



(12) 发明专利

(10) 授权公告号 CN 1645394 B

(45) 授权公告日 2012. 09. 05

(21) 申请号 200510009413. 7

(56) 对比文件

(22) 申请日 2002. 01. 31

EP 0795809 A2, 1997. 09. 17, 全文.

(30) 优先权数据

审查员 吴少鸿

09/773, 716 2001. 01. 31 US

(62) 分案原申请数据

02107711. 8 2002. 01. 31

(73) 专利权人 美国索尼电脑娱乐公司

地址 美国加利福尼亚州

(72) 发明人 茶谷公之 D·S·马林森

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 张志醒

(51) Int. Cl.

G06F 21/00(2006. 01)

G06F 1/00(2006. 01)

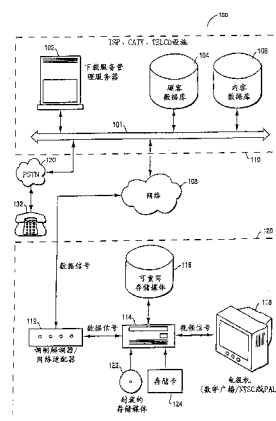
权利要求书 2 页 说明书 11 页 附图 8 页

(54) 发明名称

安全分销计算机软件产品的方法和系统

(57) 摘要

一种用于受限使用或受限数字软件产品的产品分配和支付系统。包括要被租借的软件产品数字内容数据通过可拆卸的本地存储媒体,如 DVD 或 CD-ROM 盘或通过网络连接可为顾客使用。产品数字内容可通过计算机或游戏控制台在客户位置处被访问和回放。软件产品可包括受限使用产品,其使用次数或使用期间受到限制。允许顾客使用他的计算机或回放控制台来下载和购买产品。产品购买信息被编码和传递到内容分配器。当经过播放的预置时间或次数时,软件程序被冻结并且不允许访问。在本发明的一个实施例中,执行两用公钥/私钥加密系统来在提供软件产品的服务器和顾客计算机系统之间传送产品和使用信息。



1. 一种用于提供对受限的使用数字软件标题进行访问的系统,包括:

服务器网络,它包括服务器计算机、存储用户信息的客户数据库和存储多个软件标题的内容数据库;

客户计算机,由用户操作,并且配置来回放选择的多个软件标题;

所述客户计算机的可拆卸的存储媒体,所述可拆卸的存储媒体在其上具有包括至少一个用户标识符(ID)的数据结构,其中服务器计算机向客户计算机的用户分配软件标题,并且使用包括用户标识符的信息和指导用户使用软件标题的购买选项来加密软件标题;

其中,用户向服务器计算机传送解密信息,以提供对分配给用户的软件标题的访问,并使用公钥/私钥加密系统加密软件标题,而其中用户公钥被指定并传送给用户,而客户控制台公钥在客户计算机的可拆卸的存储媒体中被指定和编码,并且用户私钥和客户控制台公钥被用于对标题私钥进行双加密,其中,

用标题公钥加密软件标题;为了启动过程,用户向服务器计算机提供用户信息;服务器计算机用用户信息生成用户公钥和用户私钥对;服务器计算机然后将用户A密钥反传给用户;然后为用户生成包含控制台A密钥和控制台B密钥的控制台公钥/私钥对;用户利用用户公钥对控制台公钥加密并将其传送给服务器计算机;用户接着将软件标题ID传送给用于待购软件标题的服务器计算机;服务器计算机检索指定的软件标题的标题私钥;标题B密钥是与用于加密指定软件标题的标题公钥相对应的私钥;然后,服务器计算机利用用户私钥和控制台公钥提供的加密将标题B密钥传送给用户;利用从服务器计算机得到的标题私钥对加密的软件标题进行最后解密后,用户能自由访问该软件标题。

2. 根据权利要求1的系统,其特征在于,软件标题通过可读出盘媒体向用户分配。

3. 根据权利要求1的系统,其特征在于,服务器计算机通过将客户计算机连接于服务器计算机的通信链路向用户分配软件标题。

4. 根据权利要求2的系统,其特征在于,用户使用经公共交换电话网连接于服务器计算机的电话将解密信息传送给服务器计算机。

5. 根据权利要求3的系统,其特征在于,用户通过通信链路向服务器计算机传送解密信息。

6. 根据权利要求1的系统,其特征在于,购买选项包括使用软件标题预置的时间周期。

7. 根据权利要求1的系统,其特征在于,购买选项包括使用软件标题预置的访问周期。

8. 根据权利要求1的系统,其特征在于,客户计算机是交互式的游戏计算机,软件标题包括可由客户计算机执行的交互式计算机游戏。

9. 一种配置和适于通过通信网络连接于一个或多个客户计算机的服务器计算机,该服务器计算机包括:

配置和适于存储用户信息的客户数据库,和存储多个软件标题的内容数据库;

应用户请求,配置和适于从该多个软件标题向一个或多个客户计算机的客户计算机的用户分配软件标题的分配模块;

配置和适于使用包括用户标识符(ID)的信息和指导用户使用软件标题的购买选项来加密软件标题的加密模块;和

配置和适于从用户接收解密信息并一经确认该解密信息即提供对软件标题的访问的解密模块;

其中,使用公钥 / 私钥加密系统加密软件标题,而其中用户公钥被指定并传送给用户,客户控制台公钥在客户计算机的可拆卸的存储媒体中被指定和编码,并通过通信网络在服务器计算机和客户计算机之间传送软件标题和解密信息,并且用户私钥和客户控制台公钥被用于对标题私钥进行双加密,其中,

用标题公钥加密软件标题;为了启动过程,用户向服务器计算机提供用户信息;服务器计算机用用户信息生成用户公钥和用户私钥对;服务器计算机然后将用户 A 密钥反传给用户;然后为用户生成包含控制台 A 密钥和控制台 B 密钥的控制台公钥 / 私钥对;用户利用用户公钥对控制台公钥加密并将其传送给服务器计算机;用户接着将软件标题 ID 传送给用于待购软件标题的服务器计算机;服务器计算机检索指定的软件标题的标题私钥;标题 B 密钥是与用于加密指定软件标题的标题公钥相对应的私钥;然后,服务器计算机利用用户私钥和控制台公钥提供的加密将标题 B 密钥传送给用户;利用从服务器计算机得到的标题私钥对加密的软件标题进行最后解密后,用户能自由访问该软件标题。

10. 根据权利要求 9 的服务器计算机,其特征在于,购买选项包括下面之一:使用软件标题预置的时间周期或使用软件标题预置的访问次数。

11. 根据权利要求 10 的服务器计算机,其特征在于,客户计算机是交互式的游戏计算机,软件标题包括可由客户计算机执行的交互式的计算机游戏。

12. 根据权利要求 11 的服务器计算机,其特征在于,软件标题通过可由客户计算机访问的可读盘媒体分配给客户计算机,用户经电话系统将解密信息传递给服务器计算机。

安全分销计算机软件产品的方法和系统

技术领域

[0001] 概括地说,本发明涉及计算机网络,尤其涉及通过计算机网络分销和租用受限使用软件产品的系统。

背景技术

[0002] 大容量数字媒体的广泛接受已经显著影响了计算机程序和普通娱乐产品的分配和销售。越来越多地,数字媒体例如 CD-ROM(光盘-只读存储器)和 DVD(数字多能盘)媒体以及用于计算机和手提数字设备的可移动存储卡开始替代用于大范围产品分销的传统的模拟媒体例如磁带和 VHS 带。例如,音乐、电影、计算机游戏、计算机程序、甚至图书都越来越多地变成被封装和分配在数字媒体上,以便在 CD 播放器、计算机、DVD 播放器和其他数字设备上回放。

[0003] 而且,随着互联网和电子商务(“e-商务”)商业模式的出现,很多基于数字的数据产品例如计算机软件、游戏、音乐、电影和其它数字内容可以很方便地在计算机网络上推销。因为可以将不同类型的软件内容和产品程序化到大容量存储产品即当前数字媒体例如 CD-ROM 上,所以这些产品的传统分销模型就变得过时了。用服务器-客户端计算机网络下载数字内容和安全加密通信的实现大大便利了数字软件产品的购买。随着 e-商务模型继续得到改进和实施,这些产品的分配也正在经历着重要的变化。在很多情况下,用户不需要光顾商店和零售商店来购买包含软件产品的实物媒体。取而代之的是,产品可以直接被下载到用户的计算机上,用于存储和回放。利用安全信用卡和其他 e-商务支付方法,同样可以在线购买产品。

[0004] 尽管目前的 e-商务分销方法方便了完全由用户购买的标准产品的销售和购买,但很多类型的娱乐产品是受限使用的产品,这种产品通常只是作为实物封装产品而非下载内容获得的。这种产品的最好例子是仅短期出租的电影或计算机游戏。当前,这些临时或受限使用的产品的分配涉及到用户光顾出租地点,租用产品,然后在租期过后返还产品。与正在为无限使用或不受限制的所有权物品而开发的在线和离线 e-商务分销系统相比,这种用于受限使用产品的传统分销渠道有点麻烦并且是不利的。

[0005] 为了鼓励使用或租用受限使用的计算机产品或样品,必须开发利用当前计算机网络能力的方便的购买和销售方法。所以,需要一种允许内容提供商或分销商提供作为实物产品或可下载的内容的受限使用产品并且准确跟踪和结算所分配的产品的系统。

发明内容

[0006] 下面描述限时使用或受限制的数字软件产品的产品分销和支付系统。包含待租软件产品的数字内容数据通过可拆卸本地存储媒体例如 DVD 或 CD-ROM 盘或通过网络连接使用户可用。软件产品能通过计算机或游戏控制台在用户地点被访问和回放。用户被允许在在线销售模型下利用他的计算机或回放控制台下载和购买产品,或者在离线销售模型下接收包含软件产品的封装媒体。软件产品可以包含在播放次数或使用时间上受到限制的受限

使用产品。产品购买信息被编码并发送给产品分配商。当过了预设播放时间和次数之后，软件程序被冻结，不允许访问程序。在本发明的一个实施例中，实施双向公钥 / 私钥加密系统在提供软件产品的服务器和用户计算机系统之间传输产品和使用信息。用户通过在线或离线方式与产品分销商通信以解密被加密的软件产品。

[0007] 本发明的其他目的、特征和优点将通过以下结合附图所作的详细描述中变得清楚。

附图说明

[0008] 举例说明本发明，但本发明不限于附图中的图形，其中相同的参考标记表示相似的部件，图中：

[0009] 图 1 是实现本发明实施例的计算机网络系统的方框图；

[0010] 图 2A 是根据本发明一个实施例的用于下载的受限使用的软件产品的销售和付费步骤的流程图；

[0011] 图 2B 是根据本发明的一个实施例，图示在客户端 / 服务器计算机网络中销售软件产品的加密 / 解密过程；

[0012] 图 3 是用于本发明的离线销售实施例的销售受限使用软件产品的步骤流程图；

[0013] 图 4 是用于本发明的在线销售实施例的访问受限使用产品的步骤流程图；以及

[0014] 图 5 示出了根据本发明的一个实施例，包括加密识别信息和用户参数的交互式游戏软件产品的组成。

具体实施方式

[0015] 下面描述在计算机网络上用于软件产品的受限使用的软件销售和租用系统。在下面的描述中，为了达到说明的目的，提出了大量的具体细节以便透澈理解本发明。但是显然，对于本领域的普通技术人员来说，没有这些具体细节也可以实现本发明。在其他情况下，在框图表中示出了公知结构和装置以便于说明。最佳实施例的描述不限制所附权利要求的范围。

[0016] 本发明的各个方面可以在一个或多个执行软件指令的计算机上实现。根据本发明的一个实施例，服务器和客户计算机系统在计算机网络或标准电话线上传输和接收数据。访问、下载和操作数据的步骤以及本发明的其他方面通过服务器和客户计算机中中央处理单元 (CPU) 执行存储在存储器中的指令序列来实现。存储器可以是随机存取存储器 (RAM)、只读存储器 (ROM)、不变存储器例如大容量存储器或这些设备的任意组合。执行指令序列使 CPU 完成根据本发明实施例所述的步骤。

[0017] 指令可以通过网络连接从存储设备或一个或多个其它计算机系统装载到服务器或客户计算机的存储器中。例如，客户计算机可以响应服务器通过网络发送给客户的消息而向服务器计算机发送一序列指令。当服务器通过网络连接接收指令时，它将指令存储在存储器中。服务器可以存储指令留待以后执行，或者当这行指令通过网络到达时执行这些指令。在一些情况下，CPU 可以直接支持下载的指令。在另一些情况下，CPU 不可以直接执行这些指令，而是通过解释这些指令的解释器来执行。在另一些实施例中，可以使用硬连接线路来代替或与软件指令组合来实现本发明。因此，本发明不限于硬件线路和软件的任何

特定组合,也不限于服务器或客户计算机执行的指令的任何特殊来源。

[0018] 图 1 是根据本发明的一个实施例,用于实现受限使用软件产品分配系统的计算机网络系统的方框图。图 1 的系统 100 能传输、执行和 / 或回放受限使用的软件产品。说明书和权利要求书正文中的术语“受限使用的软件产品”可以理解成指可下载的数字数据的集合,所述数字数据可以包括以下数据中的任何一种:视频线性流数据,例如 MPEG 或 MPEG2 格式的动画数据;线性音频流数据,例如 MP3 格式的音乐数据;二进制程序数据;计算机游戏;二进制文本数据;或者这种数据或类似数据的任何组合。通常,受限使用的软件产品不包括单用于提供网络访问的服务或数据,例如主要功能只是建立网络连接的网页浏览器软件或协议处理程序。

[0019] 如图 1 所示,系统 100 包括:包含下载服务管理服务器 102 的服务器端系统 110,客户数据库 104,内容数据库 106,它们通过局域网 (LAN) 101 互相连接。受限使用的软件产品内容通常存储在构成服务器端系统 110 的一部分的内容数据库 106 中。客户数据库 104 存储与通过双向网络 108 访问下载服务器 102 的个别客户有关的数据集合。每个个别客户的数据包括客户的姓名、家庭住址、年龄、性别、职业、收入、爱好、购买历史、偏好以及可能对正在使用该系统的卖主或广告商有用的其它描述信息。这种数据不是不变的,而是可以在基本内容数据的用户访问历史基础上可更新的。例如,可以更新数据来反映那些软件产品被访问和 / 或给定类别(例如,音乐类型、电影类型等等)的软件产品被访问多少次。这使得内容提供商和广告商对给定客户更有效地定制他们的消息。

[0020] 下载服务管理服务器 102 是配置成处理来自用户的下载请求的服务器系统。LAN101 上的路由器通常可以便于访问包含若干服务器其中之一的服务器 102,它直接向下载管理服务器 102 发出请求。当服务器 102 接收来自用户的请求时,服务器执行从内容数据库 106 请求的软件产品的下载。然后通过已知的网络协议标准例如文件传输协议 (ftp) 经网络 108 传输包含该产品的数据。

[0021] 网络 108 通常是连接用户端硬件和设在系统服务器端上的下载服务管理服务器 102 的双向数字通信网络。由于当前的技术,CATV(有线电视)双向网络、ISDN(综合服务数字网)、DSL(数字用户线)或 xDSL 高速网络是实现本发明实施例的必要网络连接的现有网络架构实例。在一个实施例中,网络 108 可以表示互联网,在这种情况下,服务器 102 通常执行网页服务器处理,以 HTML 数据的形式将数据传送给执行网页浏览器处理的客户计算机。

[0022] 图 1 所示的系统配置的客户端 120 包括调制解调器或网络适配器 112、其中利用了可拆卸存储媒体 122 的网络游戏控制台 114、以及 TV 监视器或与游戏控制台 114 相连接的任何其他合适的显示设备 118。调制解调器或网络适配器 112 是用于连接客户端硬件的设备,在这种情况下,是连接到网络 108 的游戏控制台 114。例如,如果网络 108 是 CATV 网络,调制解调器 112 可以以电缆调制解调器设备来实现;如果网络 108 是 ISDN 网络,则调制解调器 112 可以以终端适配器来实现。

[0023] 在本发明的一个实施例中,可拆卸存储媒体 122 存储交互式或非交互式附属内容的集合,如计算机游戏、电影、音乐片段、或者可由视频图象、动画、声音、java 程序等组成的广告。在一个实施例中,可拆卸存储媒体 122 包括 CD-ROM 或 DVD 盘。对于图 1 所示的实施例,可拆卸存储媒体 122 是存储供用户使用的的一个或多个软件产品的封装的存储媒体。这

种产品可以包括计算机游戏、音频内容、视频内容等。封装的存储媒体 122 也可以包括下载管理软件程序, 下载管理软件程序控制软件产品数据从内容数据库 106 下载到游戏控制台 114 中。客户系统 120 还包括与网络游戏控制台 114 连接的可重写存储媒体 116。在正常操作期间, 网络游戏控制台 114 将数据从封装的存储媒体 122 传送到可重写存储媒体上以便临时或中期存储和执行。可重写存储媒体 116 也可以用于存储客户系统 120 通过网络 108 下载的数据或程序。可重写存储媒体 116 可以通过端口连接附加到游戏控制台 114 上的硬盘驱动器 (HDD)、闪存设备或其他适当的非易失性存储设备来实现。

[0024] 对于图 1 所示的实施例, 网络游戏控制台 114 还具有安装存储卡 124 的接口端口。这种存储卡可以以专用卡格式、或标准格式设备例如 PC/MCIA 格式或类似卡格式来实现。存储卡 124 存储安装卡的特殊网络游戏控制台 114 所特有的各种固件参数和操作环境数据。例如, 可以用存储卡存储分配给特殊游戏控制台的标识号码 (ID)。在特定应用中, 可以用存储卡存储特定软件产品, 例如要在游戏控制台上回放或执行的计算机游戏或其他程序。

[0025] 通常, 网络游戏控制台 114 是交互式数字内容的可联网的回放设备。这种游戏控制台 114 通常利用封装的存储媒体 122 作为非联网环境中的内容分配媒体。换言之, 在普通使用情况下, 即使游戏控制台 114 不与网络 108 连接, 游戏控制台 114 也能回放包含在封装的存储媒体 122 上的媒体, 它通常是交互式视频程序 (例如游戏)。对于该实施例, 软件产品的分配称为“离线”分配实施例。在离线实施例中, 用户也可以与服务器系统 110 通信。在这种情况下, 将服务器与通过电话 132 访问用户的公共交换电话网 (PSTN) 130 连接。电话 132 可以是按键电话机, 它响应服务器系统提供的命令项而允许用户进行字母数字输入。或者, 用户用电话向服务器系统 110 传送声音命令或者和与服务器系统 110 相关的操作员讲话。

[0026] 在本发明的另一个实施例中, 封装的存储媒体 122 被用在网络环境中, 与下载的通过网络连接 (例如通过调制解调器 112) 检索到基本内容一道操作, 以便提供连接的或相关的用户定制的附属内容。对于这个可替换的实施例, 软件产品的分配被称为“在线”分配实施例。这种附属内容可以通过基本内容提供商服务器系统 110、或附属内容提供商或其他主要内容提供商 (未示出) 维护的独立服务器来提供。

[0027] 服务器可以实现向操作网络游戏控制台 114 的用户分配软件产品内容的各种不同方法。如上所述, 产品内容通常包括受限使用的数字内容, 例如限制用户使用的计算机游戏、音乐片段、全长音频和视频程序、电影、静止图片数据和其它相似类型的内容。例如, 内容数据可以包含出租一段特定时间的游戏或电影录像。在租期过期后, 用户不能再使用内容数据。内容还可以包括与基本内容相关的宣传或广告数据, 例如电影预览、演示版游戏、样品数据、和其他便于用户选择所分配的产品的相似类型的内容。编码在存储卡 124 或其他类似存储装置上的网络游戏控制台 114 的 ID 用于方便下载和执行在网络 108 上或通过封装的存储媒体 122 从服务器分配的软件产品。在一个实施例中, 网络游戏控制台用户建立服务器 102 管理的用户帐户。与用户帐户相关的数据被存储在客户数据库 104 中。用户被颁布一个 ID 号, 该 ID 号用于方便购买和分配用户请求的软件产品。

[0028] 在本发明的一个实施例中, 用户用网络游戏控制台 114 回放购买的或租用的软件标题。至少一个将被客户使用的编码软件产品 (也称为“软件标题”) 被存储在大容量 RAM

媒体上,所述媒体例如收藏在网络游戏控制台 114 中的 CD-ROM/DVD-ROM 上或硬盘等上的未使用的大容量存储媒体。例如,在图 1 所示的实施例中,编码的软件标题可以设置在封装的存储媒体 122 上或下载到本地存储设备例如可重写存储媒体 116 上。在典型的离线实施例中,其中,在不与网络连接的回放系统 114 上回放软件产品,该产品通过用户从零售或分配地点得到,或者响应用户请求作为认购过程的一部分送给用户。而且,利用离线装置例如电话 132 在用户和服务器之间完成用于解码编码软件产品的通信。

[0029] 图 2A 示出了根据本发明的一个实施例编码和分配受限使用软件产品的步骤。在步骤 202 中,包含待分配的软件标题的程序码被加密,或者安全地存储在大容量存储媒体上,所述媒体例如包含封装的存储媒体 122 的 CD-ROM 或 DVD 盘。在步骤 204 中,为加密的软件标题的分配建立适当的安全机制。在一个实施例中,利用双向公钥/私钥加密系统。在这种情况下,每个待分配的软件标题首先用用于这个标题的公钥加密。服务器必须访问待分配或租用的每个软件标题的私钥。在步骤 206 中,将包含加密的软件标题的可移动存储媒体分配给用户。在一个实施例中,用户被发送或得到包含该标题的封装媒体 122 例如盘或其他存储媒体的拷贝。这构成了软件产品的离线分配。在另一个实施例中,网络游戏控制台 114 可以通过计算机网络 108 连接服务器。对于这个实施例,用户能通过网络下载软件标题,以存储在他们的网络游戏控制台内的本地硬盘驱动器或存储器中。这构成了软件产品的在线分配。

[0030] 在步骤 208 中,客户解密加密的软件产品,从而获得对产品的访问权。解密步骤可以通过离线装置或在线装置完成。对于离线解密实施例,用户用电话 132 或类似设备将适当的解密信息例如私钥或私人密码信息传送给服务器。服务器则返回一个允许访问软件产品的代码。用户可以通过按键式电话或声音命令利用字母数字入口将给服务器的解密信息直接提供给系统或操作员。在在线实施例中,客户系统 120 通过网络 108 与服务器系统 110 连接,客户通过游戏控制台 114 将解密信息传送给服务器。

[0031] 在步骤 210 中,为用户提供与分配的软件标题的购买选项相关的选择。通常,有两种购买选项,用户根据被访问的程序的次数付费使用(例如游戏播放的次数),或者通过访问程序的耗时量来付费使用(例如总的游戏时间)。或者,也可以是这两种购买选项的组合。例如,程序或游戏的使用可以根据一组访问号被限制,每个访问号有特定的时间长度。

[0032] 图 2B 是根据本发明的一个实施例,在客户/服务器计算机网络中分配软件产品的加密/解密过程。图 2B 更详细地示出了图 2A 中示出的加密过程。图 2B 示出了在网络上通过用户 220 在客户计算机(“控制台”)和服务器计算机 222 上执行的加密/解密过程。服务器计算机 222 提供用户 220 请求的软件产品(也称为软件标题)。为了保证软件产品在网络上安全分配,用户和服务器之间的交换包含多层公钥加密(PKCS),以便能通过用户解密来自服务器的存储在存储媒体(例如磁或光盘)上的软件产品内容。通常,对于图 2B 所示的过程,服务器 222 对能利用在客户计算机(控制台)上生成的匹配私钥解密的密钥进行加密。服务器 222 生成一对密钥(用户 A 和用户 B)并将其中一个密钥(用户 A)传送给用户。该密钥允许用户对软件产品的内容进行解密。服务器利用从用户传送的密钥对该密钥加密,然后再次对具有其密钥对的相应密钥(用户 B)的加密密钥进行加密,并将两个加密密钥传送给用户。

[0033] 对于图 5 所示的实施例,用标题公钥(标题 A)加密软件。为了启动过程,用户 220

向服务器 222 提供信息。服务器 222 用用户信息生成用户公钥（用户 A）和用户私钥（用户 B）对 226。服务器 222 则将用户 A 密钥反传给用户 220。然后为用户 220 生成包含控制台 A 密钥 228 和控制台 B 密钥 229 的控制台公钥 / 私钥对。用户利用用户公钥（用户 A）对控制台公钥（控制台 A）228 加密并将其传送给服务器 222。用户 220 接着将标题 ID 传送给用于待购软件产品的服务器 222。服务器 222 检索指定的软件产品的标题私钥（标题 B）232。标题 B 密钥是与用于加密指定软件产品的标题公钥（标题 A）相对应的私钥。然后，服务器 222 利用用户私钥（用户 B）和控制台公钥（控制台 A）提供的加密将标题 B 密钥传送给用户 220。然后，利用从服务器 222 得到的标题私钥（标题 A）对加密的软件标题进行最后解密后，用户就能自由访问该软件标题。。

[0034] 在被服务器 222 用标题公钥（标题 A）加密的软件标题解密后，用户将购买信息 240 传送给服务器 222。利用购买信息，服务器 222 生成使用计数器 242。使用计数器可以以电子令牌体现，电子令牌以每个使用、时间段或其他测量单位被记入借方。利用控制台 A 和用户 B 密钥对计数器加密并传送给用户 220。

[0035] 如图 2A 所示，利用用户 220 提供的用户信息由服务器 222 生成用户公钥 / 私钥（用户 A / 用户 B）对 226。在一个实施例中，为用户 220 生成一个用户密钥对 226 在所有的与服务器 222 的后序事务中使用，在服务器中，用于生成密钥对的用户信息是相关的。或者，在用户 220 和服务器 222 之间为每个不同的事务生成新的密钥对 226。

[0036] 控制台公钥 / 私钥对 228、229 由用户 220 生成。该密钥对可以利用硬件标识方法在客户计算机上生成，例如与客户计算机相关的唯一的序列码，或者在客户计算机内与硬盘驱动器相关的 ID 图形。对于该实施例，可以利用在客户计算机硬盘驱动器内存储和执行的授权软件生成密钥对。或者，密钥对 228、229 可以利用硬件授权设备例如道尔芯片来生成。通常，道尔芯片是基于硬件的安全设备，它附接到客户计算机的串行或并行打印机端口，使用嵌在密钥内部的代码或密码控制对软件应用的访问。对于该实施例，用户 220 请求的软件产品仅在道尔芯片附接到客户计算机时才能运行。

[0037] 如图 2A 所示，利用图 1 的系统有四种可能的分配和客户访问实施例。在第一实施例中，利用封装的存储媒体 122 向离线客户分配软件产品，客户利用电话 132 向离线服务器提供解密信息。对于该实施例，游戏控制台用作独立设备，不与服务器系统 110 连接。

[0038] 对于剩下的实施例，游戏控制台 114 通过直接通信或计算机网络连接服务器系统 110，在客户事务的分配和 / 或解密方面利用该网络的某一方面。在第二实施例中，软件产品在网络 108 上通过产品的传送分配给在线客户，客户通过网络 108 和游戏控制台 114 向服务器系统 110 提供解密信息。在第三实施例中，软件产品通过封装的存储媒体 122 的使用分配给离线客户，客户通过网络 108 和游戏控制台 114 向服务器系统 110 提供解密信息。在第四实施例中，软件产品在网络 108 上通过产品的传送分配给在线客户，客户利用电话 132 向离线服务器系统 110 提供解密信息。

[0039] 图 3 是用于本发明的离线分配实施例的分配受限使用的软件产品的步骤流程图。图 3 总体示出了在图 1 所示分配系统的用户端和服务器端上执行的步骤。对于该实施例，假设用户对待执行或回放的出租软件产品操作网络游戏控制台 114。网络游戏控制台 114 可以以硬件系统来实现，硬件系统提供设置在可重写存储媒体 116 或封装的存储媒体 122 上存储的媒体上的内容的数字回放，并且可以包含在个人计算机、专用游戏系统（例如

Sony® Playstation®)、无线手提设备(例如个人数字助理PDA)或者其它交互式计算机娱乐系统中。为了达到说明的目的,网络游戏控制台 114 统称为“交互式计算机娱乐系统”。

[0040] 对于图 3 流程图所示的离线实施例,为了产品分配的目的,交互式计算机娱乐系统作为独立游戏播放或内容回放系统进行操作,不与网络 108 连接。通常,用户通过电话线 130 与服务器 102 交互,与客服人员会话或者通过经电话 132 键盘输入的字母数字代码进行通信。

[0041] 在一个实施例中,本发明的方面用在产品分配系统中,在该系统中,用户与服务器 102 建立帐户以便接收软件产品。因此,在图 3 的步骤 302 中,用户与服务器建立帐户以购买和接收软件产品。为了访问他或她的帐户,用户利用按键式电话打电话到服务器中,利用电话上的数字键盘输入帐户和购买信息。服务器系统建立有预置菜单,以指示用户输入需要的信息来完成购买事务。例如,一旦用户已经建立了一个帐户,则向用户发放一个 ID 号。在步骤 302 中,用户利用按键式电话 132 输入他或她的 ID 号。

[0042] 为了在客户端用户和服务器之间建立安全连接,服务器建立数据加密/解密系统。这样,在步骤 304 中,服务器为用户生成用户公钥和用户私钥。在步骤 306 中,服务器向用户提供用户公钥。对于用户通过电话线与服务器通信的实施例,该信息可以通过读出用户公钥的语音合成器经电话或类似装置传送给用户。或者,客服人员或操作人员可以读出给用户的公钥信息。

[0043] 包含所选软件产品的封装的媒体被分配给用户。这通常可以在授权过程之前的任何时候进行,并且可以通过若干方式完成,例如向客户发送封装的媒体或者通过零售商提供对媒体的访问。利用交互式计算机娱乐系统,用户指示他或她将租用或购买哪个受限使用的软件标题。用户可以提交显示待租程序或内容标题的选择菜单。在步骤 308 中,用户将他或她的用户公钥输入到交互式计算机娱乐系统中。在步骤 310 中,交互式计算机娱乐系统将待租的软件标题的 ID 号加密到用户公钥中。交互式计算机娱乐系统还将存储卡公钥加密到用户公钥中。在一个实施例中,存储卡公钥是根据存储在存储卡中的信息生成的并被编程到使用时插入到交互式计算机娱乐系统内的存储卡中。步骤 312 中,交互式计算机娱乐系统则将该加密的信息显示在连接系统的显示设备的屏幕上。

[0044] 提供给用户的加密信息包含用户提供给服务器来验证用户被授权接收和使用该产品的解密信息。如图 2A 所示,用户根据游戏控制台是否通过计算机网络与服务器系统连接而将解密信息传送给离线或在线用户。因此,在步骤 316 中,确定是否用户通过在线装置或离线装置连接到服务器上。如果用户不直接连接服务器(离线),用户通过电话将显示在屏幕上的解密信息传送给服务器,步骤 318。如果游戏控制台通过直接通信网络连接服务器,则用户通过网络线将解密信息传送给服务器,步骤 320。

[0045] 在用户将解密信息传送给用户之后,服务器证实该用户被授权接收产品。在一个实施例中,可以对服务器编程,为用户提供与产品购买或租用选项有关的菜单选择。通过接受字母数字用户输入的预定一组菜单引导用户。或者,可以实施声音识别系统,使得用户利用自然语言输入键入命令。在步骤 322 中,用户跟随服务器的指令,选择他或她想购买的选项。对于受限使用的产品,可以提示用户在租用一段时间产品或租用特定访问次数(游戏运行次数)或其组合之间选择。在用户已经建立包括待支取资金的一个帐户的实施例中,从用户帐户上支付适当的购买和租用费用。或者,可以建立其他付费方法,例如通过信用卡

在电话上付费或者其他电子资金传送方法。

[0046] 从步骤 324 继续过程,其中服务器从步骤 318 或 320 中接收的解密数据(用户公钥数据)中检索软件标题的 ID 号和交互式计算机娱乐系统的存储卡的公钥。服务器则从数据库检索软件标题的相应私钥并将其加密到存储卡公钥和用户私钥,步骤 326。在一个实施例中,软件标题的软件程序被存储在紧密或疏松地连接于服务器 102 的内容数据库 106 中。在这一步骤中,服务器还对用户选入存储卡公钥和用户私钥中的购买项数据进行加密。

[0047] 在步骤 328 中,服务器将加密的私钥和购买项信息传送给用户。对于图 3 所示的离线分配实施例,该信息可以通过电话 132 提供给用户。用户则将该加密的信息输入到交互式计算机娱乐系统中,步骤 330。在步骤 332 中,交互式计算机娱乐系统利用用户私钥解密数据并将解密的数据存储在存储卡上。

[0048] 对于图 3 的离线分配实施例,在封装的存储媒体例如盘 122 上提供所选标题的软件产品。用户选择时,用户在选择待访问的标题之前得到该媒体,或者在选择该标题之后由用户发送或获得。在用户将封装的存储媒体插入交互式计算机娱乐系统中之后,系统则引导软件标题,步骤 334。引导时,软件标题利用存储卡私钥解密标题的私钥和购买项信息。交互式计算机娱乐系统利用标题私钥解密软件标题,使得可以在系统上访问或播放它。

[0049] 在本发明的一个实施例中,购买项信息可以以表示游戏运行次数单位的“令牌”形式编码。这些令牌通过每次标题被重新启动或特定间隔的游戏时间的适当单位数进行更新。例如,对于游戏,在每次游戏结束时更新令牌。当分配的时间或者游戏剩余次数达到零时,标题冻结,不允许用户访问直至用户重建他或她的租用。

[0050] 图 3 所示的过程表示一个实施例,在该实施例中,游戏控制台 114 用在离线环境中,不通过网络连接与服务器 102 连接来进行分配,并且用作独立回放或游戏控制台。对于该离线模式,用户得到包含所选标题的封装的存储媒体,通过电话或其他方法与服务器 102 通信。在另一种在线分配模式下,游戏控制台通过通信或计算机网络 108 与服务器系统连接。

[0051] 图 4 是用于本发明在线分配实施例的受限使用的软件产品的分配步骤流程图。对于该实施例,网络游戏控制台 114 通过网络 108 与服务器连接并在在线模式下使用。对于在线实施例,作为网络游戏播放或内容回放系统来操作交互式计算机娱乐系统。因此,尽管它用作独立单元,但交互式计算机娱乐系统通过网络接口与网络 108 连接。这允许用户直接通过交互式计算机娱乐系统而不是通过离线装置例如电话或第二个网络计算机与服务器 102 通信。对于该实施例,在用户与服务器交互的某些步骤中,例如接收用户公钥和向服务器发送游戏和购买选择信息是利用在网络上直接与服务器通信的网络接口来进行的。提供菜单命令和选项的图形用户界面可以在连接网络游戏控制台 114 的监视器 118 上提供。

[0052] 在图 4 的在线分配实施例的一个版本中,编码的标题仍然提供在用户获得的封装的存储媒体上以便插入到交互式计算机娱乐系统中。在在线分配实施例的另一个版本中,所选软件产品的传送也是利用网络连接完成的。对于该实施例,服务器可以从数据库中检索软件标题的相应私钥并将其加密到存储卡公钥和用户私钥中。用于软件标题的软件程序可以存储在与服务器 102 紧密或疏松连接的内容数据库 106 中。在该步骤中,服务器还对用户选择进入存储卡公钥和用户私钥中的购买项数据加密。当用户请求时,服务器将所选的软件产品传送给网络交互式计算机娱乐系统,它又对适当的解密数据和受限使用信息进

行解密,引导软件。

[0053] 图 4 示出的多个基本处理步骤类似于图 3 示出的离线分配处理中执行的那些。主要的不同在于在步骤 406 中,服务器通过网络连接在线地向用户提供公钥。服务器通过网络连接将软件产品传送或下载到交互式计算机娱乐系统。一般地,这可在处理期间在任何时候发生。对于在线分配处理,用户可通过在线或离线方式与服务器计算机就解密信息进行通信。在步骤 416 中,确定用户在线还是离线地传送解密信息。如果是离线,则在步骤 148,用户经电话 132 将解密信息传送到服务器。如果是在线,用户经网络 108 将解密信息传送到服务器。在线分配处理的剩余步骤基本上类似于参考图 3 讨论的离线实施例。

[0054] 对于图 3 和 4 示出的处理,限制租借的软件产品的使用的参数体现在购买选择信息中,并且可作为时间标记或访问次数来表现。在本发明的一个实施例中,掌握着软件产品的受限访问的使用参数被编程到包含该产品的数字媒体中。图 5 表示可在图 1 的系统中使用的软件产品例子的构成。

[0055] 图 5 示出包括视频游戏的软件程序。游戏程序 500 通过技术上已知的过程被编程到数字媒体,如 CD-ROM 或 DVD 盘上。如图 5 所示,包含游戏程序 502 的软件程序或标题 500 具有与其相关的某些不同类型的编码段。游戏程序 502 包括构成游戏自身的可执行码。与游戏数据相关的是将游戏码的各段映射到其上存储标题 500 的物理盘上的扇区表 504。扇区表包括文件名、修改日期、校验和和其它与包括游戏程序 502 的模块相关的数据。

[0056] 在一个实施例中,一组程序使用参数 506 与游戏程序 502 相关。程序使用参数包括对游戏程序 502 的受限使用限制条件进行编码的变量。例如,程序使用参数可以是用于对游戏程序使用的消耗时间进行计数的计数值。在这种情况下,游戏程序可在基于时间的租借基础上来分配。当计数器到达某值时,阻止对游戏程序 502 的访问。或者,程序使用参数可以是对访问游戏程序的次数进行计数的计数值。一旦超出了预置访问次数,阻止对游戏程序的进一步访问。从而,使用程序使用参数,一旦经过了特定的租借周期,游戏程序或内容自动过期。这使得不再需要用户将媒体返回内容提供商,或者不需要向内容提供商证明产品被丢弃或不再被使用。

[0057] 在一个实施例中,软件包 500 也包括游戏 ID 部分 508。这个部分用于对系统识别游戏。游戏 ID 部分 508 也被用于编码某些加密数据,如由系统 100 使用的一些公钥 / 私钥数据,用来向用户分配游戏。

[0058] 对于图 1 中示出的实施例,软件产品分配模式使用一个方面,其中用户购买的物品不必要是产品媒体自身,而是可用于打开在媒体上存储的程序的密钥。用户传送的标识信息由服务器使用来产生用户使用的打开密钥。在另一实施例中,服务器使用与媒体如 CD 盘 ID 号相关的标识信息产生打开密钥。这个盘 ID 可直接提供在媒体自身上或包装上,或以类似方式来提供,使得其对于购买了软件产品的用户而言是可视的。这个实施例的使用例是自由分配包含程序样品的 CD 或 DVD 盘(如,计算机游戏、音乐、电影等)。该盘运行验证或程序样品或应用软件,并且向用户提供选项,通过电话或网站进行订购来购买完整的可执行程序。当进行购买时,向用户提供软件密钥(通常是字符串),该密钥将打开加密存储在自由(free)盘上的软件程序的所有版本。媒体识别符,如 CD/DVD 序列号用于确保用户与服务器之间的交易。与媒体识别符相关的密钥的使用防止与基于回放机器识别符来提供密钥相关的问题,并且其中所有分配的媒体是相同的。当密钥与媒体相关时,媒体可被放

置在任何兼容机器上,但是该特定的密钥不能被用于访问其他锁住的盘拷贝。

[0059] 在另一实施例中,用于许可用户访问在媒体上包含的所有程序的安全机制是包括媒体标识符(如盘序列号)和回放机器识别符(如客户计算机序列号)以产生打开密钥的组合密钥。对于这个实施例,然后软件将被制定给盘和特定的回放机器。尽管由于密钥对于 CD 也是惟一的而使得出现盘不能在另一回放机器上播放的情况,但却给出了允许其的机制。

[0060] 当用户进行购买时,通过在线或离线方式(如电话),维持记录回放机器的序列号和盘的序列号的数据库记录。如果用户曾被迫替换其回放机器,他或她可通过将盘插入新的回放机器来请求新的打开密钥。然后数据库确认盘序列号表示出与其相对的购买,从而对用户产生新的打开密钥。在一个实施例中,实施访问计数,以便数据库仅仅允许这个过程被执行有限的次数。同样的过程可用于在不同的回放机器上播放盘,而并非更换。通过限制新的密钥可产生的次数,可消除大批量制造单一序列号的盘造成的侵权。尽管未批准的用户仍可能产生很多不同的序列号盘,但他们要购买软件来用于序列号的每个拷贝。一般地,只要新密钥的限制低(也就是说,仅仅允许 2 个更换密钥),这在成本上说将是低效的。另外,对于更换密钥要求另外的安全性。例如,如果请求更换密钥,必须回答安全问题,或者密钥必须被寄送到特定的物理地址或电子邮件,或者重复呼叫用户,这样允许识别的一些人来请求更换密钥。

[0061] 对于上述实施例,用户首先接收自由分配盘或包括包含软件产品的样品或受限版本的媒体的其它程序。在自由试验或验证的最后,显示命令页,其告知用户如何即时购买游戏。购买可通过访问显示的 URL 来连接自动的网页在线进行,或者通过呼叫显示的电话号码或向显示的地址发邮件或向传真号发传真来离线地进行。盘上的软件例行程序接着将产生安全密钥。如上所述,该密钥可从这个盘序列号或从都通过应用软件读出的盘序列号和回放机器的序列号来产生。在一个实施例中,密钥是字母和数字组合构成的字符串。产生的密钥可由服务器计算机使用来唯一地识别盘序列号和回放机器的序列号。

[0062] 当用户通过在线 URL 或离线电话号码访问服务器计算机时,要求他或她输入密钥和他们的信用卡记账信息。安全数据库记录这个信息,并且审核信用卡等。在这个步骤后,服务器产生打开密钥。产生打开密钥,该密钥为用户提供的密钥与特定的应用软件所使用的主密钥的组合。基于盘序列号服务器可获知该应用软件。打开密钥安全地存储在中央数据库,并且它也是字母和数字的字符串。一旦密钥被传递到用户并且用户确认了接收,则完成交易并且数据库记录交易和密钥。如果用户忘记了或者需要再次访问其密钥,则由于数据库知道这是合法购买的密钥,他们仅仅需要呼叫或再次在线进行,输入盘 ID 密钥,并且检索打开密钥,其中该盘 ID 密钥一经登录盘将总是存在。

[0063] 一旦用户接收到打开密钥,密钥通过输入装置,如键盘或一些形式的虚拟键盘被输入到回放机器。回放机器在静态存储区域,如存储卡或硬盘空间中存储打开密钥。一旦执行,购买的软件产品的主应用程序证实密钥对特定的盘和回放机器真实正确。假设密钥是许可的,主应用程序被打开。为了附加的安全性,主可执行文件可被加密,使得它不易被未授权的用户攻击。

[0064] 对于这个实施例,打开密钥在用户和服务器计算机之间的传送可使用参考图 2A 到图 5 所示的加密/解密机制来完成。例如,参考图 3A 所示的处理,媒体标识符被用于在

步骤 310 产生打开密钥结果的实施例包括了向产品 ID 添加盘或媒体序列号以及以用户公钥方式加密的用户存储卡 ID。在图 4 所示的流程图中可组合类似的添加。

[0065] 上面说明中,描述一种经计算机网络分配受限使用软件产品的系统。尽管本发明参考具体的特定实施例进行了说明,但显然在不背离权利要求中提出的本发明的更宽的精神和范围的情况下可对这些实施例作修改和改变。因此,认为说明书和附图是示意性的而不是限制性的。

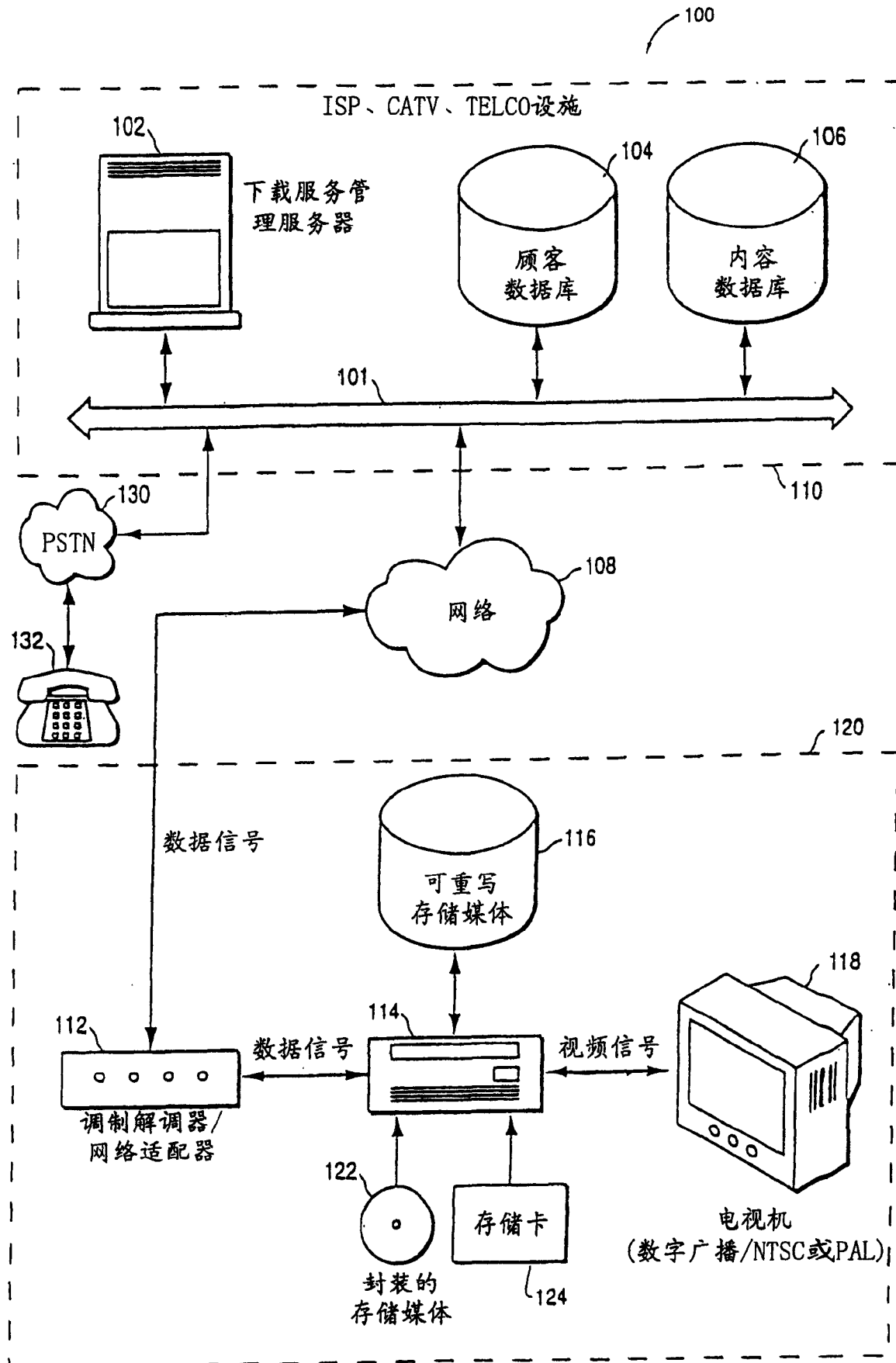


图 1

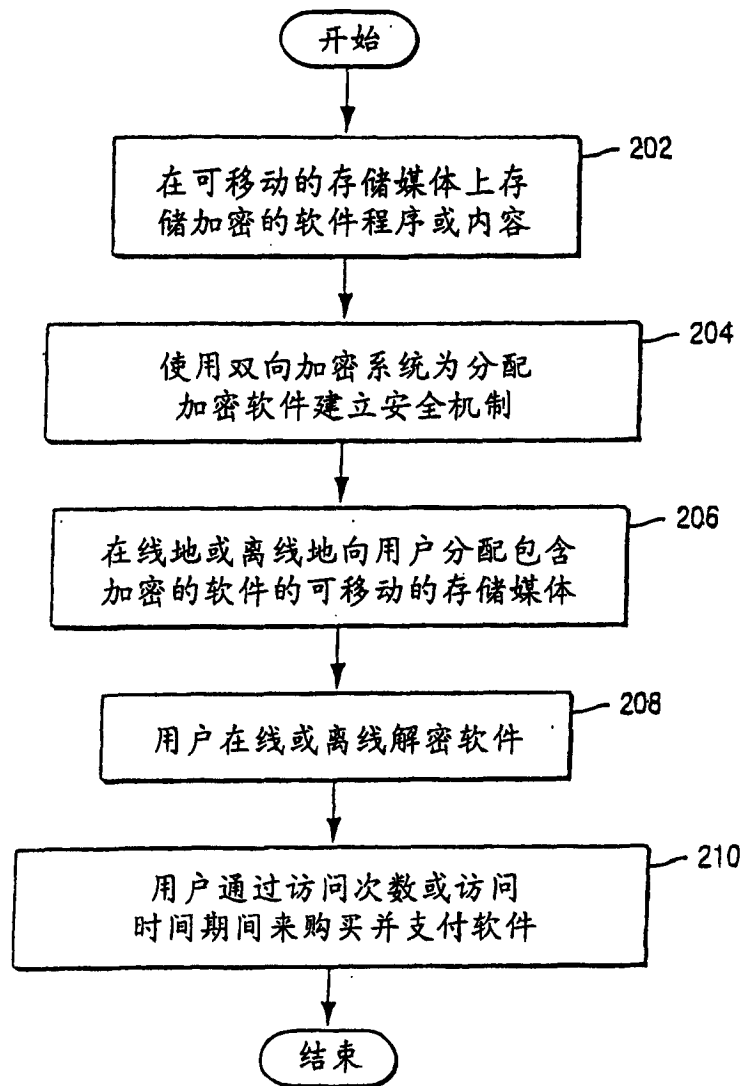


图 2A

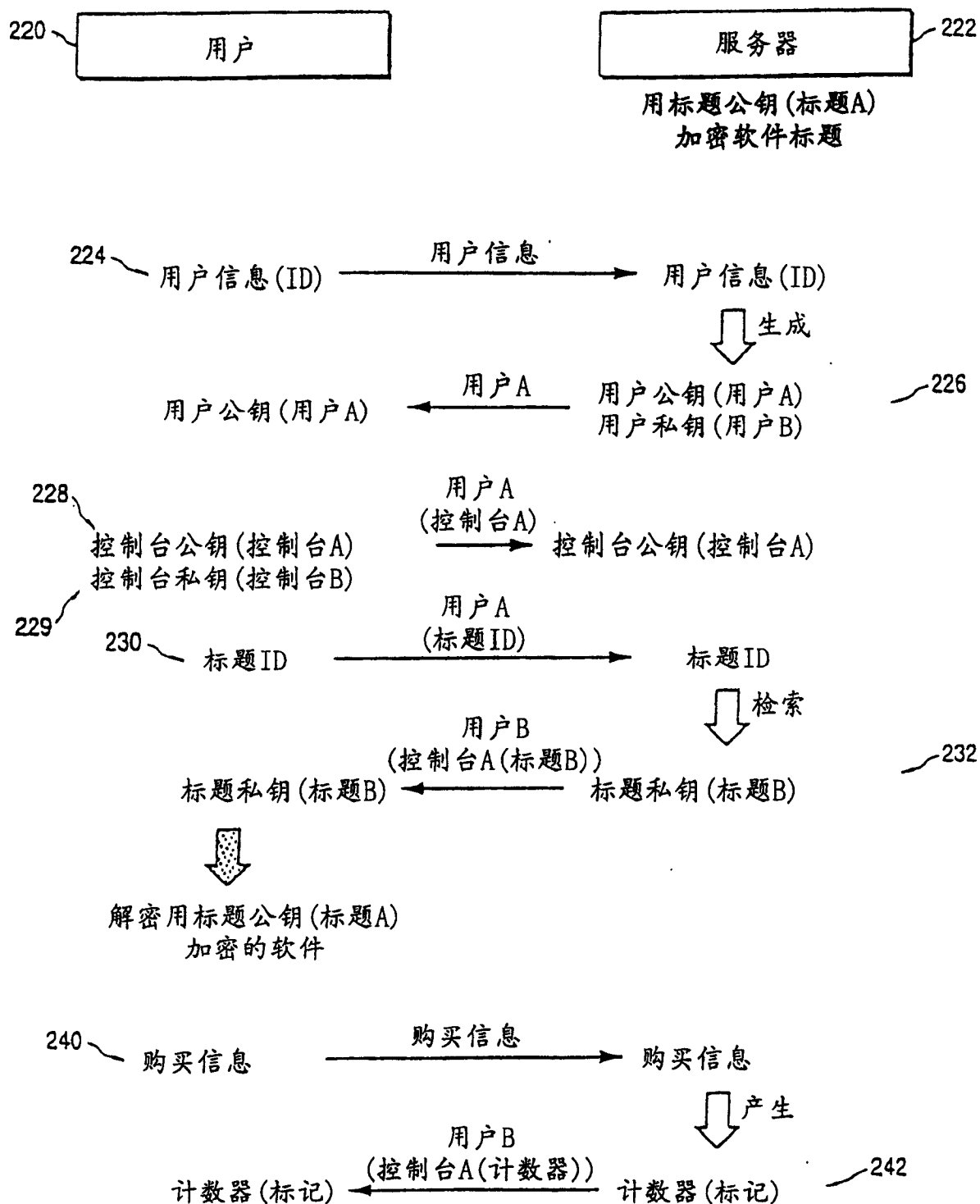


图 2B

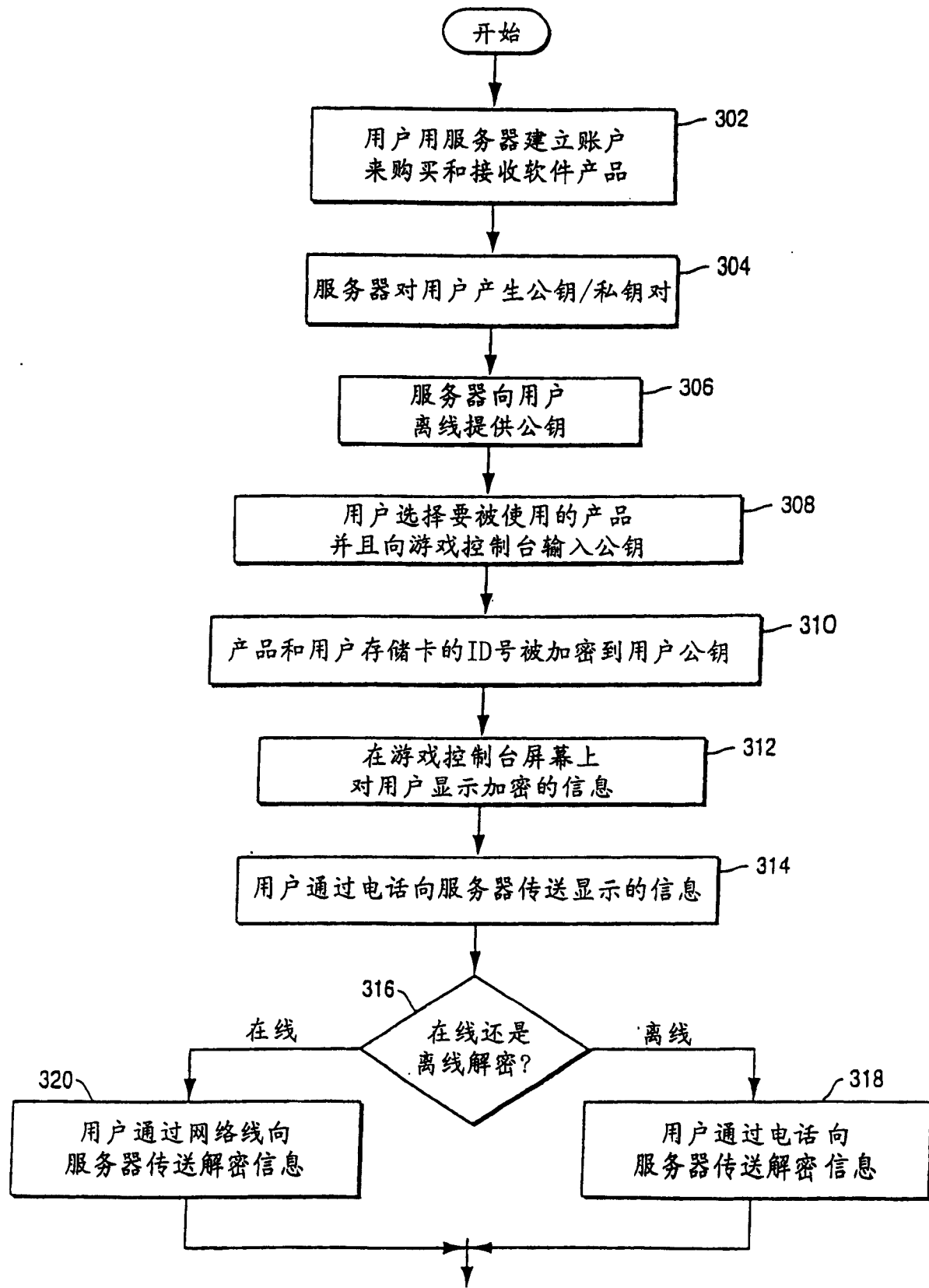


图 3A

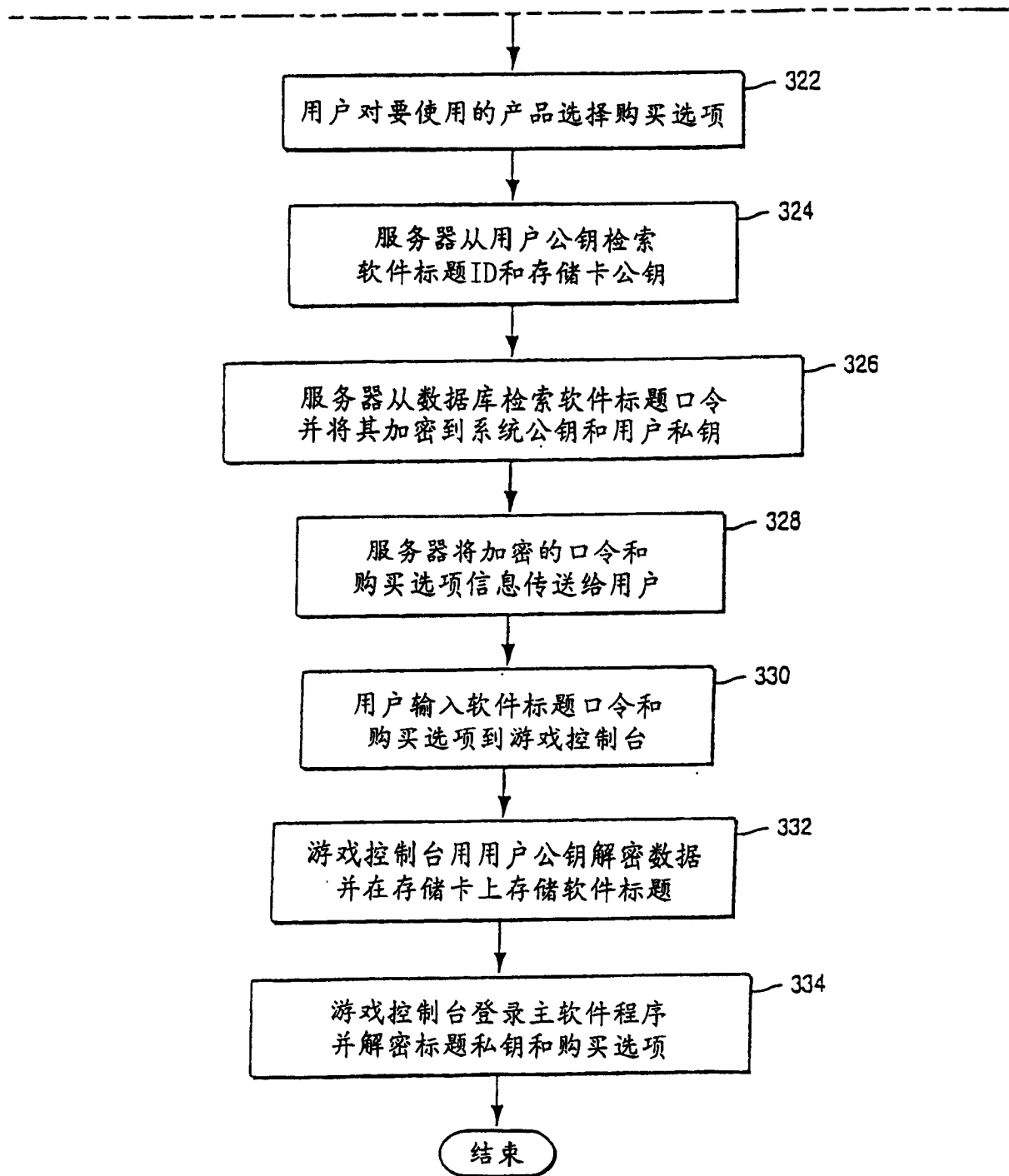


图 3B

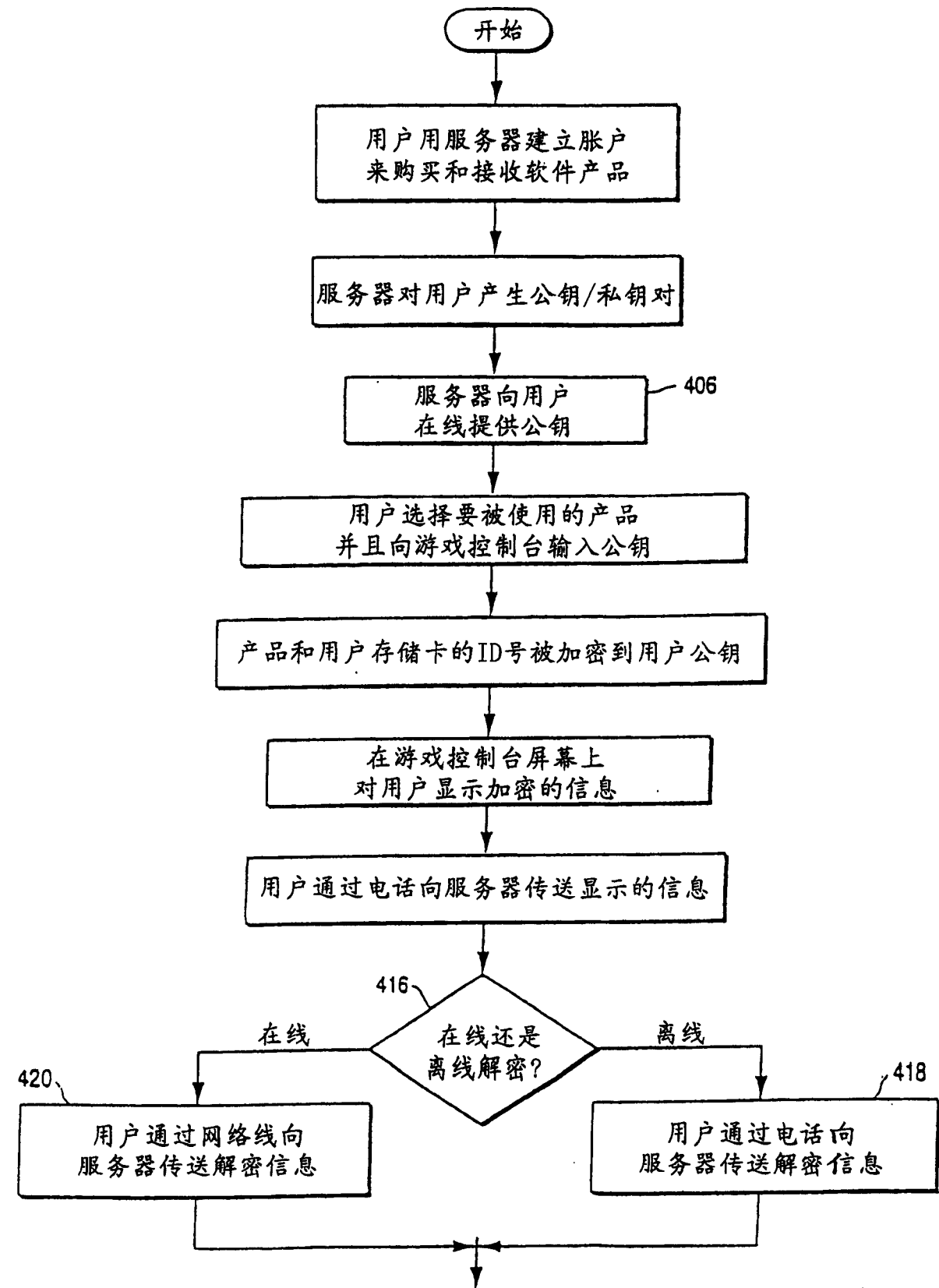


图 4A

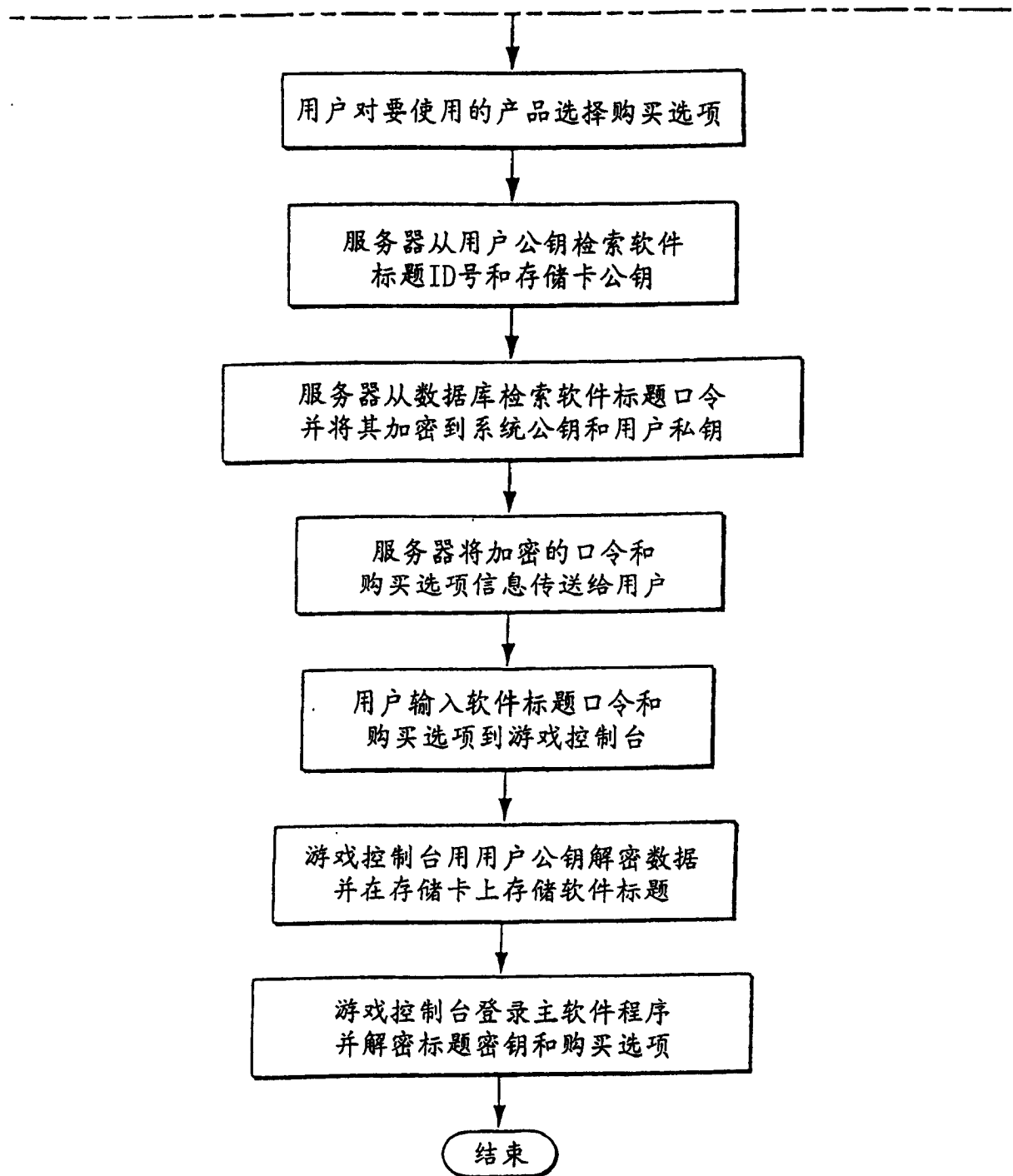


图 4B

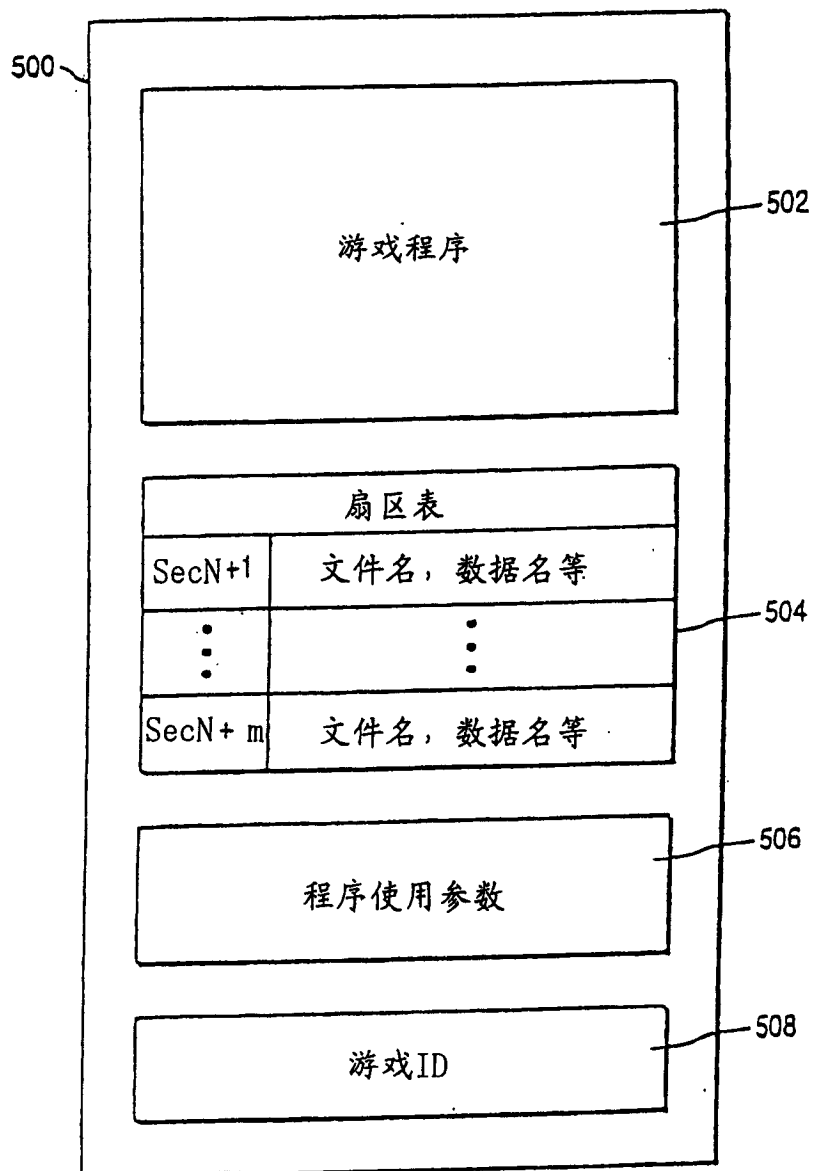


图 5