[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 03814013.6

[43] 公开日 2005 年 8 月 31 日

[11] 公开号 CN 1663174A

[22] 申请日 2003.5.27 [21] 申请号 03814013.6
[30] 优先权
[32] 2002. 6.17 [33] EP [31] 02077423.8
[86] 国际申请 PCT/IB2003/002340 2003.5.27
[87] 国际公布 WO2003/107589 英 2003.12.24
[85] 进入国家阶段日期 2004.12.16
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 P·J·勒努瓦 J·C·塔斯特拉
S·A·F·A·范登霍伊维尔
A·A·M·斯塔林格

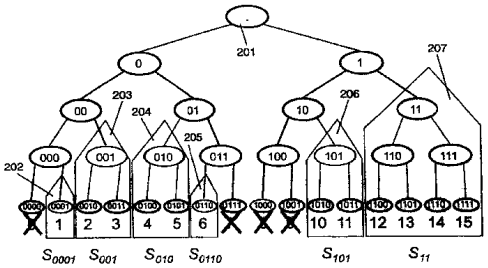
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 刘 杰

权利要求书 1 页 说明书 16 页 附图 5 页

[54] 发明名称 用于在设备之间进行验证的方法

[57] 摘要

证书授权中心提供一个方法，用于基于白名单控制在系统(100)中第一设备(102)向第二设备(103)的验证。该方法包括向第一设备(102)发出一个群体证书，它识别未撤销的设备标识符的范围，所述的范围包含第一设备(102)的设备标识符。优选地，设备标识符对应于分层排序树中的叶节点，并且群体证书识别树中表示子树的一个节点(202－207)，其中该叶节点对应于所述的范围。群体证书还可以识别子树中表示子子树的另一节点(308、310、312)，其中的各叶节点对应于已撤销的设备标识符。替换地，设备标识符从依次排序的范围中被选择，并且群体证书识别依次排序范围的子范围，所述的子范围包含白名单列出的设备标识符。



ISSN1008-4274

1. 一种用于控制第一设备对第二设备的验证的方法，这些设备被分配相应的设备标识符，该方法包括向第一设备分发一个识别未撤销的设备标识符的范围的群体证书，所述的范围包含第一设备的设备标识符。

2. 权利要求1的方法，其中，各相应的设备标识符对应于在分层排序树中的各叶节点，该方法还包括在群体证书中识别分层排序树中的一个节点，所述的节点表示一个子树，该子树的各个叶节点对应于未撤销的设备标识符的范围。

3. 权利要求2的方法，还包括在群体证书中识别子树中的另外的节点，所述的另外的节点表示另一个子树，其中的各个叶节点对应于排除在未撤销的设备标识符的范围之外的各设备标识符。

4. 权利要求1的方法，其中，相应的设备标识符是从依次排序的范围中选择的，该方法还包括在群体证书中识别依次排序范围中的子范围，所述的子范围包含未撤销的设备标识符的范围。

5. 权利要求1的方法，还包括在单个群体证书中识别未撤销的设备标识符的多个相应范围。

6. 权利要求5的方法，其中，单独一个群体证书中多个相应范围被顺序地排序，该方法还包括通过在顺序地排序中最低和最高的相应范围的标记来识别单个群体证书中多个相应范围。

7. 权利要求1的方法，其中，群体证书包括有效期的标记。

8. 权利要求1的方法，其中，群体证书包括版本标记。

用于在设备之间进行验证的方法

本发明涉及一种控制第一设备向第二设备的验证的方法，这些设备被分配相应的设备标识符。

发明背景

近年来，内容保护系统的数量已经有了快速的增长。其中一些系统仅仅保护内容以防被非法拷贝，而其它系统还禁止用户访问内容。第一个类别被称作拷贝保护(CP)系统并传统上已经是消费电子设备(CE)的主要焦点，这是因为这类内容保护被认为是可用廉价的方法来实施的并且不需要与内容供应商双向相互作用。这样的例子是CSS(内容加扰系统)，即DVD ROM(只读存储器)盘以及DTCP(数字传输内容保护)，即IEEE 1394连接的保护系统。该第二类别已知有若干名称。在广播领域中，它们通常被称为CA(有条件接收)系统，而在互联网领域中它们通常被称为DRM(数字权利管理)系统。

近来，新的内容保护系统已经被引入(像来自Thomson的智能版权或来自DTLA的DTCP)，其中，一组设备可以通过双向连接彼此验证。在这个验证的基础上，这些设备将彼此信任并且这将使它们能交换受保护的内容。在伴随着内容的许可证中，描述了用户具有哪些权利和他/她被允许对该内容执行什么操作。

设备之间互通信所必需的信任基于一些秘密，这种秘密仅仅为经过测试和被证明具有安全的执行过程的那些设备所知。对该秘密的认知是使用验证协议测试的。用于这些协议的最佳解决方案是那些使用'公开密钥'密码学的那些方案，它们使用两个不同的一对密钥。将被测试的秘密则是一对密钥中的保密密钥，而公开密钥可以被用来校验测试结果。为了确保公开密钥的正确性和检查密钥对是否是被验证设备的合法的密钥对，公开密钥伴随有一个证书，这个证书由证书授权中心经数字方式签名，这个组织管理所有设备的公开/保密密钥对的分发。在一个简易的执行过程中，证书授权中心的公开密钥被硬编码在设备的硬件中。

证书是一个比特串，它包括M个比特的消息部分和附加到其上面的C个比特的签名部分。C通常在512...2048比特的范围内并且一般来说

是1024比特。对于M<C，签名是基于消息本身计算的，而对于M>C则是基于消息摘要而计算的。下面把第一种情况：M<C，作为更相关的一种情况。签名敏感地随消息内容而定，并且具有只能由证书授权中心构造而能被大家校验的特性。在本文中的校验意指：检查该签名是与该消息一致的。如果某人已经改变消息的哪怕只是一个比特，则签名就不再是一致的。

在典型安全方案中，存在涉及到的几个不同的设备，它们可能不全部都是用相等的防篡改（tamper-proofing）级别来实现的。因此，这样的系统将能抵抗对各个独立设备的入侵，这些入侵可能是非法存储、拷贝和/或把数字内容再分发。增加抵抗力的一个重要技术是所谓的撤销这些被入侵的设备。

撤销意指将那个设备中的信任撤回。撤销的效果是网络中的其它设备不再想要与已撤销的设备进行通信。撤销可以用几种不同的方式来实现。两个不同的技术可以使用所谓的黑名单(已撤销的设备列表)或白名单(未撤销的设备列表)。

在黑名单方案中，要校验其通信伙伴的信任的那个设备需要有该列表的最新版本并且检查另一个设备的标识符是否在那个列表上。黑名单的优点是设备被默认是可信任的，并且只有当它们的ID被列在撤销列表上的时候才撤销对它们的信任。这个列表最初很小，但是它能潜在地无限制增长。因此，这些撤销列表在CE设备上的分发和存储两者最终可能都是成问题的。

在白名单方案中，设备必须向其它设备证明它仍然是在被允许的通信伙伴的列表上。这将通过给出最新版本的证书来完成，最新版本的证书声明该设备是在白名单上。通过只把证明该设备是在白名单上的一个定长证书存储在每个设备中，白名单技术克服了存储问题。撤销由向已撤销的之外的所有设备发送新版本的白名单证书来完成。尽管这时设备中的存储量是有限制的，然而如果没有可用的有效方案，则分发白名单证书是一个几乎不可克服的问题。

发明内容

本发明的一个目的是根据前文提供一个系统，它能有效分发和存储白名单证书。

这个目的根据本发明用一个方法来实现，包括向第一设备分发用

于识别未撤销的设备标识符的范围一个群体证书，所述的范围包含第一设备的设备标识符。

本发明提供一个技术，它结合了黑名单(最初的小的分发列表)的优点和白名单(有限的存储)的主要优点。优选地，这个技术另外还使用一个设备证书，它证明设备的ID。这个设备证书已经作为初始信任的基础而存在于设备之中(与撤销无关)并且例如在工厂生产期间就已安装。

现在，每个设备只须存储单独一个群体证书，即识别包含它自己的设备标识符的范围的那个群体证书。这是指证书的存储需求是固定的并且可以被提前计算。现在对这些设备的实现进行优化是可能的，例如通过安装一个容量正好合适的存储器而不是像在现有技术中那样必须安装一个“足够大”的存储器。

至于分发，现在不再需要总是向系统中的每一个设备发送单独的证书。通过选择一个适当的设备标识符的分群，单独一个群体证书足够该群体中所有设备之用。从而该方法更为有效。

第一设备现在可以通过向第二设备出示群体证书来验证它自己。当然，第一设备向第二设备的验证可能包括除了出示群体证书之外的其它步骤。例如，第一设备还可以与第二设备建立安全验证信道，向第二设备出示包括它的设备标识符的证书，等等。如果第二设备确定第一设备的设备标识符确实包含在群体证书给出的范围中，则验证是成功的。通过简单地也让第二设备向第一设备出示它自己的群体证书，验证是可以相互进行的。

在一个实施例中，相应的设备标识符对应于分层排序树中的各个叶节点，而群体证书识别分层排序树中的一个节点，所述的节点表示一个子树，该子树中各个叶节点对应于未撤销的设备标识符的范围。这具有这样的优点，即使用分层结构使很有效地识别一个群成为可能。一个很大的设备群可以用对应于分层结构中高级节点的单个标识符来识别。

在这个实施例的改进中，群体证书还识别子树中的另外的一个节点，所述的另外的节点表示另一个子树，其中的各叶节点对应于排除在未撤销的设备标识符范围之外的各设备标识符。在先前的方法中，如果子树中的一个设备被撤销，则需要发出很多新的证书用于仍然是

未撤销的子树。本改进具有下列优点，即当子树中的少量设备被撤销时，不需要立即为大量的新子树发出新的证书。

作为一种提高，可以发出用于识别又一个子树的群体证书，这个子树是另一个子树的一部分。这样，子树的这个部分可以被维持在未撤销的设备标识符的范围内。

一般都希望在事先就同意总是撤销群中的一个设备ID，例如设备ID零。这样，即使没有实际的设备被撤销，群体证书也总被始终如一地形成。

在还一个实施例中，相应的设备标识符是从依次排序的范围中选择的，并且群体证书识别依次排序的范围的子范围，所述的子范围包含未撤销的设备标识符的范围。这有利地结合了上述的简易黑名单方法的小的发送规模和白名单方法的小的存储规模。如果现在所有已撤销的设备的排序表(例如递增排列)被建立，则被授权的各个群包括这个列表任何两个单元之间的设备。这时，发送规模最多等于简易黑名单情况中的规模(当然，被发送的数据与黑名单一致但其解释不同)。

在又一个实施例中，一个群体证书识别未撤销的设备标识符的多个相应范围。这样，不用以很大的计算成本来校验很多数字签名，网关设备就可以容易地分辨一个特定的群体证书是否可能与各特定的设备有关。然后，它可以滤出那些根本不相关的群体证书，或者在那些相关的群体证书上校验任何数字签名。

在这个实施例的变形中，单独一个群体证书中的多个相应范围被依次排序，并且单独一个群体证书经由连续排序中的最低和最高相应范围的标记来识别多个相应范围。这允许过滤器来决定这个证书是否可能是相关的。然后，这可以由被指定设备自己检验签名来校验。它可以迅速排除大量不相干的证书。

在又一个实施例中，群体证书包括有效期的标记并且如果所述的有效期是可接受的，则第二设备验证第一设备。“可接受的”可以简单地指“当天和当时是在所指出的时期之内”，不过优选地也指对所指出时期的一些延伸应该是可接受的。这样，传送新的群体证书中的延迟不致于使自动使装置验证失败。

在还有一个实施例中，群体证书包括版本标记。这使得以下情况成为可能，即第二设备向第一设备分发含有可接受证书最低版本的标

记的受保护内容，和如果群体证书中的版本标记至少等于可接受的证书最低版本的标记，则成功地验证第一设备。

尽管设备可以从它们的通信伙伴要求至少与它们所使用的版本一样新的版本，然而由于处在已撤销的列表中的设备被完全锁定在任何内容交换之外，仍然可能产生问题。它们甚至被锁定在旧的内容之外，这些旧的内容在新的撤销列表被分发之前还是允许他们操作的。在这个实施例中避免了这些问题。即使第一设备以后被撤销，它仍能用它的旧的群体证书来访问旧的内容。

“版本”可以被数字地识别，例如“版本3.1”，或者被联系到某个时间点，例如“2002年1月的版本”。后者具有下列优点，即便于向人们解释由于特殊版本太旧而不再是可接受的，这通过比较当前时间和时间点可以很容易地被看出。使用纯数字的版本号这将困难得多。

附图简要说明

本发明在下面用举例的方法并且参考附图而更加详细地被描述，其中：

图1大略地示出包括经由网络互连的设备101-105的系统100;

图2是一个框图，说明用于被完善的子树方法的二叉树的结构;

图3是一个框图，说明用于子集差异法的二叉树的结构;

图4是一个框图，说明被修改的黑名单方法；和

图5是一个表，说明用于产生证书的优化方案。

具体实施方式

在全部的附图中，相同的参考数字指出类似或对应的部件。在附图中指出的一部分部件一般以软件实现，而这些表现为软件实体，比如软件模块或对象。

系统总体结构

图1大略地示出包括经由网络110互连的设备101-105的系统100。在这个实施例中，系统100是一个家庭网络。标准的数字家庭网络包括很多设备，例如无线电接收机、调谐器/解码器、CD播放器、一对扬声器、电视机、录像机、磁带机等等。这些设备通常被互连以允许一个设备，例如电视机，来控制另一设备，例如录像机。诸如调谐器/解码器或机顶盒(STB)之类的一个设备通常是提供对其它设备的中央控制的中央设备。

一般包括像音乐、歌曲、电影、电视节目、图片等等之类东西的内容经由住宅网关或机顶盒101被接收。来源可以是对宽带电缆网络、互联网连接、卫星下行链路等等的一个连接。内容能因此在网络110上被传送到一个用于呈现的接收器（Sink）。转接器可能是例如，电视显示器102、便携式显示设备103、移动电话104和/或音频播放设备105。

内容项被呈现的确切方或取决于设备的类型和内容的类型。例如，在无线电接收机中，显示包括产生音频信号并且把它们供给到喇叭。对于电视接收机，呈现通常包括产生音频和视频信号并且把它们供给到显示屏和喇叭。对于其它类型的内容，必须采取类似的适当行动。呈现也可能包括比如将接收的信号解密或去扰，使音频和视频信号同步等等操作。

机顶盒 101，或系统 100 中的任何其它设备可能包括存储介质 S1，比如适当的大硬盘以允许被接收内容的记录和以后的播放。存储器 S1 可能是一些种类的个人数字记录器(PDR)，例如与机顶盒 101 连接的 DVD+RW 记录器。存储在上诸如小型盘(CD)或数字通用盘(DVD)之类的载体上的内容也可以被提供给系统 100。

便携式显示设备 103 和移动电话 104 被无线连接到使用基站 111 的网络 110，例如使用蓝牙或 IEEE 802.lib。其它一些设备使用常规有线连接来连接。为了让设备 101-105 交互作用，可以用几个交互性标准，它们让不同的设备交换消息和信息以及相互控制。一个熟知的标准是 2000 年 1 月公开的家用音频/视频交互(HAVi)标准版本 1.0，并且可在互联网地址 http://www.havi.org/上得到。其它的熟知标准是家用数字总线(D2B)标准，这是在 IEC1030 中描述的通信协议以及通用即插即用(http://www.upnp.org)。

确保本地网络中的设备 101-105 没有拷贝未被授权的内容往往是很重要的。为了做到这点，一个一般称为数字版权管理(DRM)系统的安全构架是必需的。

在一个这样的构架中，本地网络被概念地划分成有条件接收(CA)领域和拷贝保护(CP)领域。转接器一般位于 CP 领域。这确保当内容提供给转接器时，由于拷贝保护方案位于 CP 领域，所以未被授权内容的拷贝不能进行。CP 领域中的设备可能包括做临时拷贝的存储媒介，不过这类拷贝不能从 CP 领域输出。这个构架在与本申请相同的申请人的

欧洲专利申请01204668.6(代理人记事表PHNL010880)中被描述。

无论选择哪种具体的方法，实现安全构架的家庭网络中的所有设备都根据实现需求来这样做。使用这个构架，这些设备可以彼此验证以及安全地分发内容。对内容的访问由安全系统管理。这防止了无保护的内容被泄漏给未被授权的设备和来源于不可靠设备的数据进入系统。

设备只把内容分发到已经预先被成功地验证的其它设备是很重要的。这确保对手不能使用恶意的设备来做出未被授权的拷贝。只有当一个设备由被授权厂商制造时它才能够被成功地验证，举例来说，因为只有被授权厂商知道成功验证所需的特殊秘密或者它们的设备具有由被信任的第三方所发出的证书。

设备撤销

通常，如果设备内部的保密信息(例如标识符或译码密钥)已经被破坏或者经由入侵被发现，则设备的撤销是它的一个或多个功能被缩减或完全取消。例如，CE设备的撤销可能限制该设备能够解密和使用的数字内容的类型。替换地，撤销可以使得一个CE设备不能再执行某些功能，比如对它接收的任何数字内容做出拷贝。

撤销的常见效果是网络110中的其它设备不再想要与已撤销的设备进行通信。撤销可以用几种不同的方法来实现。两个不同的技术将使用所谓的黑名单(已撤销的设备列表)或白名单(未撤销的设备列表)。

可能存在多个版本的撤销列表。几个机理可以被用于新版本的实施。例如，设备可以向它们的通信伙伴要求至少与它们自己所使用的版本一样新的版本。然而，因为已撤销的列表中的设备被完全锁定在任何内容交换之外，所以这可能产生问题。它们甚至被锁定在旧的内容之外，这些旧的内容在新的撤销列表被分发之前还是允许他们操作的。

另一个版本控制机理是把被分发内容连接到撤销列表的某个版本，即撤销列表的当前版本号是伴随着内容的许可的一部分。于是只有当它们所有的通信伙伴都有至少与内容所需版本一样新的版本时，设备才将分发内容。版本编号可以通过例如使用单调地增加号数而被实现。

存在确定撤销机理的吸引力(因此应用可能性)的多个成本因素。一

个因素是发送规模：每个未撤销的设备必须接收一个用于证明它仍然带有撤销系统的当前版本这个事实的签名消息。另一个因素是存储规模：每个未撤销的设备必须存储证明它仍然带有撤销系统的当前版本的证书。这两个因素看上去好像是对立的。对于小的发送规模，授权机构最好是广播一个包括所有已撤销的设备身份的签名消息，不过对于大约100,000个已撤销的设备的情况下这会导致无法实现的存储器需求。为了使存储规模最小化，证书授权中心将最好是发送一个独立证书到每个未撤销的设备，包括那个设备的设备ID(例如序列号、以太网地址等等)；然而这使得也许要广播上亿条消息。当然在双向链路的情况下(例如有电话联结器的机顶盒)，人们可以仅仅下载与AD中的各设备有关的证书。

本发明的其中一个目的是在如上所述的黑名单方法和白名单方法给出的两个极端之间提供一个有意义的折衷。本发明部分地基于在密码学中已知的分级密钥分发方案。在本发明的一个实施例中，证书授权中心发送签名消息，签名消息确认某群设备没有被撤销：每个未撤销的群有一个签名消息。一般来说群数比设备数小得多，因此这需要有限的发送规模。进一步，设备只存储关系到它作为成员而所在群的消息，并且从而只需要有限的存储规模。然后在两个设备之间的验证期间，“证明者”出示两个证书：最新的撤销消息，它表明证明者作为成员而所在群没有被撤销，和一个证书(在工厂中安装的)，它确认它的设备ID(即这个设备是在涉及到最新撤销消息的步骤中提到的群的成员)。

一般来说，这类证书包括设备标识符i和公开密钥PK_i。根据在前面提及的验证协议，已经拦截到i作为成员所在群的证书并且试图假冒i的攻击者不会有对应于PKi的私人密钥SK_i，并且所有进一步的通信都被中断。

为了描述这些优点，引入以下注释：

· 每个设备都具有一个设备标识符i，$0<i<N$，其中$N=2^n$是设备总数：每个设备标识符数是一个n个比特的串；

· $D = \{0,1,...,N-1\}$是所有设备的集；

· $R=\{f_1,f_2,...,f_r\}$是已撤销的设备集(它一代接一代地改变/增长)。

证书授权中心发送一个(各不相同的)消息到 m 个群$S_1,...,S_m$的每个

设备，证明该群的各成员没有被撤销。群 i 的每个成员存储群 i 的消息/证书。这些群是这样选择地，使$S_1 \cup S_2 \cup ... \cup S_m$= D|R (即所有群 S_k 一起形成未撤销的设备群，1≤k≤m,它等于 D 减去已撤销的设备的群)。

要解决的问题是在给定 R 时怎样选择把 D|R 的划分成为 $S_1,...,S_m$。注意，当 R 已经改变时这个划分在下一代中将是不同的。假设 N 一般是一个 40 个比特的数(实际上在整个世界中允许给每个人提供大约 200 个设备)，和 r = |R|，已撤销的设备数小于 100000。在下面要论述五个这类划分以及在发送和存储规模中它们相应的成本。这些划分方案是简易黑名单；简易白名单；完整的子树方法；子集差异法；和被改进的黑名单方法。在论述划分法和它们的成本之后，签名的影响将被考虑。

简易黑名单

如上所述，为了最小化发送规模，能做的最佳方法是发送一个签名消息到声明是R的一分子的所有设备。实际上D\R被划分到单个群中，m=1。发送规模的理论下限是:

$$\log_2\binom{N}{r} \approx r\log_2 N - r\log_2 r = rn - r\log_2 r \quad \text{个比特}$$

当1<<r<<N时此近似成立，它是内容保护系统相关的参数的范围。很接近这个下限的一个普通的实施过程对于授权中心来说是用 $r \cdot n$ 比特来发送所有的已撤销的设备签名列表(每个设备都有n个比特的设备标识符)。存储规模显然同样是 $r \cdot n$ 个比特(~1/2 Mbyte)。

简易白名单

为了使存储规模最小化，授权中心发送单独的证书到每个未撤销的设备，证书包括它的设备标识符。实际上D/R被划分成m=|D/R|=(N-r)-群，每群只有一个成员。发送规模是 $(N-r)\cdot n$(或者可能是 $(N'-r)\cdot n$，其中N' = # －迄今为止已发出的设备)。

完整的子树方法

一个方法，用于把一群标识符划分成分层排序的群，它在D. Naor, M. Naor, J. Lotspiech的 “Revocation and Tracing Schemes for Stateless Receivers”，Adv. In Cryptology, CRYPTO'01，LNCS 2139，Springer 2001，pp.41-62中被描述，但是该文不讨论使用排序的集来创建像本发明中的群标识符。

为了讨论完整的子树方法，和在下面进一步阐述的子集差分法，

所有可能的n个比特的设备标识符都作为(n+1)层的二叉树的叶(终点)被解释。一部分术语:

· 树的端点被称作叶。在一个(n+1)层的树中存在2^n个叶。

· 一个节点是树的各个分支结合的位置。叶也被认为是节点。

· 根是最顶端的节点。

· 当节点υ直接位于节点u上时，υ被称为u的父，而u是υ的子。υ的其它子u'被称作u的兄弟。υ和它的父和祖父一起被称作u的上代，反之u是它们的子代。

· 以υ为根的子树是包括了υ和它的所有子代的集。

沿着树向上移动就像是砍掉设备标识符的二进制表示的LSB(最低位)，每层一位。假设许多的 $R=\{f_1,f_2,...,f_r\}$数目的叶已经被撤销。现在从已撤销的叶的每一个中向上画出一条通路一直到树根。各通路把合并的集合被称作斯坦纳树 ST(R)，它对应于叶 R。这在图 2 中被说明，其中，给出了用于 N=16 个设备的一个二叉树的结构。设备标识符为 0、7、8 和 9 的设备已经被撤销。经由已撤销的各节点并最后连接到最顶层节点 201 的树的通路形成了对应的斯坦纳树 ST(R)。这些通路处于闭合区域 202-207 之外。在每个闭合区域的顶端是与斯坦纳树断开的兄弟节点，这些节点产生由闭合区域表示的群 S_i，它们被标记为 S0001、S001、S010、S0110、S101 和 S11。

对于完整的子树法集中在断开的节点 ST(R)上，即 ST(R)上的节点的兄弟，被称作$\{\upsilon_1...\upsilon_m\}$。证书授权中心现在选择划分$S_1,...,S_m$，其中，$S_i$对应于以 υ_i为根的子树的叶。每个证书只包括一个 υ_i。根据构造，R 的元件都不可能是 S_i 的元件并且 D/R 的每个元件必须被包括在$S_1 \cup S_2 \cup ... \cup S_m$中。这些群是不相重叠的。

可以认为，大约有m=r-n个从ST(R)断开：每个撤销设备(它到根的通路中有n个节点)有n个节点和r个设备。然而可以表明：$m \le (r \cdot \log_2 r)$。原因是ST(R)中的通路在它们到达根很久之前就趋向于合并。利用这一点以及每个υ_i都是一个n比特数这一事实，撤销消息的发送规模由$n \cdot r \cdot (n - \log_2 r)$[数十个Mbytes]的上限来界定。关于存储规模：一个设备只存储它所属于的S_i的签名：n个比特。

如果还必须撤销一个设备，例如图2中设备标识符为3的设备，则一个新的群(并且对应群体证书)S_{0010}被创建来替换S_{001}。这个替换可以

通过例如向S_{0010}增加一个较高的版本号来实现。如果群体证书带有有效期指示符，则证书S_{0010}在它的有效期已经过去之后自动期满，这样替换就是自动进行的。

如果设备标识符为14的设备被撤销，则必需两个新的群体证书。对应于群S_{110}的第一个群体证书识别不包含设备标识符14的群S_{11}的子树。第二个群体证书对应于S_{1111}的子树。

子集差分法

在图3中说明的这个方法用于N=16个设备，把设备的设备标识符解释为二叉树中的叶，与上面讨论的完整的子树法相似。再一次画出斯坦纳树ST(R)。现在，出度（outdegree）的链1在ST(R)上被识别：即在斯坦纳树ST(R)上只有一个子或兄弟的连续节点：见图3中的虚线。对于每个这样的链指定一个群$S_{a,b}$，对它发送一个证书如下：让a是该链的第一单元(正好在出度2的节点之后)，而b是最后一个(出度2的一个叶或节点)。然后，$S_{a,b}$是以a为根的子树的各个叶的集，减去以b为根的子树的叶。

设备标识符为0、7、8和9的设备已经被撤销。对应的斯坦纳树由标记为0000、000、00、0、01、011、0111、1000、1001、100、10、1的各节点和顶节点301形成。a是在每个闭合区域的顶端的节点302、304和306，而b是节点308、310和312。$S_{a,b}$是最外面的闭合区域减去由断开b节点308-312的子树所占据的区域。

问题在于这类链(在从树的底端朝着顶端走的两个通路的合并之间)可能永远没有被撤销的后代(否则斯坦纳树上的这个链中将存在一个节点出度2)。注意，由于使用了二叉树这一事实，这些群是不相重叠的。当然，其它类型的树或分级排序可以被使用，其中将出现重叠。这个对本发明没有影响。

可以表明这个构造是很有效的：为了覆盖DIR最多只需要2r-1个群$S_{a,b}$。实际上，最坏的情况模糊了这个事实，即对于随机选择的$R=\{f_1,f_2,...,f_r\}$，更实际的群数是$1.25\cdot r$。为了确定发送规模，需要计算怎样有效地编码$S_{a,b}$中的{a,b}对。注意，如果a在层j而b在层k，则b具有和a一样的最初j个比特。

用于编码{a,b}的实际方法是发送比特串$j\|k\|b$，其中，“‖”表示并置。因为j和k占用$\log_2 n$个比特(对于实际的N，r来说近似于6个比

特)，所以j|| k|| b的长度由上限$(n+2\cdot\log_2 n)$界定。从而，总的发送规模被界定在$(2r-1)\cdot(n+2\cdot\log_2 n)$并且更典型地是$1.25r\cdot(n+2\cdot\log_2 n)$[用典型值时约1Mbytes]。

如果还需要撤销一个设备，例如图3中设备标识符为3的设备，则新的群(并且对应群体证书)$S_{001,0011}$和$S_{000.0000}$被建立来替换$S_{00,0000}$。

修改的黑名单方法

这个方法直接结合了上述的简易黑名单方法的小的发送规模和白名单方法的小的存储规模。基本上，D/R被划分到m=|D/R|=(r+1)个群中，其中，每个群S_i包括设备$\{f_i+1...f_{i+1}-1\}$。在一个不成熟的方案中，这导致了$2\cdot r\cdot n$×的发送规模。一个更有效的方案如下：如果现在所有已撤销的设备的排序表(例如按递增排序)被建立，则被授权的群包括这个列表中任何两个单元之间的设备。现在，发送规模最多为r · n，这只等于简易黑名单情况中的规模(当然，被发送的数据与黑名单一致但解释则不同)。

对于存储，设备只提取包括两个已撤销设备的设备标识符的证书，它包括它自己的设备标识符。例如在图4中，设备4将只存储覆盖群$S_{0,7}$的证书：大约有2n个比特的信息。

排序的表的上下限的标记当然可以用各种各样的方法来选择。在上述示例中，号码0和7表示两个已撤销的设备，并且未撤销的列表包括号码1到6。人们可以提及群$S_{1,6}$就像提及群$S_{0,7}$一样。这纯粹是因为惯例和为了便于标记。

有效的证书分发

上述部分略述了怎样用有效的方法(考虑发送和存储规模)通过把设备划分成群和分发群体证书来向设备提供撤销/授权信息。下面将讨论一些示例，关于怎样把群标识符(群ID)，比如$S_{a,b}$中的a,b，变成证书：即怎样把证书授权中心的签名应用到这类群标识符。如上所述，签名以C比特扩展一个消息，一般为1024比特，和消息本身的大小无关。因此简单地说，如果证书被发送到m个群，其中每个群的标识符是l个比特，则总的发送规模不是$m\cdot l$个比特而是$m\cdot(l+C)$个比特。因为对于上述方法来说l一般只是在40...100个比特的量级，即l<<C，所以签名构成了发送/存储规模的主要部分。然而，因为C与签名所保护的消息的大小无关，所以发明者建议用下列优化来明显地减少签名造成的开销。

在第一个优化方案中，证书用包括多个群的群标识符的消息部分来构造，所有这些群的标识符上的签名被添加到消息部分上。证书照原样验证各个群中的一个群。注意：因为实际的原因，在各个群中的一个群的群标识符的总的长度优选地不超过C。

在一个进一步优化的方案中，证书的信息部分被压缩。长度m<C的消息的签名可能具有消息可以就从签名本身被检索的特性！人们可能简单地认为不再需要把群标识符本身包括在证书的消息部分中。然而，过滤证书，即例如由网关设备决定哪个证书必须去到哪个设备，就变得很困难/昂贵，这是因为签名处理是很昂贵的并且必须对每个证书都执行。

为了帮助这类过滤设备而给出以下建议：如果有可能确定在群标识符中的次序，比如在简易白名单、完整的子树方法或修改过的黑名单的情况下，则证书的信息部分只须包括存在于各个群内一个群中的“最低”和“最高”群标识符(其中“最低”和“最高”相对于排序关系被确定)。这让过滤器决定这个证书是否可能包括相关的群标识符。然后，这可以由被指定设备本身来检验签名而验证。它迅速排除了大量不相干的证书。

以上所述在图5的表中被说明。参考数字402指出一个方案，其中k个群$S_1,\ldots,S_k$一个群集的每个相应的群具有一个相应的签名$Sign[S_1],\ldots,Sign[S_k]$。如上所述，每个群$S_i$由长度一般约为40比特的串被识别。签名$Sign[S_i]$的长度一般是如上所述的1024比特。

参考数字404表明上述的第一优化方案。在此为k的签名数量现在被替代成验证整个群$S_1,\ldots,S_k$的单个签名。如果存在超过k个的签名，则需要创建更多的证书(每个证书用于k个证书的每个群)。然而，显然这仍然实质性地节省了需要被分发的证书数量：每k个原始证书有一个。

参考数字406涉及上述的进一步的优化，它包括把消息$S_1S_2\ldots S_k$减少到S_1S_k。这个进一步的优化把第一方案的因子2减少到大约为$(1024+80)/1024\cong 1.08$的因子。简言之，来自签名的开销几乎完全被消除。这些优化影响了早些论述过的不同的划分方案如下。

<u>简易黑名单</u>

在证书被附加了$r\cdot n$个比特的很长黑名单的情况下，它得到总共$r\cdot n+C$个比特的发送规模。对于存储这同样成立。签名规模是可以忽略

的。相对于签名的应用优化不起作用，因为只存在一个群。

简易白名单

总共有(N-r)个群，每个大小大致为n个比特。附加一个签名产生(N-r)·(C+n)的发送规模。用第一优化方案，对于每$\lfloor C/n \rfloor$个未撤销的设备只需要单个签名被计算/发送(因为$\lfloor C/n \rfloor$个序列号要用$\lfloor C/n \rfloor \cdot n \approx C$个比特)。为了作进一步的优化，(未撤销的)设备被排序，例如用设备标识符，并且只有$\lfloor C/n \rfloor$序列号那个群中的第一和最后被放入消息部分本身。这形成了$(N-r)/\lfloor C/n \rfloor \cdot (2n+C) \approx N \cdot (n+2n^2/C) \approx N \cdot n$的发送规模。(在这里N是被发出设备的总数)。对于存储，显然只需要一个证书被检索和存储：C个比特。

完整的子树方法

存在1.25r个群，每个群由一个$(n+2\cdot\log_2 n)$个比特的数(树节点)来描述。按照第一优化，其中的$\lfloor C/(n+2\cdot\log_2 n) \rfloor$可以被装入C个比特中，并且为它们一起提供单个签名。进一步优化也可以通过对树节点进行排序来实行，并且然后在消息本身中只留下两个树节点(最低和最高)。总的发送规模是

$(r\cdot(n-\log_2 r)/\lfloor C/n \rfloor)\cdot(2n+C) \approx r\cdot(n-\log_2 r)\cdot(n+2n(n+1)/C) \approx nr\cdot(n-\log_2 r)$。对于存储来说，只需要存储单个证书：C个比特。

子集差异法

(统计地)存在1.25r个群，每个由$(n+2\cdot\log_2 n)$个比特(两个树节点)来描述。按照第一优化，其中的$\lfloor C/(n+2\cdot\log_2 n) \rfloor$可以被容纳在C个比特中并且单个签名可以被一起提供给它们全部。进一步的优化也可以借助于对树节点作排序而执行，在消息本身中只留下两个树节点。于是总的发送规模是$(1.25r/\lfloor C/(n+2\cdot\log_2 n) \rfloor)\cdot(2n+C) \approx 1.25r\cdot(n+2\cdot\log_2 n)$。对于存储来说，只需要单个证书的签名部分要存储，消息本身不是必需的：C个比特。

改进的黑名单方法

存在(r+1)个群，由每个为n个比特的r个数来描述。按照第一优化，$\lfloor C/n \rfloor$个数可以被容纳进C个比特并且可以向它们全部一起提供单个签名。进一步优化也可以如下被执行：例如一个签名保护由$\{f_1,f_2,\ldots,f_k\}$描述的各个群内的一个群，即各个群$S\{f_1,f_2\}$ $S\{f_2,f_3\}$ $\ldots S\{f_{k-2},f_{k-1}\}$ $S\{f_{k-1},f_k\}$。这类各个群内的一个群可以只要通过把f_1和f_k放入消息部分而被

描述。然后，发送规模变成$((r+1)/\lfloor C/n \rfloor)\cdot(C+2n)\approx r\cdot n$。对于存储来说，只需要单个签名的签名部分被存储，消息本身不是必需的：C个比特。

注意，对于已撤销的设备是随机分配的情况，改进的黑名单方法目前比其它方法更为出众。实际上，它几乎达到了黑名单所需的发送规模的下限和白名单所需的存储规模的下限。如果设备按照分层来组织，例如一般来说如果某个型号的所有设备都需要被撤销，则其它方法可能变得是合适的。

因此，通过不发送大多数证书的消息部分而在接收时根据签名部分重建它，本发明提供了几个方法来减少签名的开销。从加密的观点来看，这可能引入一个危险因素，因为它把签名有效地组合，而且消息几乎没有冗余，而没有太多冗余的签名被认为是不安全的：它们太易于在不用证书授权中心的秘密密钥的情况下被创建。黑客只需产生一个随机的C比特号并且将它作为证书出示。如果几乎所有的消息都被认为是有效的，则所有的签名也将被认为是有效的！下面将要讨论的是，为什么仍然有足够多的冗余留在各个群内各个群的描述中，因此黑客构造无效签名实际上是不可能的。

除了证书授权中心的公开密钥之外，证书的签名检验还需要先了解它的内部格式。一个通常所使用的技术是对整个消息计算一个散列值，并将它包含在签名保护的数据中(即使用证书授权中心的秘密密钥加密)。这个技术具有如下缺点，即除了消息非常短的情况下，它把消息的大小至少按散列值的大小扩展了。注意，签名所覆盖的这个数据可能包括原始消息的一部分，在别的情况下那一部分是不发送的，这种情况被称为具有消息恢复的数字签名。替换地，整个消息可能与签名分开地发送，这种情况被称为有附录的数字签名。

对于在此描述的几个方法，可以使用一种替换技术，对于证书规模来说它是更加有效的。如上所述，两个证书正在被使用来保证设备的授权。第一个是所谓的设备证书，其包括设备的ID和它的公开密钥。它在制造中就被嵌入设备内部。第二个是所谓的授权证书，它包括被授权的一些设备标识符的列表。只有能够出示其标识符列在对应的授权证书上的设备证书的那些设备才能通过系统验证。这两个证书之间的关系是要用于签名检验进程的要素之一。另一个要素是对授权证书中被授权设备标识符的编码格式的知识。注意，只有验证才考虑授权

证书的签名。设备证书的签名验证可以根据标准技术执行，例如使用散列函数的那些技术。

在下面，假设被授权的设备标识符的列表被划分成群的一个集，它们的特征在于n个比特数。此外，假设签名即授权证书的大小是C个比特。可以被表示的群的总数是$N=2^n$。最后，为了(稍微)减少编码复杂度，假设设备0和N-1从一开始就被撤销。

每个证书组合$k=\lfloor (C-m)/n \rfloor$个群标识符，m表示对证书序列号的比特数和其它的相关信息进行编码的比特数。有效证书的边界条件是所有的群标识符都是唯一的，并且按升序排序的，例如$ID_0<ID_1<...<ID_{k-1}$。现在，如果包含的证书比k个群标识符少，则空余部分将填充上符合这个边界条件的随机数据。由m表示的被保留的比特部分然后被用来表明有效项的数量。产生随机签名对应于对k个群标识符的随机序列进行签名。满足边界条件的概率P(即它们被排序)等于：

$$P=[N.(N-1)...(N-k+1)]/N^k k! \approx \{1-[(k-1)k]/2N\}/k! \approx 1/k!$$

对于C和n的实际值，例如，n=40和C=1024，这个概率$P_{list} \cong 1/2^{83}$。这个数的含义是一个攻击者将不得不在2^{82}和2^{81+m}的公开密钥之间执行运算以求产生有效的授权证书。这个数对于攻击者要成功地产生假证书来说是大到无法完成的。

应当注意，上述实施例说明但不限制本发明，而且本领域普通技术人员将能够在不背离所附权利要求的范围前提下设计许多替换实施例。

在权利要求中，任何括号内的参考标记都不应该被看作是限制权利要求。单词“包括”不排除不同于权利要求中列出那些的元件或步骤的存在。放在一个元件之前的单词“一个”不排除多个这种元件的出现。本发明可以借助于包含几个不同的元件的硬件和一个被适当编程的计算机来实现。

在设备权利要求中枚举了几个装置，这些装置的部分可以由一个和相同元件的硬件来体现。某些措施在相互不同的从属权利要求中被陈述的简单事实不意味着这些方法的组合不能有益地使用。

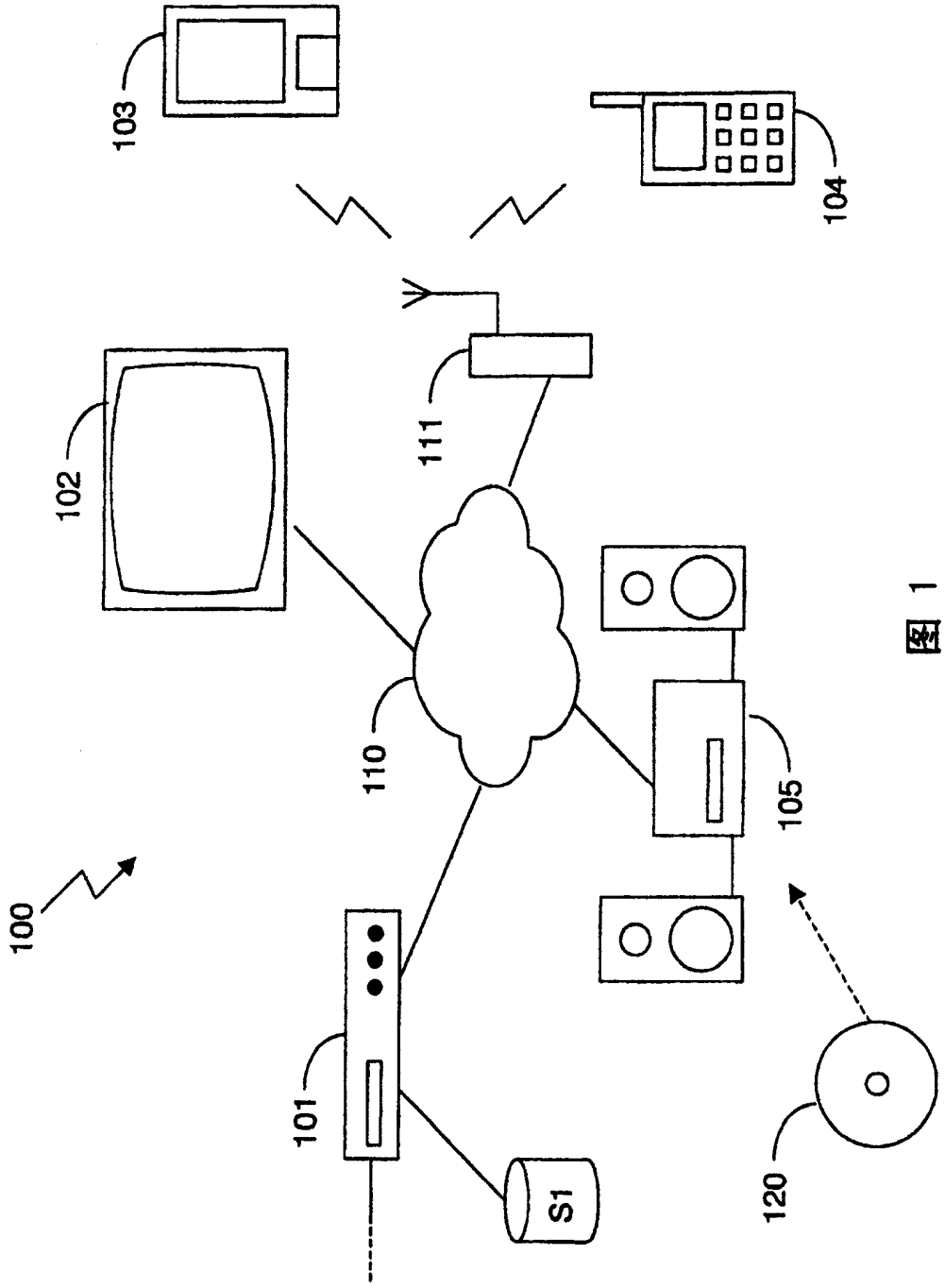


图 1

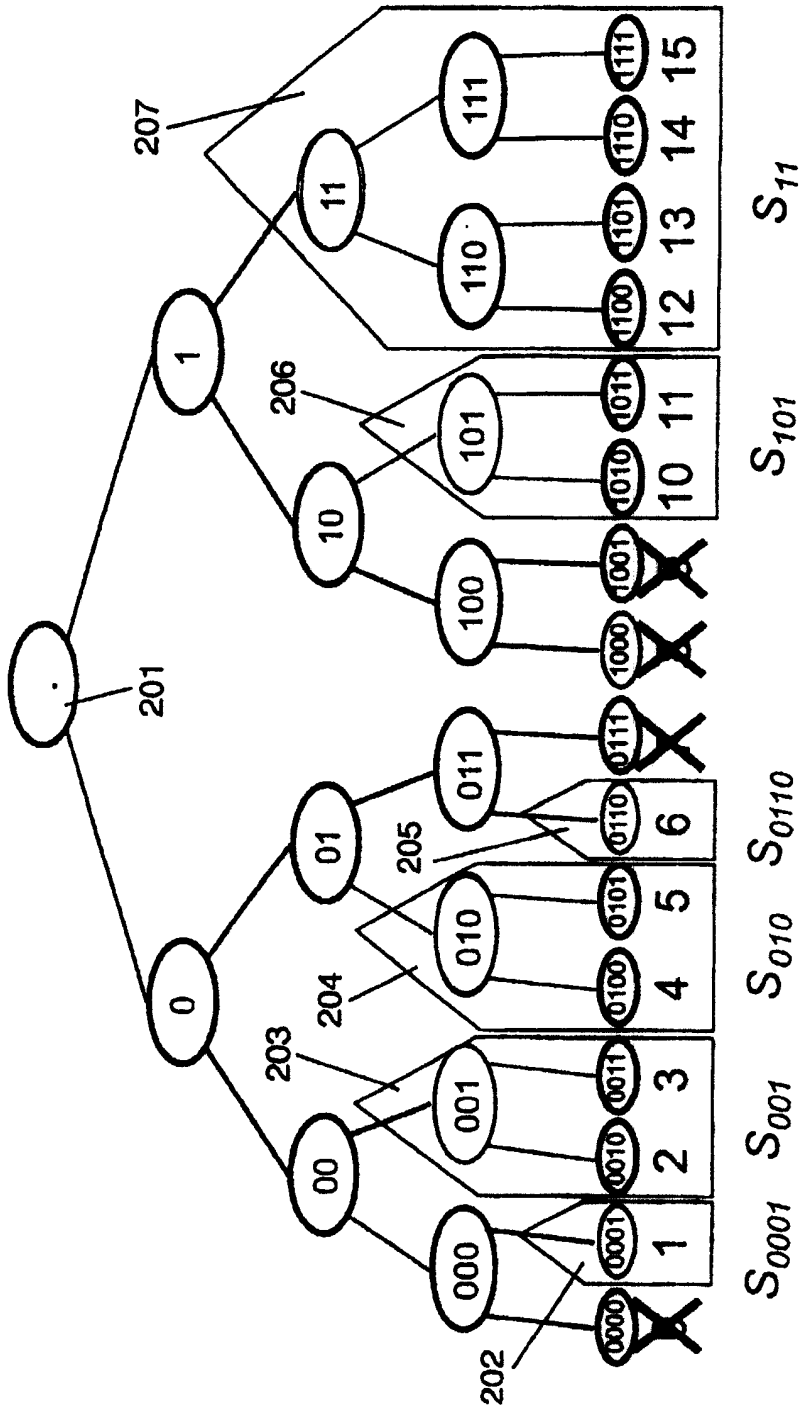

207
201
206
205
204
203
202
0
1
00
01
10
11
000
001
010
011
100
101
110
111
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111
1 2 3 4 5 6 10 11 12 13 14 15
S_{0001} S_{001} S_{010} S_{0110} S_{101} S_{11}

图 2

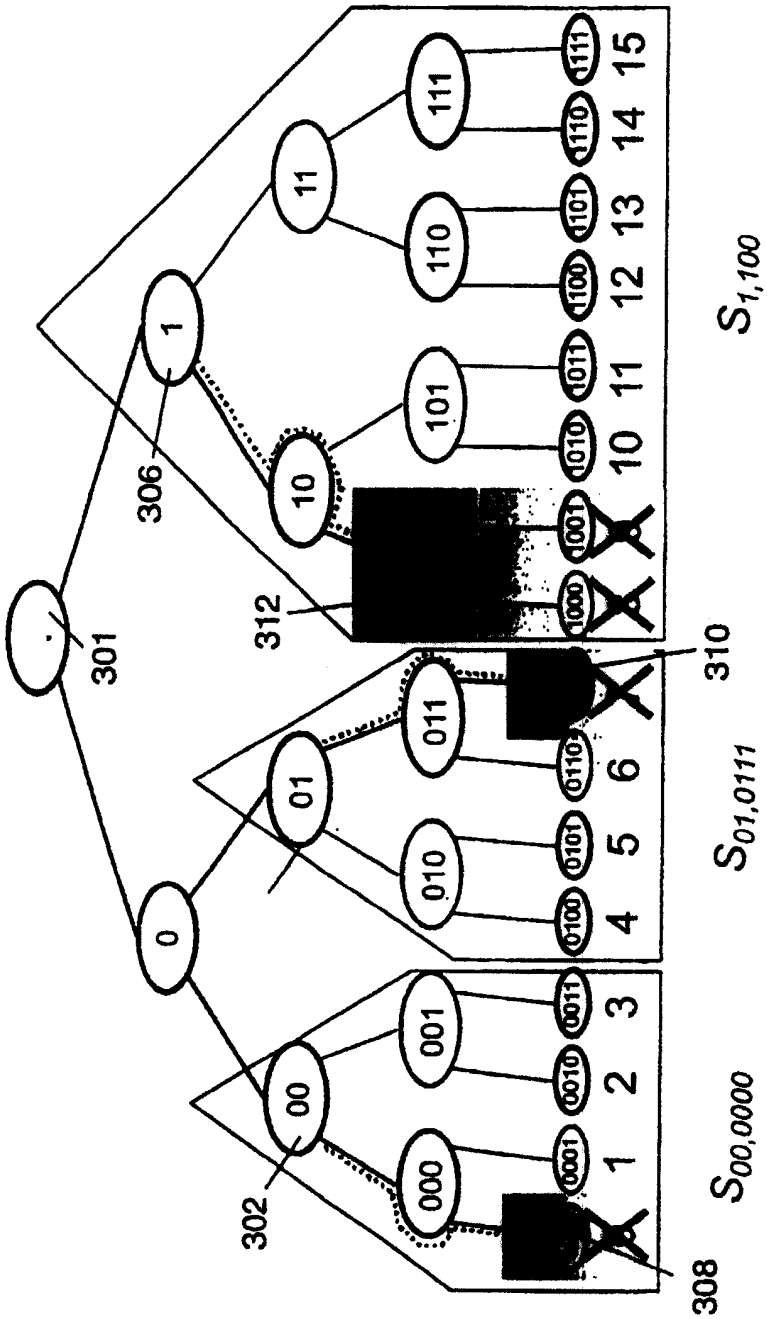

301
306
312
310
302
308
$S_{00,0000}$
$S_{01,0111}$
$S_{1,100}$
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

图 3

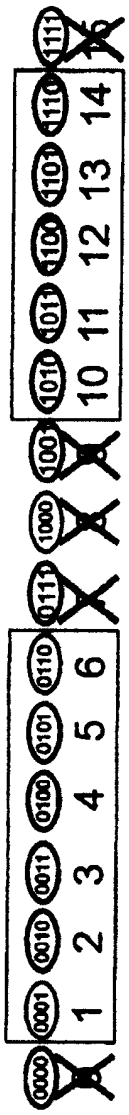

0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111
1 2 3 4 5 6
10 11 12 13 14
$S_{0,7}$
$S_{9,15}$

图 4

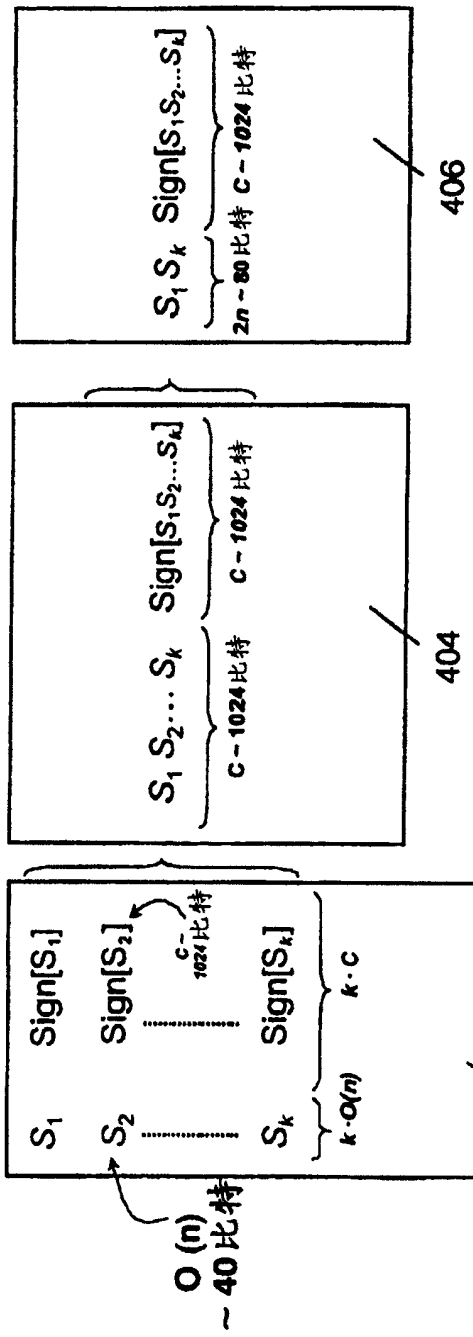

S1 Sign[S1]
S2 Sign[S2]
c~1024比特
Sk Sign[Sk]
k·Q(n) k·c
402
O(n)~40比特
S1 S2 ... Sk Sign[S1,S2...Sk]
c-1024比特 c-1024比特
404
S1 Sk Sign[S1,S2...Sk]
2n~80比特 c-1024比特
406

图 5