系统管理器 808。一般来说,文件系统管理器 808 经配置以管理并处置对存储在存储器装置中的内容的存取(例如,读取、写入及其它存取操作)。举例来说,文件系统管理器 808 可从存储器装置读取内容且将所述内容传输到内容保护平台 304 以供处理。主机计算装置 114 可与存储器装置介接。主机计算装置 114 因此可包括与文件系统管理器 808 进行通信的装置驱动器 810 以与所述存储器装置介接。装置驱动器 810 可(举例来说)包括较低级接口功能以与存储器装置进行通信。较低级接口功能的实例包括与数据到达及来自所述存储器装置的输入及输出相关联的输入/输出功能。

[0055] 图 9 是根据本发明实施例的可包括在存储器装置中的程序应用程序的简化框图。存储器装置 116 可包括 DRM 模块 902、内容保护平台 306、密码引擎 904 及安全存储器件 906。在存储器装置 116 中,DRM 模块 902 允许存储器装置 116 管理存储在所述存储器装置中的内容的数字权利。举例来说,DRM 模块 902 可经配置以强制执行内容权利。如上文所论述,内容保护平台 306 是用于保护存储在存储器装置 116 上的内容的技术平台。内容保护平台 306 可经配置以基于与许可证及所述内容相关联的参数产生对密码密钥的参考,以基于参数及变量产生会话票证,且可经配置以用于其它操作。密码引擎 904 处置密码操作且安全存储器件 906 存储所述密码密钥。

[0056] 应了解,在其它实施例中,图 8 的主机计算装置 114 及图 9 的存储器装置 116 可包括除图 8 及 9 中所示的那些程序应用程序以外的更少或更多程序应用程序。举例来说,如图 8 中所示,文件系统管理器 808 及装置驱动器 810 可集成到内容保护平台 304 中。图 8 的主机计算装置 114 因此可包括 DRM 模块 806 及内容保护平台 304。

[0057] 图 10 是根据本发明实施例的适合于托管内容保护平台及其它程序应用程序的主机计算装置的总览的简化框图。在某些实施例中,主机计算装置 114 可用于实施计算机程序(例如,内容保护平台)、逻辑、应用程序、方法、过程或其它软件以存取内容。主机计算装置 114 的实例包括桌上型计算机、服务器、便携式计算装置、个人数字助理、蜂窝式电话、器具内的计算引擎及其它计算机系统。如图 10 中所示,主机计算装置 114 包括用于传送信息的总线 1002 或其它通信机构,其互连子系统及装置,例如处理器 1004、系统存储器 1006(例如,随机存取存储器 (RAM))、存储装置 1008(例如,只读存储器 (ROM)、磁盘驱动器、光盘驱动器及其它存储装置)、通信接口 1012(例如,现代或以太卡)、显示器 1014(例如,阴极射线管 (CRT) 或液晶显示器 (LCD))、输入/输出装置 1016(例如,键盘) 及光标控制 1018(例如,鼠标或轨迹球)。

[0058] 在某些实施例中,当执行存储在系统存储器 1006 中的一个或一个以上程序指令的一个或一个以上序列时,主机计算装置 114 通过处理器 1004 执行特定操作。可从另一计算机可读媒体(例如,存储装置 1008)将此类程序指令读入系统存储器 1006 中。在某些实施例中,可使用硬接线电路来取代软件程序指令或与软件程序指令组合使用来实施本发明的实施例。

[0059] 应了解,术语“计算机可读媒体”是指参与向处理器 1004 提供供执行的程序指令的合适媒体。此种媒体可采取许多形式,其包括但不限于:非易失性媒体、易失性媒体及传输媒体。非易失性媒体可包括(举例来说)光盘或磁盘,例如存储装置 1008。易失性媒体可包括动态存储器,例如系统存储器 1006。传输媒体包括同轴电缆、铜导线及光纤,其中包括包含总线 1002 的导线。传输媒体也可采用声波或光波的形式,例如在无线电波及红外线数据通信期间产生的那些声波或光波。计算机可读媒体的普遍形式包括(举例来说)磁性媒体(例如,软盘、软磁盘、硬磁盘、磁带及其它磁性媒体)、光学媒体(例如,压缩光盘只读存储器(CD-ROM)及其它光学媒体)、具有图案的物理媒体(例如,穿孔卡、纸带、任何其它物理媒体)、存储器芯片或盒式磁带、载波(例如, RAM、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、快闪存储器及其它存储器芯片或盒式磁带)及计算机可从其进行读取的任何其它媒体。

[0060] 在某些实施例中,用以实践所述实施例的程序指令序列的执行可由单个计算装置 114 执行。在其它实施例中,由通信链路 1020(例如,局域网(LAN)、公共交换电话网(PSTN)、无线网络及其它通信链路)耦合的两个或两个以上计算机系统(例如,主机计算装置 114)可执行程序指令序列以彼此协作实践所述实施例。另外,计算装置 114 可通过通信链路 1020 及通信接口 1012 传输及接收消息、数据及指令,包括程序,即应用程序代码。在接收到所述程序指令时,所接收的程序指令可由处理器 1004 执行,及 / 或存储在存储装置 1008 中或其它非易失性存储装置中以供稍后执行。

[0061] 图 11 是根据本发明实施例的存储器装置的简化框图。如图 11 中所示,存储器装置 116 包括与存储器 1104 进行通信的存储器控制器 1102。一般来说,存储器控制器 1102 控制存储器 1106 的操作。操作的实例包括写入(或编程)数据、读取数据、擦除数据、检验数据及其它操作。另外,存储器控制器 1102 可经配置以基于与许可证及内容相关联的若干参数产生一参数,基于参数及数字产生会话票证,且可经配置以用于上文所说明的其它操作。

[0062] 存储器装置 116 可包括各种非易失性存储器结构及技术。存储器技术的实例包括快闪存储器(例如,NAND、NOR、单级单元(SLC/BIN)、多级单元(MLC)、分裂位线 NOR(DINOR)、AND、高电容耦合率(HiCR)、不对称不接触晶体管(ACT)及其它快闪存储器)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)、只读存储器(ROM)、一次可编程存储器(OTP)及其它存储器技术。在一个实施例中,存储器装置 116 可以是使用快闪存储器的快闪存储器卡。快闪存储器卡的实例包括各种以下商标的产品,例如 Secure Digital<sup>TM</sup>(符合由加利福尼亚圣拉蒙(San Ramon)的 SD 卡协会维持的规范),MultiMediaCard<sup>TM</sup>(符合由加利福尼亚帕洛阿尔托(Palo Alto)的多媒体卡协会(“MMCA”)维持的规范),MiniSD<sup>TM</sup>(如由晟碟公司制造),MicroSD<sup>TM</sup>(如由晟碟公司制造),CompactFlash<sup>TM</sup>(符合由加利福尼亚帕洛阿尔托的微型快闪(CompactFlash)协会(“CFA”)维持的规范),SmartMedia<sup>TM</sup>(符合由日本横滨(Yokohama)的固态软盘卡(“SSFDC”)论坛

维持的规范),xD-Picture Card<sup>TM</sup>(符合由日本东京(Tokyo)的xD-图片卡许可证颁发办公室(xD-Picture Card Licensing Office)维持的规范),Memory Stick<sup>TM</sup>(符合由日本横滨的固态软盘卡(“SSFDC”)论坛维持的规范),TransFlash<sup>TM</sup>(如由晟碟公司制造),及其它快闪存储器卡。在另一实施例中,存储器装置116可实施为非抽换式存储器装置。

[0063] 以下专利文档包含可与本文中所说明实施例一同使用的实施例。这些专利文档中的每一者在与本申请案相同的日期提出申请,转让给本发明的受让人,且在此以引用方式并入本文中:“用于将内容与许可证链接的方法(Methods for Linking Content with License)”,美国专利申请案第11/599,655号;“用于将内容与许可证链接的设备(Apparatuses for Linking Content with License)”,美国专利申请案第11/600,270号;“用于基于会话票证存取内容的设备(Apparatuses for Accessing Content Based on a Session Ticket)”,美国专利申请案第11/600,273号;“用于将内容绑缚到单独的存储器装置的方法(Methods for Binding Content to a Separate Memory Device)”,美国专利申请案第11/600,262号;“用于将内容绑缚到单独的存储器装置的设备(Apparatuses for Binding Content to a Separate Memory Device)”,美国专利申请案第11/600,245号;“用于允许多个用户存取预览内容的方法(Method for Allowing Multiple Users to Access Preview Content)”,美国专利申请案第11/599,994号;“用于允许多个用户存取预览内容的系统(System for Allowing Multiple Users to Access Preview Content)”,美国专利申请案第11/599,995号;“用于允许受第一DRM系统保护的内容由第二DRM系统存取的方法(Method for Allowing Content Protected by a First DRM System to Be Accessed by a Second DRM System)”,美国专利申请案第11/600,005号;“用于允许受第一DRM系统保护的内容由第二DRM系统存取的系统(System for Allowing Content Protected by a First DRM System to Be Accessed by a Second DRMSystem)”,美国专利申请案第11/599,991号;“用于连接到与内容相关联的网络位置的方法(Method for Connecting to a Network Location Associated with Content)”,美国专利申请案第11/600,300号;及“用于连接到与内容相关联的网络位置的系统(System for Connecting to a Network Location Associated with Content)”,美国专利申请案第11/600,006号。

[0064] 虽然已出于清楚地理解的目的而以一定详细程度说明了上述实施例,但本发明并不限于所提供的细节。可存在许多用以实施所述实施例的替代方式。相应地,应将所述所揭示实施例视为说明性而非限制性实施例,且本发明并非打算将所述实施例限定为本文中给出的细节,而是可在所附权利要求书的范围及等效范围内作出修改。在权利要求书中,元件及/或操作并不暗示操作的任何特定次序,除非权利要求书中明确指出。

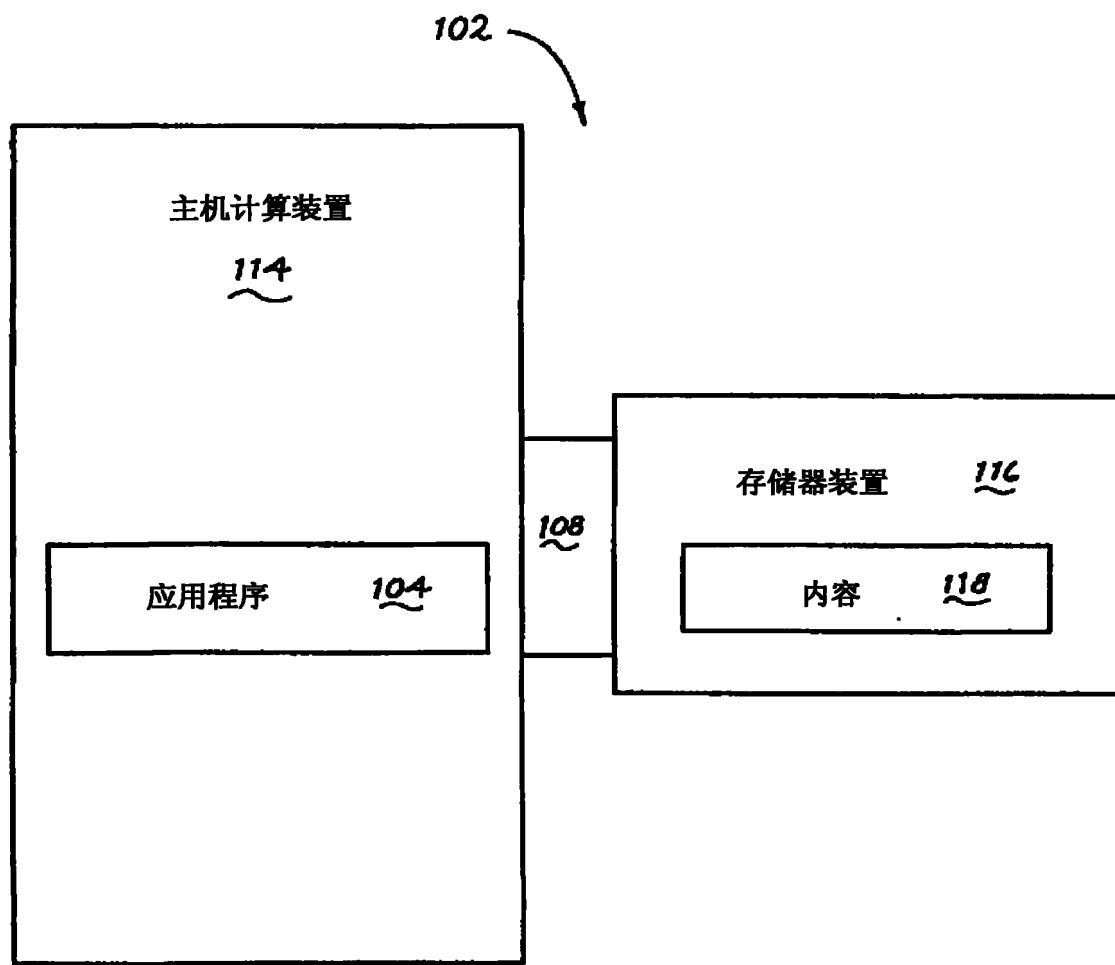


图 1

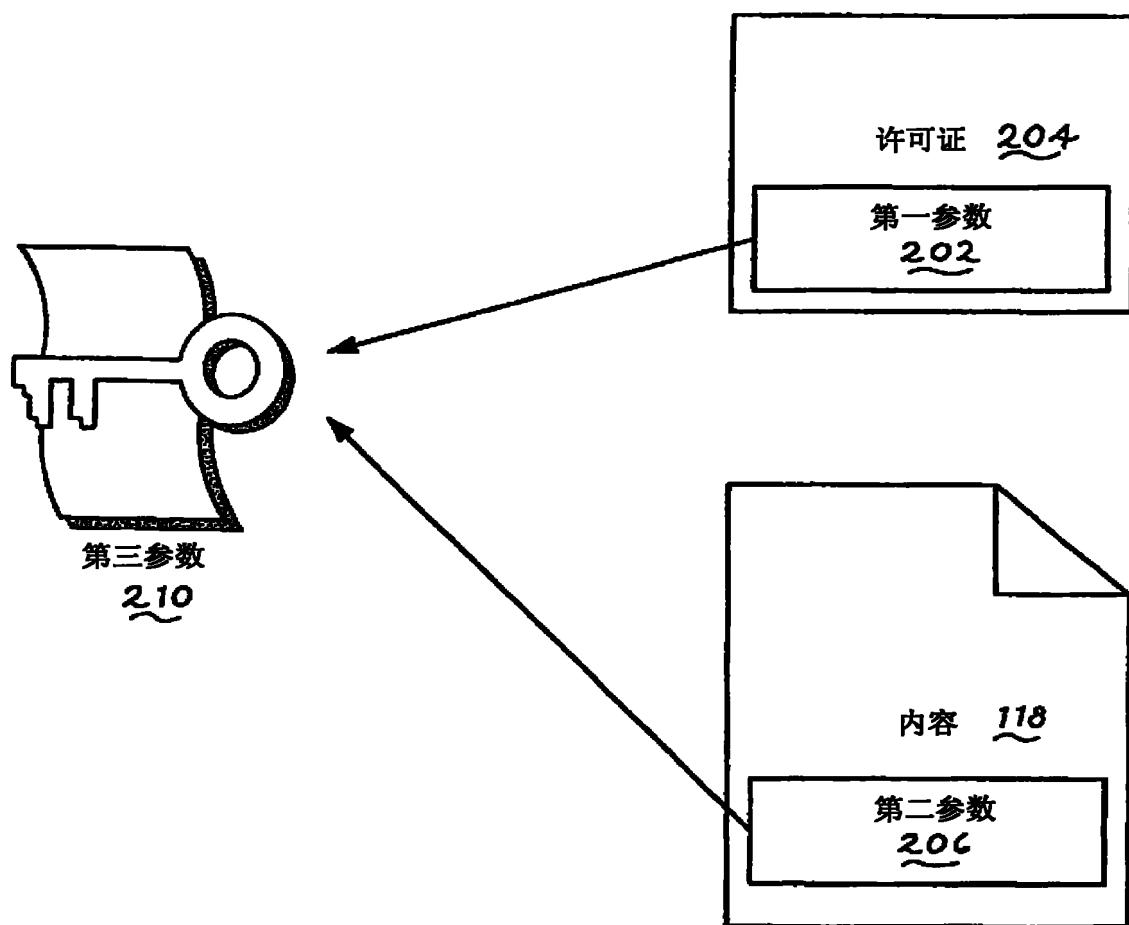


图 2

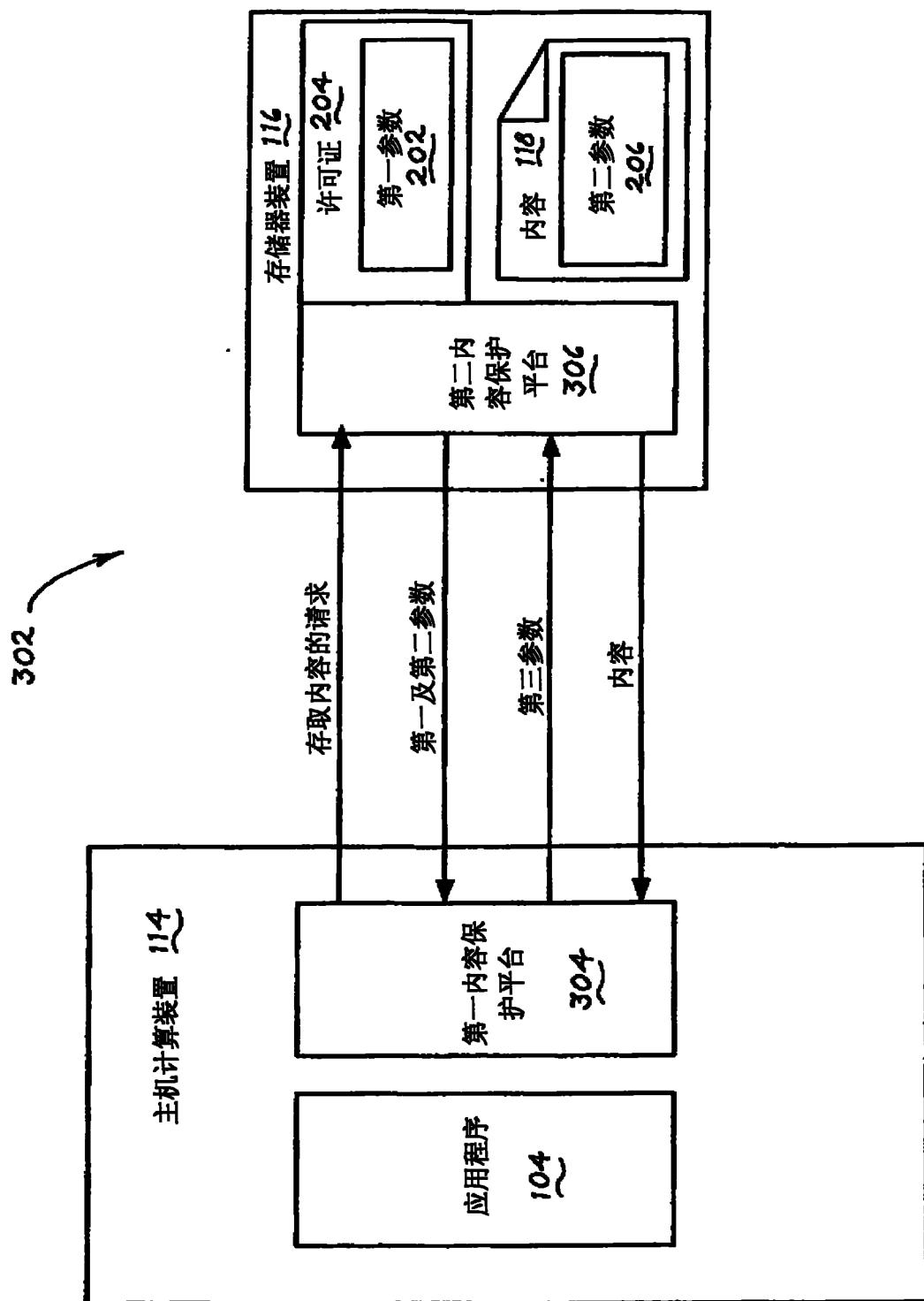


图 3

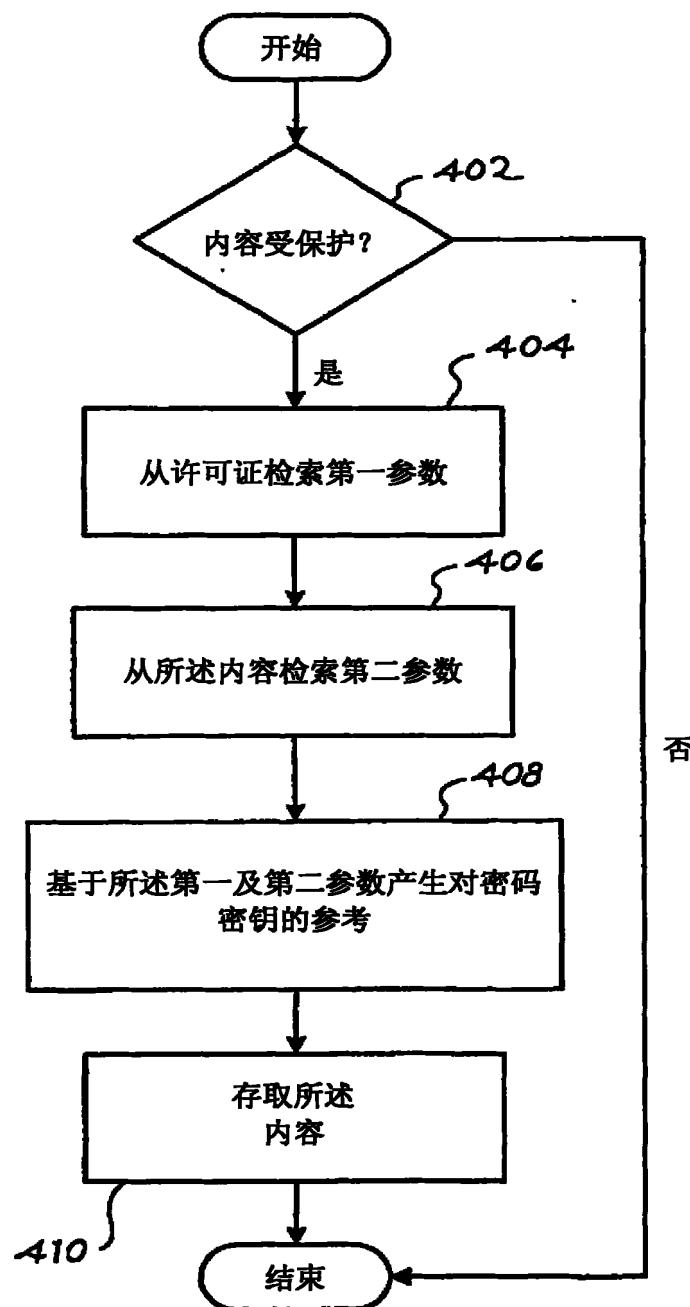


图 4

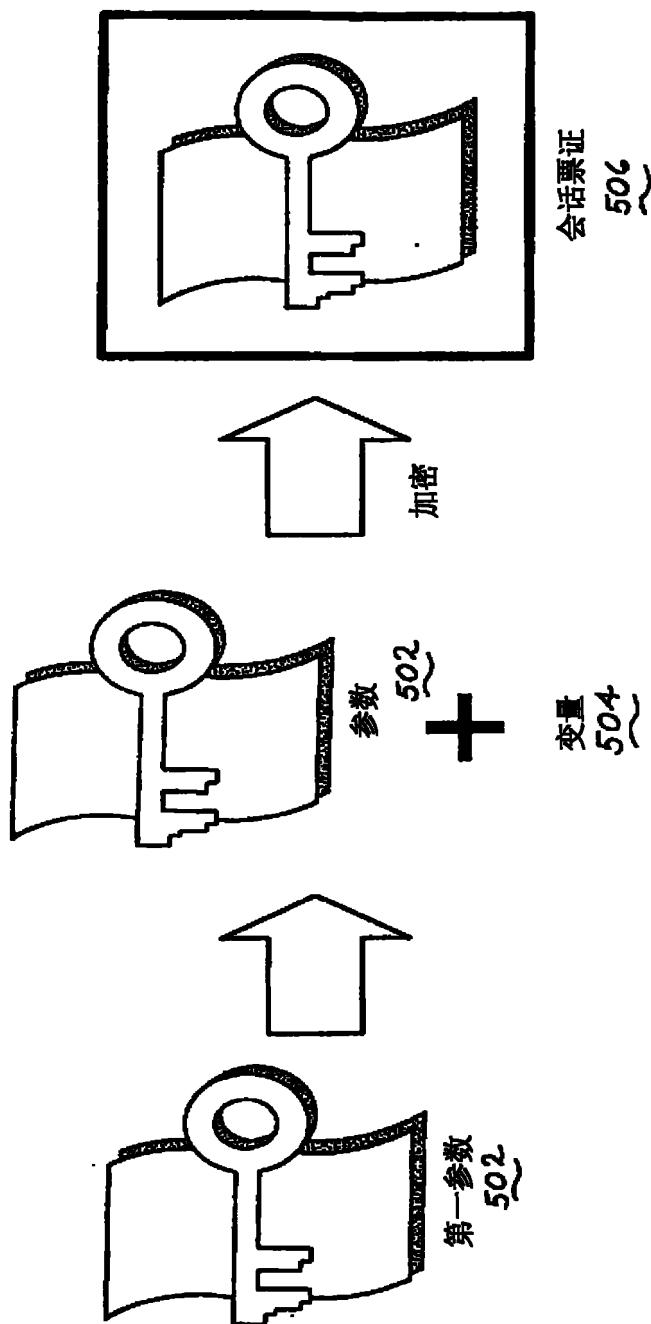


图 5

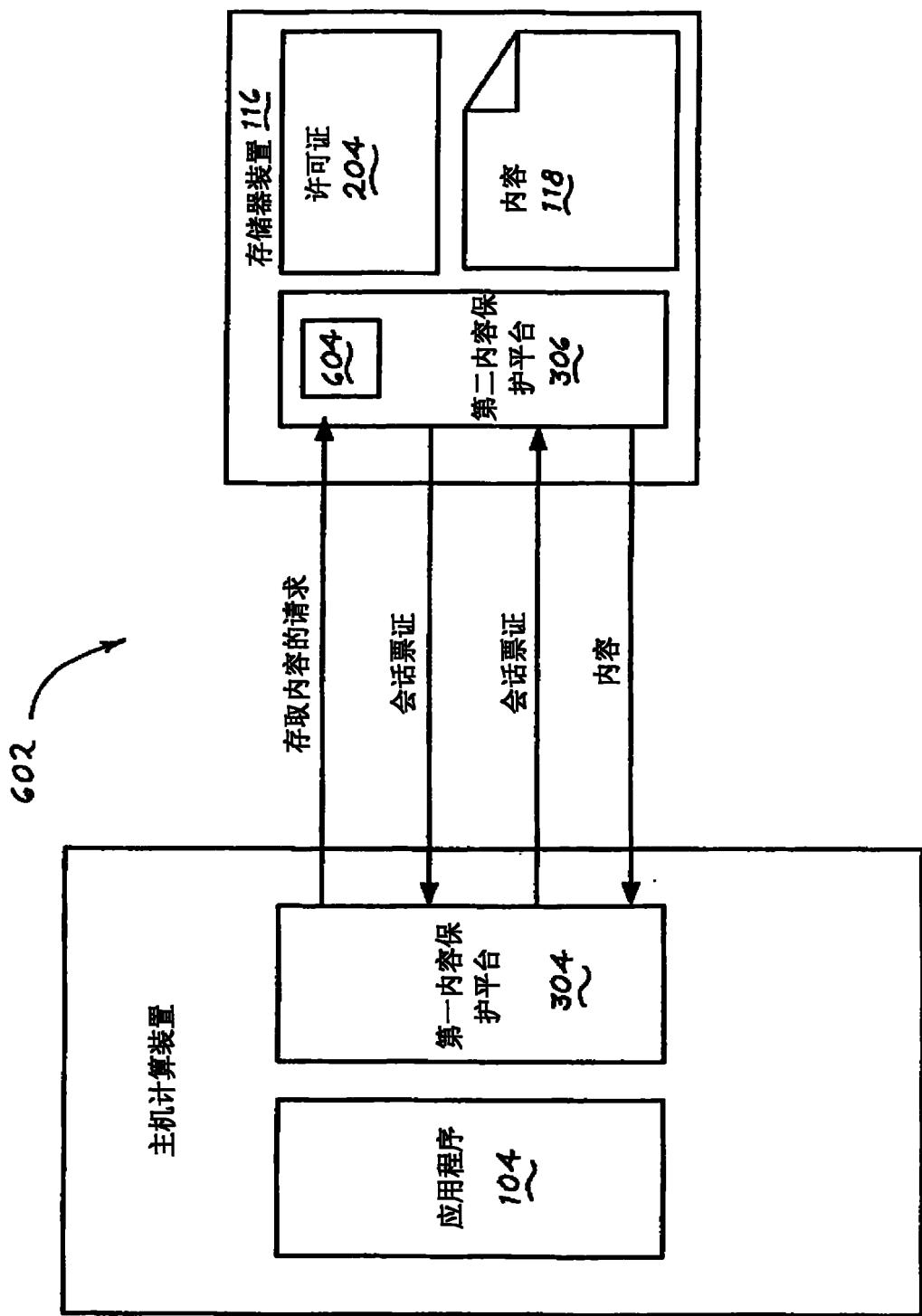


图 6

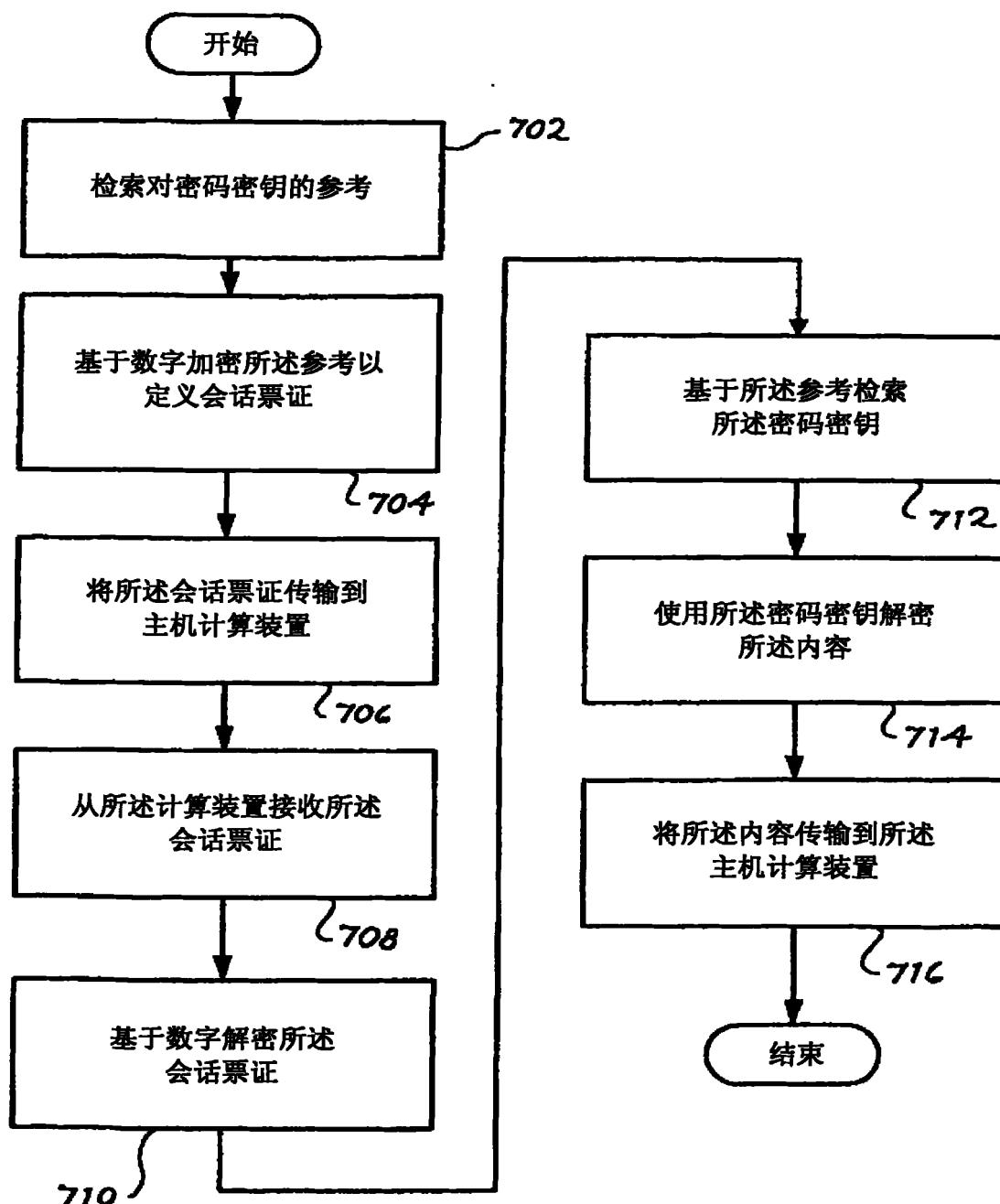


图 7

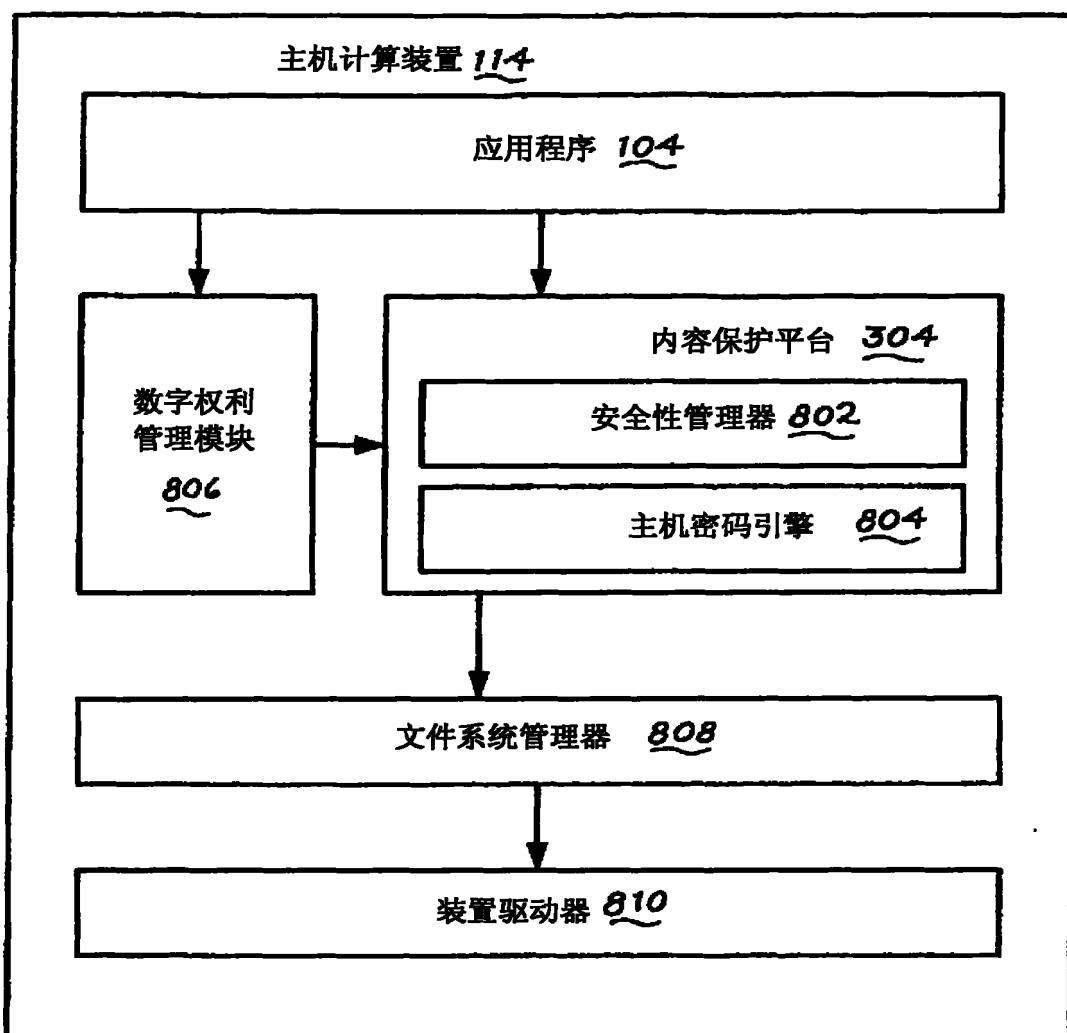


图 8

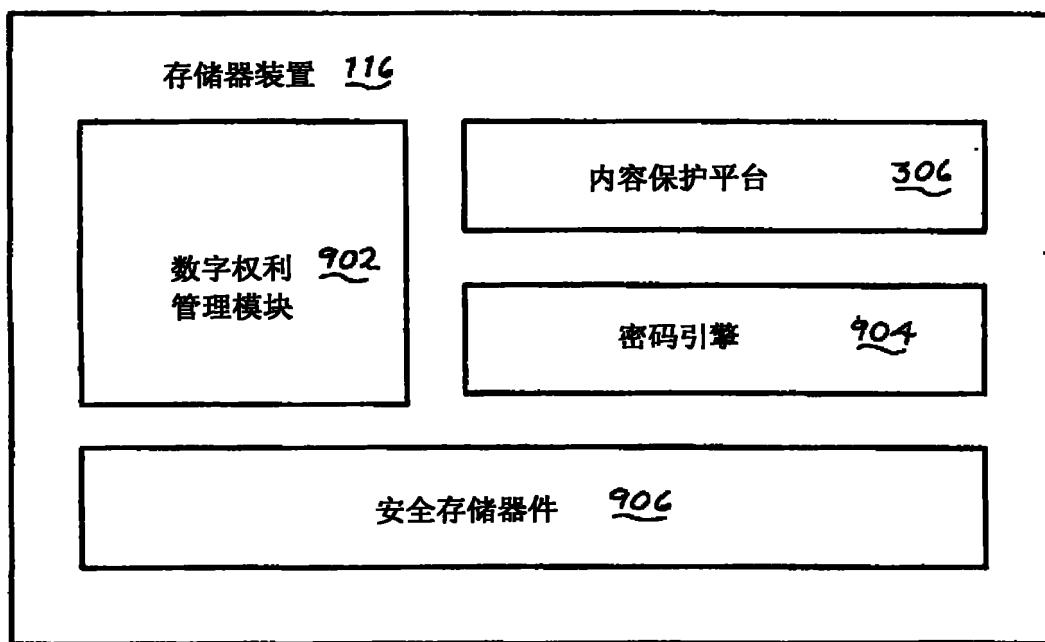


图 9

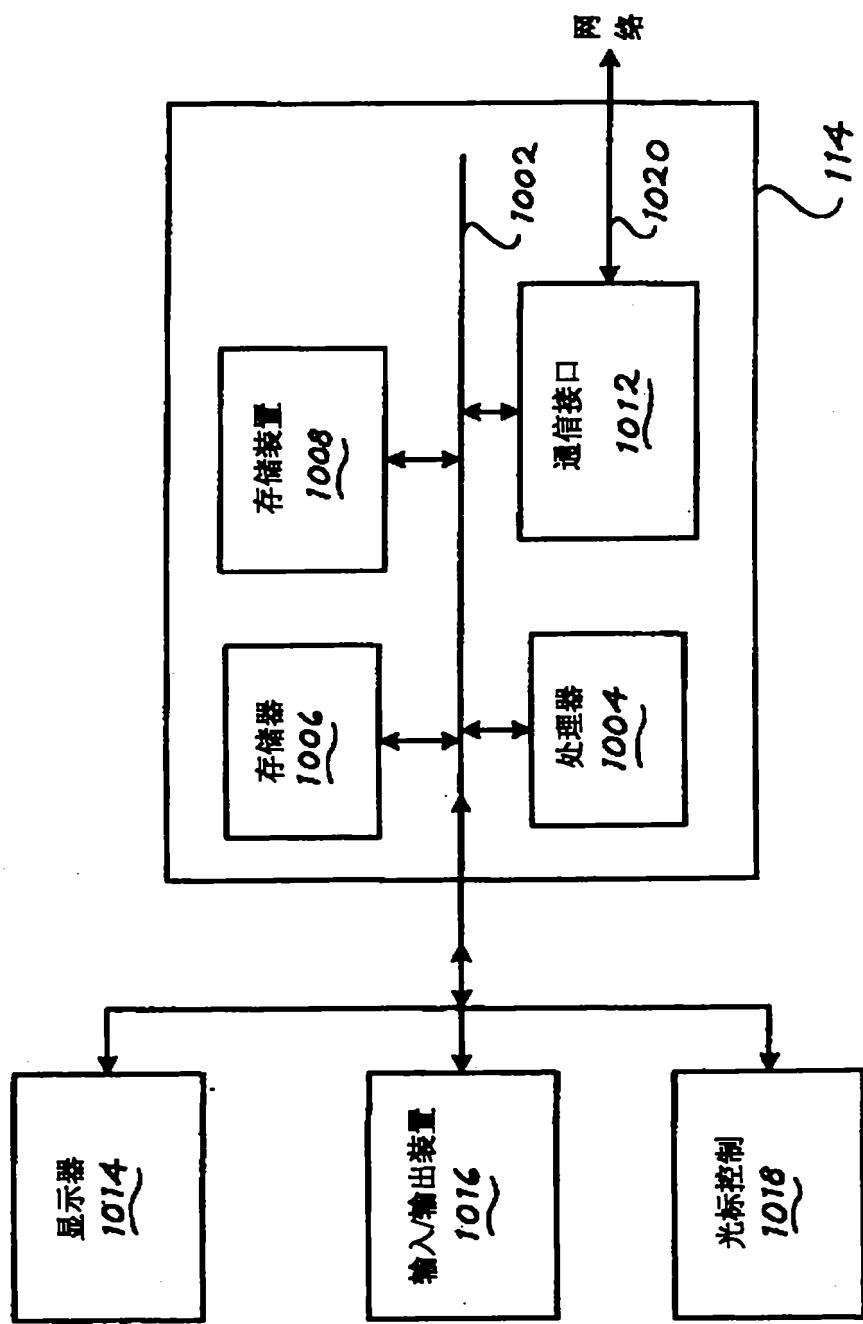


图 10

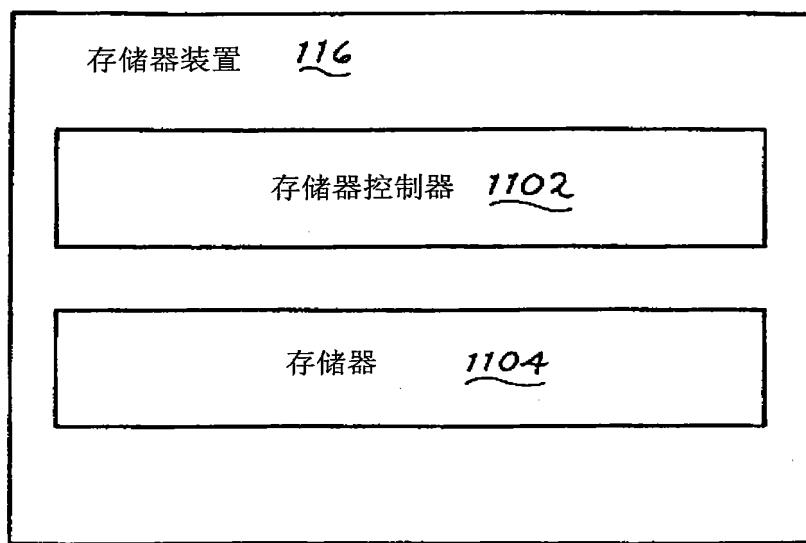


图 11