[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
G11B 20/10 (2006.01)
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 01806075.7

[45] 授权公告日 2008 年 8 月 20 日

[11] 授权公告号 CN 100413246C

[22] 申请日 2001.11.9 [21] 申请号 01806075.7

[30] 优先权

[32] 2000.11.9 [33] JP [31] 341431/00

[86] 国际申请 PCT/JP2001/009841 2001.11.9

[87] 国际公布 WO2002/039655 日 2002.5.16

[85] 进入国家阶段日期 2002.9.4

[73] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 石黑隆二 浅野智之

[56] 参考文献

JP11－187013A 1999.7.9

JP11－205305A 1999.7.30

CN12124962A 1999.8.4

US6049878A 2000.4.11

CN1166899A 1997.12.3

审查员 张艳青

[74] 专利代理机构 北京市柳沈律师事务所

代理人 黄小临

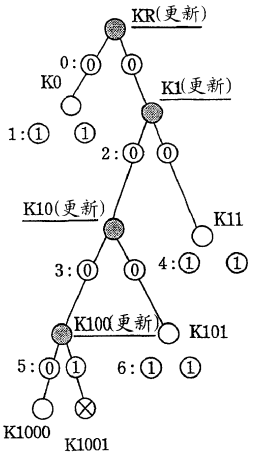
权利要求书 2 页 说明书 23 页 附图 17 页

[54] 发明名称

信息处理装置及信息处理方法

[57] 摘要

本发明是使采用了有效密钥块(EKB)的取消实体的检测处理成为可能的信息处理系统及方法，其根据用于树结构的密钥发布结构的有效化密钥块(EKB)来判定作为取消(排除)实体的装置或服务提供商等。 在公钥证明书中存储可识别分层密钥发布树的位置的 ID，基于从公钥证明书取得的 ID 实行采用了有效密钥块(EKB)的标记的跟踪处理，判定是否是可进行 EKB 处理(解密)的位置的 ID，并判定有没有对应于 ID 的实体的取消。



1. 一种信息处理装置，对应于将固有的密钥与各个节点及叶对应的分层树结构的各叶，存储了由各个与上述分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密钥组，其特征在于：具有

通信装置（120），接收包含由下位节点密钥或叶密钥将上述分层树结构的更新节点密钥加密了的加密密钥数据的有效密钥块；和

控制装置（170），当与上述节点或叶对应的实体被指定为排除对象实体时，根据上述排除对象实体的识别符，执行上述有效密钥块中所包含的密钥配置识别标记的跟踪处理，使用上述密钥组，验证上述有效密钥块是否可以解密；

在上述控制装置中，验证上述信息处理装置是否为排除对象实体。

2. 权利要求 1 中记载的信息处理装置，其特征在于：

上述控制装置进一步地读出上述验证对象实体的识别符中包含的、在上述分层树结构中的节点或叶的位置信息，

并从上述有效密钥块中的上述密钥配置识别标记，判别上述有效密钥块中的各个加密密钥数据的下位层的加密密钥数据的有无，

上述控制装置根据上述位置信息，执行跟踪上述标记的处理。

3. 权利要求 2 中记载的信息处理装置，其特征在于：

上述控制装置根据上述位置信息执行对上述标记的跟踪处理的结果，判定可否到达上述验证对象实体的对应的节点位置或叶位置。

4. 权利要求 3 中记载的信息处理装置，其特征在于：

上述控制装置在不能到达上述验证对象实体的对应的节点位置或叶位置时，根据是否属于没有被更新的节点密钥的下位的判定，执行上述解密可能性的判定。

5. 权利要求 4 中记载的信息处理装置，其特征在于：还具有

加密处理装置（150），取得与构成上述分层树结构的节点或叶对应的实体的识别符，使用执行上述有效密钥块的跟踪处理而得到的下位层节点密钥，将利用上述节点密钥把用以将内容加密的内容密钥加密了的加密内容密钥解密，而得到内容密钥。

6. 一种信息处理方法，对应于将固有的密钥与各个节点及叶对应的分层

树结构的各叶，存储了由各个与上述分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密钥组，其特征在于：包括

通信步骤，接收包含由下位节点密钥或叶密钥将上述分层树结构的更新节点密钥加密了的加密密钥数据的有效密钥块；和

控制步骤，当与上述节点或叶对应的实体被指定为排除对象实体时，根据上述排除对象实体的识别符，执行上述有效密钥块中所包含的密钥配置识别标记的跟踪处理，使用上述密钥组，验证上述有效密钥块是否可以解密；

在上述控制步骤中，验证上述信息处理方法是否为排除对象实体。

7. 权利要求 6 中记载的信息处理方法，其特征在于：

上述控制步骤进一步地读出上述验证对象实体的识别符中包含的、在上述分层树结构中的节点或叶的位置信息，

并从上述有效密钥块中的上述密钥配置识别标记，判别上述有效密钥块中的各个加密密钥数据的下位层的加密密钥数据的有无，

上述控制步骤根据上述位置信息，执行跟踪上述标记的处理。

8. 权利要求 7 中记载的信息处理方法，其特征在于：

上述控制步骤根据上述位置信息执行对上述标记的跟踪处理的结果，判定可否达到上述验证对象实体的对应的节点位置或叶位置。

9. 权利要求 8 中记载的信息处理方法，其特征在于：

上述控制步骤在不能到达上述验证对象实体的对应的节点位置或叶位置时，根据是否属于没有被更新的节点密钥的下位的判定，执行上述解密可能性的判定.

10. 权利要求 9 中记载的信息处理方法，其特征在于：还包括

加密处理步骤，取得与构成上述分层树结构的节点或叶对应的实体的识别符，使用执行上述有效密钥块的跟踪处理而得到的下位层节点密钥，将利用上述节点密钥把用以将内容加密的内容密钥加密了的加密内容密钥解密，而得到内容密钥。

信息处理装置及信息处理方法

技术领域

本发明涉及信息处理装置及信息处理方法和程序记忆媒体，特别涉及发布在伴有加密处理的系统中的加密处理密钥的系统及其方法，进而详细地涉及采用树结构的分层密钥发布方式，使有效地实施特定装置的取消（排除）成为可能。

背景技术

目前，游戏程序、音响数据、图像数据等，各种各样的软件数据（以下，将它们称为内容（Content）），通过因特网等的网络或DVD、CD等的可流通的记忆媒体的流通盛行起来了。这些流通内容通过用户所有的PC（Personal Computer）、游戏机，完成数据接收或记忆媒体的安装后进行再生，或者通过来自于存储在附属于PC等的记录再生机器内的记录装置如存储于存储卡、硬盘等中的存储媒体的新的再生而加以利用。

在视频游戏机、PC等的信息机器中，具有为从网络接收流通内容或者为访问DVD、CD等的接口，进而具有作为对再生内容的必要的控制手段、程序、数据的存储域而使用的RAM、ROM等。

音乐数据、图像数据或程序等的各种各样的内容，由来自于作为再生机器而利用的游戏机、PC等的信息机器本身的用户指令，或者通过连接的输入手段的用户指令，从记录媒体调出，通过信息机器本身或连接的显示器、扬声器等进行再生。

游戏程序、音乐数据、图像数据等很多的软件·内容，一般是由其制作者、经销者保有着出版权等。从而，当发布这些内容时，采用了有一定的使用限制，即只对正规的用户允许软件的使用，不能进行没有许可的复制等的，即采用着考虑了安全的结构。

实现对用户的使用限制的一种方法是发布内容的加密处理。例如，一种手段是发布通过因特网等加密了的音响数据、图像数据、游戏程序等的各种内容，同时只对确认出是正规用户的人，解密所发布的加密内容，即提供解密密钥的结构。

加密数据可以通过指定的手续的解密处理恢复成可利用的解密数

据（明文）。由此可充分了解到在这样的信息的加密处理中使用加密密钥，在解密处理中使用解密密钥的数据加密、解密的方法。

在使用加密密钥和解密密钥的数据加密·解密方法的形态中有各种各样的种类，但作为其中的一个示例有所谓称为通用密钥加密方式的方式。通用密钥加密方式是以用于数据的加密处理的加密密钥和用于数据的解密处理的解密密钥作为通用的密钥，将用于这些加密处理、解密的通用密钥给与正规的用户，取消没有密钥的非法用户的数据访问。这个方式的代表方式中有 DES（数据加密标准：Deta encryption standard）。

用于上述加密处理、解密的加密密钥、解密密钥，例如基于有的口令等，可以得到应用于散列函数等的单方向性函数。所谓的单方向性函数是指从它的输出非常难以反方向地求出输入的函数。例如，以用户决定的口令作为输入应用单方向性函数，基于其输出生成加密密钥、解密密钥。如此，从得到的加密密钥、解密密钥反方向地求出其原始数据的口令，实质上是不可能的。

而且，以加密时使用的加密密钥的处理和解密时使用的解密密钥的处理，作为不同的算法的方式，是所谓的称为公钥加密方式的方式。公钥加密方式是不特定的用户使用可使用的公钥的方法，使用其特定个人发行的对特定个人的加密文档的公钥，进行加密处理。通过公钥加密了的文档，仅能够通过使用其加密处理的公钥对应的私钥进行解密处理。由于私钥仅为发行了公钥的个人所有，所以通过其公钥加密了的文档，只有持有私钥的个人可以解密。在公钥加密方式的代表方式中，有 RSA（Rivest-Shamir-Adleman）加密。通过利用这样的加密方式，使加密内容仅对正规的用户可解密的系统成为可能。

在如上述的内容发布系统中广泛采用着下述结构，即加密内容后存储于网络或 DVD、CD 等的记录媒体中提供给用户，仅给合法的用户提供解密加密内容的内容密钥的结构。当前正提出，为防止内容密钥本身的非法的复制等的加密内容密钥并提供给合法的用户，用只有合法用户才有的解密密钥，解密加密内容密钥并以内容密钥作为可使用的结构。

是否是合法的用户的判定，一般是例如在内容发送者的内容提供商和用户装置之间，或发送接收内容的用户装置之间，在发布内容或

内容密钥之前，通过实行认证处理而实行的。

不过，有时会发生下述情形，例如不小心泄露了自己装置的私钥，非法的用户装置将该私钥存储于装置中成为合法的装置，从而进行内容的接收等。为应对这样的情形，密钥的管理中心将被称为非法者清单（黑清单）的非法装置的ID列表后的消除清单，发布给合法装置，通过消除清单进行通信对方的ID是否包含在清单中的检查。

消除清单列表化非法装置的ID，为防止涂改可附加密钥发行中心的署名，被称为CRL（Certificate Revocation List），随着新的非法装置的产生，顺次更新，并发布给合法的装置。不过，随着非法装置的增加，消除清单中记录的非法装置的ID持续增加，使清单的大小（数据量）变大，清单数据的发布负荷也增大，而且，在发布目地的的合法装置内存储并保存清单也成为记忆空间的负担。

发明内容

本发明是针对于伴随上述那样的消除清单的数据的增大造成的处理负荷、在装置中的清单存储的记忆空间的问题点而提出的，其目的是提供不使用非法装置的ID清单而通过使用分层树结构的密钥发布结构，能够检测、排除非法装置的信息处理装置及信息处理方法和程序记忆媒体。

涉及本发明的信息处理装置，对应于将固有的密钥与各个节点及叶对应的分层树结构的各叶，存储了由各个与上述分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密钥组，其特征在于：具有

通信装置，接收包含由下位节点密钥或叶密钥将上述分层树结构的更新节点密钥加密了的加密密钥数据的有效密钥块；和

控制装置，当与上述节点或叶对应的实体被指定为排除对象实体时，根据上述排除对象实体的识别符，执行上述有效密钥块中所包含的密钥配置识别标记的跟踪处理，使用上述密钥组，验证上述有效密钥块是否可以解密；

在上述控制装置中，验证上述信息处理装置是否为排除对象实体。

在涉及本发明的信息处理装置中，验证对象实体的识别符包含该实体的上述分层树结构中的对应的节点或叶的位置信息，上述有效密

钥块（EKB）中的密钥配置识别标记，是作为识别有效密钥块（EKB）中的各个加密密钥数据的下位层的加密密钥数据的有无的标记而构成的。跟踪处理是基于验证对象实体的识别符中包含的、在该实体的分层树结构中的位置信息，作为跟踪标记的处理来实行的。

进而，在涉及本发明的信息处理装置中，验证对象实体的识别符包含在该实体的分层树结构中对应的节点或叶的位置信息，上述有效密钥块（EKB）中的密钥配置识别标记，是作为识别有效密钥块（EKB）中的各个加密密钥数据的下位层的加密密钥数据的有无的标记而构成的。这个信息处理装置通过基于验证对象实体的识别符的标记的跟踪处理，由可否到达验证对象实体的对应的节点位置或叶位置的判定及在不能到达时是否属于没有被更新的节点密钥的下位的判定，来实行解密可能性的判定。

进而，在涉及本发明的信息处理装置中，验证对象实体的识别符是存储于该实体的公钥证明书中的识别符，信息处理装置具有从该实体的公钥证明书中取得验证对象实体的识别符的结构。

进而，涉及本发明的信息处理装置，在由构成分层树结构的节点或叶对应的实体提供的加密内容的解密中，从实体的公钥证明书中取得该实体的识别符，实行基于该取得的识别符的有效密钥块（EKB）的标记的跟踪处理，判定该实体是否是取消·实体，同时实行基于从有效密钥块（EKB）取得的内容加密密钥 Kcon 的加密内容的解密处理。

而且，本发明是与将各个节点及叶与固有密钥相关联的分层树结构的各叶相关联，存储了由各个分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密钥组的信息处理装置中的信息处理方法，一种信息处理方法，对应于将固有的密钥与各个节点及叶对应的分层树结构的各叶，存储了由各个与上述分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密胡组，其特征在于：包括

通信步骤，接收包含由下位节点密钥或叶密钥将上述分层树结构的更新节点密钥加密了的加密密钥数据的有效密钥块；和

控制步骤，当与上述节点或叶对应的实体被指定为排除对象实体时，根据上述排除对象实体的识别符，执行上述有效密钥块中所包含

的密钥配置识别标记的跟踪处理，使用上述密钥组，验证上述有效密钥块是否可以解密；

在上述控制步骤中，验证上述信息处理方法是否为排除对象实体。

进而，涉及本发明的信息处理方法中，验证对象实体的识别符包含该实体的分层树结构中的对应的节点或叶的位置信息，有效密钥块（EKB）中的密钥配置识别标记，是作为识别有效密钥块（EKB）中的各个加密密钥数据的下位层的加密密钥数据的有无的标记而构成的。跟踪处理是基于验证对象实体的识别符中包含的、在该实体的分层树结构中的位置信息，作为跟踪标记的处理来实行的。

在涉及本发明的信息处理方法中，验证对象实体的识别符包含在该实体的分层树结构中对应的节点或叶的位置信息，有效密钥块（EKB）中的密钥配置识别标记，是作为识别有效密钥块（EKB）中的各个加密密钥数据的下位层的加密密钥数据的有无的标记而构成的。这个信息处理方法通过基于验证对象实体的识别符的标记的跟踪处理，由可否到达验证对象实体的对应的节点位置或叶位置的判定及在不能到达时是否属于没有被更新的节点密钥的下位的判定，来实行解密可能性的判定。

进而，在涉及本发明的信息处理方法中，验证对象实体的识别符是存储于该实体的公钥证明书中的识别符，该信息处理方法是从该实体的公钥证明书中取得验证对象实体的识别符。

而且，涉及本发明的信息处理方法，在由构成分层树结构的节点或叶对应的实体提供的加密内容的解密中，从实体的公钥证明书中取得该实体的识别符，实行基于该取得的识别符的有效密钥块（EKB）的标记的跟踪处理，判定该实体是否是取消·实体，同时实行基于从有效密钥块（EKB）取得的内容加密密钥 Kcon 的加密内容的解密处理。

更进一步，本发明是提供使在与将各个节点及叶与固有密钥相关联的分层树结构的各叶相关联，存储了由各个上述分层树结构的自身的叶对应的叶密钥和至上位层的路径上的节点密钥组成的密钥组的信息处理装置中的信息处理在计算机·系统上实行的计算机·程序的程序记忆媒体，其中，此记忆媒体中存储的计算机·程序包含与节点或叶对应的实体是否是作为排除对象实体的取消·实体的验证处理步

骤，验证处理步骤具有通过由验证对象实体的存储密钥组是否可解密包含由下位节点密钥或叶密钥将分层树结构的更新节点密钥加密了的加密密钥数据的有效密钥块（EKB）的判定来实行的步骤。解密可能性的判定步骤包含由基于验证对象实体的识别符的有效密钥块（EKB）中的密钥配置识别标记的跟踪处理来实行的步骤。

其中，涉及本发明的程序记忆媒体，是针对例如可实行各种各样的程序·代码的凡用计算机·系统，以计算机可读的形式提供计算机·程序的媒体。

这样的程序记忆媒体是定义了用于在计算机·系统上实现指定的计算机·程序的功能的、计算机·程序与记忆媒体的结构上或功能上的协同关系的媒体。换言之，通过该记忆媒体，在计算机·系统中安装计算机·程序，以此在计算机·系统上发挥协同的作用。

本发明的进一步其他的目的、特征和优点，将基于下述的本发明的实施示例和附图，通过更详细的说明加以明确。

附图说明

图 1 是表示应用了涉及本发明的信息处理装置的内容发布系统的框图。

图 2 是表示应用了涉及本发明的信息处理装置的记录再生装置的框图。

图 3 是说明有关在涉及本发明的信息处理装置中实行的各种密钥、数据的加密处理的树结构图。

图 4A 及图 4B 是表示针对涉及本发明的信息处理装置的各种密钥、数据的发布中使用的有效密钥块（EKB）的例图。

图 5 是表示针对涉及本发明的信息处理装置的内容密钥的有效密钥块（EKB）发布示例和解密处理示例的图。

图 6 是表示在涉及本发明的信息处理装置中的有效密钥块（EKB）的格式示例的图。

图 7A、图 7B 及图 7C 是说明有效密钥块（EKB）的标记结构的图。

图 8A 及图 8B 是表示同时发布有效密钥块（EKB）和内容密钥、内容的数据结构示例的图。

图 9 是表示在同时发布了有效密钥块（EKB）和内容密钥、内容时的装置中的处理示例的图。

图 10 是说明有关在记录媒体中存储了有效密钥块（EKB）和内容时的对应关系的图。

图 11 是表示伴随公钥加密方式的认证处理的取消实体验证序列的图。

图 12 是表示公钥证明书的结构示例的图。

图 13A 及图 13B 是表示用于进行取消实体判定的 EKB 跟踪处理过程的图。

图 14A 及图 14B 是表示用于进行取消实体判定的 EKB 跟踪处理过程的图。

图 15 是表示用于进行取消实体判定的 EKB 跟踪处理过程的过程图。

图 16 是说明有关使用了 EKB、公钥证明书的内容发布处理的图。

图 17 是说明分层树结构的类型分类的示例的图。

实施方式

可应用涉及本发明的信息处理装置中的处理的内容发布系统，如图 1 所示构成。

在图 1 表示的系统中，内容的发布方 10 对内容接收方 20 所具有的各种各样的内容可再生的机器，将内容或内容密钥加密并发送。在接收方 20 中的机器，将接收到的加密内容或加密内容密钥等解密，取得内容或内容密钥，进行图像数据、声音数据的再生或者各种程序的实行等。内容的发布方 10 和内容接收方 20 之间的数据交换，通过因特网等的网络，或者通过 DVD、CD 等的可流通的记忆媒体实行。

作为内容的发布方 10 的数据发布手段，有因特网 11、卫星广播 12、电话线路 13、DVD、CD 等的媒体 14 等，另一方面，作为内容接收方 20 的装置，有个人计算机（PC）21、便携装置（PD）22、便携式电话和 PDA（Personal Digital Assistants）等的便携机器 23、DVD、CD 播放机等的记录再生器 24、游戏终端等的再生专用器 25 等。这些内容接收方 20 的各装置，从网络等的通信手段或者媒体 30 取得来自内容发布方 10 提供的内容。

作为图 1 表示的内容接收方 20 的信息处理装置的一个示例，将记录再生装置 100 的结构框图表示在图 2 中。记录再生装置 100 具有输入输出 I/F（Interface）120、MPEG（Moving Picture Experts Group）

编解码器 130、具备了 A/D、D/A 转换器 141 的输入输出 I/F（Interface）140、加密处理手段 150、ROM（Read Only Memory）160、CPU（Central Processing Unit）170、存储器 180、记录媒体 195 的驱动 190，这些通过总线 110 相互连接着。

输入输出 I/F120，接收构成由外部供给的图像、声音、程序等的各种内容的数字信号，并输出到总线 110 上，同时接收总线 110 上的数字信号，并输出到外部。MPEG 编解码器 130，将通过总线 110 供给的 MPEG 编码后的数据进行 MPEG 译码，并输出到输入输出 I/F140，同时将由输入输出 I/F140 供给的数字信号进行 MPEG 编码，并输出到总线 110。输入输出 I/F140，内置着 A/D、D/A 转换器 141。输入输出 I/F140，接收作为由外部供给的内容的模拟信号，并用 A/D、D/A 转换器 141 进行 A/D（Analog Digital）转换，而作为数字信号输出到 MPEG 编解码器 130，同时将来自于 MPEG 编解码器 130 的数字信号，用 A/D、D/A 转换器 141 进行 D/A（Digital Analog）转换，而作为模拟信号输出到外部。

加密处理手段 150 具有，例如用 1 个芯片的 LSI（Large Scale Integrated Curcuit）构成的，实行作为通过总线 110 供给的内容的数字信号的加密、解密处理或认证处理，将加密数据、解密数据等输出到总线 110 上的结构。其中，加密处理手段 150 不局限于一个芯片 LSI，也可以通过组合各种的软件或者硬件的结构加以实现。关于通过软件结构的处理手段的结构在下面叙述。

ROM160 存储由记录再生装置处理的程序数据。CPU170 实行 ROM160、存储器 180 中记忆的程序，从而控制 MPEG 编解码器 130 和加密处理手段 150 等。存储器 180，例如是非易失性存储器，记忆 CPU170 实行的程序和 CPU170 的动作上必要的数据，进而由装置实行的加密处理中使用的密钥组。关于密钥组在后面进行说明。驱动 190 通过驱动可记录再生数字数据的记录媒体 195，从记录媒体 195 读出（再生）数字数据，并输出到总线 110 上，同时将通过总线 110 供给的数字数据，供给并记录于记录媒体 195。

记录媒体 195 是，例如 DVD、CD 等的光盘、光磁盘、磁盘、磁带或 RAM 等的半导体存储器等的可记忆数字数据的媒体，在本实施方式中，对驱动 190 采用可装卸的结构。但是，记录媒体 195 也可以采用

内置于记录再生装置100中的结构。

其中，图2中表示的加密处理手段150，也可以作为一个的1芯片LSI而构成，而且也可以通过组合软件、硬件的结构而实现的结构。

其次，用图3说明在由图1中表示的从内容发布方10，在给内容接收方20的各装置发布加密数据时的各装置中加密处理密钥的原有结构及数据发布结构。

在图3的最下层表示的号码0～15是内容接收方20的各个装置。即图3中表示的分层树（树）结构的各叶（叶：leaf）相当于各个装置。

各装置0～15，在制造时或装载时或在其后，如图3中表示的分层树（木）结构中，从本身的叶到达根的节点中所分配的密钥（节点密钥）及各叶的叶密钥组成的密钥组，存储于存储器。在图3的最下层表示的K0000～K1111是分别分配给各装置0～15的叶密钥，以从最上层的KR（根密钥）到最下层第2层的节（节点）中记载了的密钥：KR～K111作为节点密钥。

图3表示的树结构中，例如装置0拥有叶密钥K0000和节点密钥：K000、K00、K0、KR。装置5拥有K0101、K010、K01、K0、KR。装置15拥有K1111、K111、K11、K1、KR。其中，图3的树中装置只记载了0～15的16个，树结构也可以表示为4层结构的均衡的左右对称的结构，进而更多的装置在树中被构成，在树的各部中具有不同的层数结构。

在图3的树结构中包含的各信息处理装置（装置）中，包含着各种各样的记录媒体，例如，使用装置嵌入型或者在装置中自由装卸地构成的DVD、CD、MD、光存储器等的各种各样的类型的信息处理装置。进而，各种各样的应用服务是可共存的。在这样的不同的装置、不同的应用的共存结构之上，可应用图3所示的内容或者密钥发布结构的分层树结构。

在这些的各种各样的信息处理装置（装置）、应用共存的系统中，例如图3中用虚线围着的部分，即装置0、1、2、3作为使用相同的记录媒体的1个组而设定。例如，对用虚线围着的组内包含的装置，解决实行下述处理，即加密通用的内容并从提供商发送，发送各装置通用使用的内容密钥，或者从各装置同样加密并输出给提供商或清算机

关等内容费用的支付数据。内容提供商或清算处理机关等，进行和各装置的数据发送接收的机关，图 3 用虚线围着的部分，即装置 0、1、2、3 作为 1 个组，一并实行发送数据的处理。这样的组在图 3 的树中存在多个。内容提供商或清算处理机关等，进行和各装置的数据发送接收的机关，是作为信息数据发布手段进行的功能。

其中，节点密钥、叶密钥，既可以通过某一个的密钥管理中心统一管理，也可以通过进行对各组的各种各样的数据发送接收的提供商、清算机关等的信息数据发布手段，对每个组进行管理的结构。这些的节点密钥、叶密钥，例如在密钥泄漏等的情况下可实行更新处理，这种更新处理由密钥管理中心、提供商、清算机关等实行。

在这个树结构中，如从图 3 明确的那样，一个组中包含的装置 0、1、2、3，作为节点密钥具有通用的密钥 K00、K0、KR。通过利用这个节点密钥的共享结构，例如仅给装置 0、1、2、3 提供通用的内容密钥成为可能。例如，如果以通用地具有的节点密钥 K00 本身作为内容密钥而设定，则可以不实行新的密钥发送，仅进行装置 0、1、2、3 通用的内容密钥的设定是可能的。而且，如果将用节点密钥 K00 加密了的新的内容密钥 Kcon 的值 Enc（K00，Kcon），通过网络或者存储于记录媒体的，发布给装置 0、1、2、3，则仅有装置 0、1、2、3 使用在各个的装置中具有的共享节点密钥 K00，解开加密 Enc（K00，Kcon），得到内容密钥：Kcon 成为可能。其中，Enc（Ka，Kb）表示通过 Ka 将 Kb 加密了的数据。

而且，在某时刻 t 中，发现了装置 3 拥有的密钥：K0011、K001、K00、K0、KR，由攻击者（黑客）解析并已暴露时，之后，为保护在系统（装置 0、1、2、3 的组）中发送接收的数据，有必要从系统断开装置 3。因此，有必要将节点密钥 K001、K00、K0、KR 分别更新为新的密钥 K（t）001、K（t）00、K（t）0、K（t）R，并将其更新密钥传送给装置 0、1、2。在此，K（t）aaa 表示密钥 Kaaa 的新生代（Generation）：t 的更新密钥。

说明关于更新密钥的发布处理。密钥的更新，例如将通过图 4 所示的称为有效密钥块（EKB: Enabling Key Block）的块数据构成的表，存储于如网络或记录媒体中，并通过供给装置 0、1、2 加以实行。其中，有效密钥块（EKB）是通过为给构成如图 3 所示的树结构的各叶

对应的装置发布的新更新了的密钥的加密密钥构成的。有效密钥块（EKB）也称为密钥更新块（KRB: Key Renewal Block）。

在图 4A 中表示的有效密钥块（EKB）中，作为块数据可以构成只有节点密钥需要更新的装置具有可更新的数据结构。图 4A 的示例是，在图 3 中表示的树结构中的装置 0、1、2 中，以发布新生代 t 的更新节点密钥为目的而形成的块数据。如从图 3 所明确的，装置 0、装置 1 作为更新节点密钥，K（t）00、K（t）0、K（t）R 是必要的，装置 2 作为更新节点密钥，K（t）001、K（t）00、K（t）0、K（t）R 是必要的。

如图 4A 的 EKB 中所示 EKB 中包含多个加密密钥。最下层的加密密钥是 Enc（K0010，K（t）001）。这是通过装置 2 具有的叶密钥 K0010 被加密了的更新节点密钥 K（t）001，装置 2 可以通过本身具有的叶密钥解密这个加密密钥，得到 K（t）001。而且，使用由解密得到的 K（t）001，可解密从图 4A 的下面第二层的加密密钥 Enc（K（t）010，K（t）00），可以得到更新节点密钥 K（t）00。以下顺序，解密从图 4A 的上面第二层的加密密钥 Enc（K（t）00，K（t）0），解密更新节点密钥 K（t）0、从图 4A 的上面第一层的加密密钥 Enc（K（t）0、，（t）R），得到 K（t）R。另一方面，装置 0、1 不包含在更新节点密钥 K000 的对象中，作为更新节点密钥必要的是 K（t）00、K（t）0、K（t）R。装置 0、1，解密从图 4A 的上面第三层的加密密钥 Enc（K000，K（t）00），取得 K（t）00，以下解密从图 4A 的上面第二层的加密密钥 Enc（K（t）00，K（t）0），解密更新节点密钥 K（t）0、从图 4A 的上面第一层的加密密钥 Enc（K（t）0，K（t）R），得到 K（t）R。据此，装置 0、1、2 可以得到更新了的密钥 K（t）R。其中，图 4A 的索引表示作为解密密钥而使用的节点密钥、叶密钥的绝对地址。

在图 3 中表示的树结构的上位层的节点密钥：K（t）0、K（t）R 的更新是不必要的，只有节点密钥 K00 的更新处理是必要的情况下，采用图 4B 中表示的有效密钥块（EKB），就可以将更新节点密钥 K（t）00 发布给装置 0、1、2。

图 4B 中表示的 EKB，例如在特定的组中发布共享的新的内容密钥时是可利用的。作为具体示例，使用图 3 中用虚线表示的组内的装置 0、1、2、3 的记录媒体，作为新的通用的内容密钥 K（t）con 是必要

的。此时，使用将装置 0、1、2、3 的通用的节点密钥 K00 更新了的 K（t）00，同时将加密了的新的通用的更新内容密钥：K（t）con 的数据 Enc（K（t），K（t）con），发布给图 4B 中表示的 EKB。通过这种发布，在装置 4 等其他组的机器中，作为不被解密的数据的发布成为可能。

即，装置 0、1、2，如果进行 EKB 处理，使用得到的 K（t）00，解密上述加密语句，则在 t 时刻得到内容密钥 K（t）con 成为可能。

图 5 作为得到在 t 时刻的内容密钥 K（t）con 的处理示例，表示通过记录媒体接受了将使用 K（t）00 加密了的新的通用的内容密钥 K（t）con 后的数据 Enc（K（t）00，K（t）con）和图 4B 中表示的 EKB 的装置 0 的处理。即是以 EKB 的加密信息数据作为内容密钥 K（t）con 的示例。

如图 5 所示，装置 0 通过使用记录媒体中存储着的新生代：t 时刻的 EKB 和本身预先存储着的节点密钥 K000 进行和上述相同的 EKB 处理，生成节点密钥 K（t）00。进而，使用解密后的更新节点密钥 K（t）00，解密更新内容密钥 K（t）con，之后为使用它，用只有本身具有的叶密钥 K0000 加密并存储。

其中，装置 0 如果具备着安全地存储更新内容密钥 K（t）con 的手段，则没有必要用叶密钥 K0000 加密。

图 6 表示有效密钥块（EKB）的格式示例。版本 601 是表示有效密钥块（EKB）的版本的识别符。其中，版本具有识别最新的 EKB 的功能以及表示和内容之间的对应关系的功能。深度表示对有效密钥块（EKB）的发布目的地的装置的分层树的分层数。数据指针 603 是表示有效密钥块（EKB）中的数据部的位置的指针，标记指针 604 是表示标记部的位置的指针，署名指针 605 是表示署名的位置的指针。

数据部 606 存储如加密了的更新的节点密钥的数据。例如，存储有关图 5 所示的被更新了的节点密钥的各加密密钥等。

标记部 607 是表示存储于数据部的已加密了的节点密钥、叶密钥的位置关系的标记。使用图 7 说明这个标记的赋与规则。在图 7 中表示了将图 4A 说明的有效密钥块（EKB）发送到作为数据的目的处的示例。此时的数据如图 7 的表中所示。以此时的加密密钥中包含的顶点节点的地址作为顶点节点地址。这样的情况下，由于包含着根密钥的

更新密钥K（t），所以顶点节点地址成为KR。此时，例如最上层的数据Enc（K（t）0，K（t）R），在图7A中表示的分层树中表示的位置。在此，其次的数据是Enc（K（t）00，K（t）0），在树上前面的数据的左下方的位置。有数据的情况下标记设定为0，没有的情况下设定为1。标记是作为｛左（L）标记，右（R）标记｝而设定的。因为在最上层的数据Enc（K（t）0，K（t）R）的左面有数据，所以L标记＝0，因为在右面没有数据，所以R标记＝1。以下，对所有的数据设定标记，构成图7C中表示的数据列及标记列。

标记是为表示数据Enc（Kxxx，Kyyy）位于树结构的何处而设定的密钥配置识别标记。数据部中存储的密钥数据Enc（Kxxx，Kyyy）...，因为只不过是单纯地被加密了的密钥的罗列数据，所以通过上述标记可以判别作为数据存储了的加密密钥的树上的位置。不使用上述标记，如用先前的图4说明了的结构，使用与加密数据相对应的节点·索引，例如

0：Enc（K（t）0，K（t）root）

00：Enc（K（t）00，K（t）0）

000：Enc（K（（t）000，K（T）00）

...的数据结构也是可能的，但如果使用了这样的索引的结构，冗长数据的数据量将增加，通过网络的发布等不令人满意。对此，通过以上述的标记作为表示密钥位置的索引数据而使用，使以很小的数据量判别密钥位置成为可能。作为规定标记和节点的顺序的规则，例如在相同的深度中，按从左端到右端的顺序地记述，之后，可以使用向下一层的左端的节点移动的‘bredth first’的方法。

返回图6，进一步说明关于EKB格式。署名（signature）是由发行了有效密钥块（EKB）的发行局，如密钥管理中心、内容提供商、清算机关等实行的电子署名。领受了EKB的装置通过署名验证，确认是合法的有效密钥块（EKB）发行者发行了的有效密钥块（EKB）。

在上述的示例中，说明了有关仅将内容密钥同EKB一起发送的示例，以下说明有关同时发送用内容密钥加密了的内容和用根密钥、节点密钥等加密密钥加密了的内容密钥和通过EKB加密了的内容密钥加密密钥的结构。

图8中表示这种数据结构。在图8A中表示的结构中表示，Enc

（Kcon，content）801是用内容密钥（Kcon），将内容（Content）加密了的数据，Enc（Kroot，Kcon）802是用根密钥（Kroot），将内容密钥（Kcon）加密了的数据，Enc（EKB，Kroot）803是通过有效密钥块（EKB），将根密钥Kroot加密了的数据。

在此，根密钥Kroot也可以是图3所示的节点密钥(K000,K00…)。

图 8B 表示多个内容被记录于媒体，并分别利用着相同的 Enc（EKB，Kroot）805 时的结构示例，在这样的结构中，不给各数据附加相同的Enc（EKB，Kroot），也可以将表示连结于Enc（EKB，Kroot）的连结目的地的数据作为附加给各数据的结构。

图9中表示使用更新了图3所示的节点密钥K00的更新节点密钥K（t）00，将内容密钥Kcon加密了的情况下的处理示例。这种情况下，用图 3 的虚线框围着的组中的装置 3 例如作为因密钥的泄漏而被取消（排除）着的，通过对其他的组的成员，即装置 0、1、2，发布图 9 所示的有效密钥块（EKB）和用更新节点密钥 K（t）00 将内容密钥（Kcon）加密了的数据和用内容密钥（Kcon）将内容（content）加密了的数据，装置0、1、2可以得到内容。

在图9的右侧，表示了在装置0中的解密步骤。装置0，首先从领受了的有效密钥块，通过使用了本身保有的叶密钥 K000 的解密处理，取得K（t）00。其次，通过K（t）00的解密取得内容密钥Kcon，进而通过内容密钥Kcon进行内容的解密。通过这些处理，装置0可以利用内容。在装置1、2中也通过各种不同的处理步骤处理EKB，可取得内容密钥的加密密钥，同样可利用内容。

图3中表示的其他的组的装置4、5、6…，既使接收了这个同样的数据（EKB），也不能使用本身保有的叶密钥、节点密钥取得K（t）00。同样地，既使在被取消了的装置 3 中，用本身保有的叶密钥、节点密钥也不能取得K（t）00，只有具有合法权利的装置才可以解密并利用内容。

如此，如果使用利用了 EKB 的内容密钥的发送，数据量很小且安全地发布作为只有合法权利者可解密的加密内容成为可能。

其中，有效密钥块（EKB）、内容密钥、加密内容等是通过网络可安全地发布的结构，但将有效密钥块（EKB）、内容密钥、加密内容存储于 DVD、CD 等的记录媒体也是可能的。这种情况下，对存储于记录

媒体的加密内容的解密，如果构成如使用由存储于同一记录媒体的有效密钥块（EKB）的解密而得到的内容密钥，则仅通过预先保有合法权利者的叶密钥、节点密钥，可利用的加密内容的发布处理，即限定了可利用的用户装置的内容发布用简易的结构就可以实现。

图 10 表示将加密内容同有效密钥块（EKB）存储于记录媒体的结构示例。在图 10 表示的示例中，记录媒体中可存储内容 C1～C4，进而可存储与各存储内容对应的有效密钥块（EKB）相关联的数据，进而存储着版本 M 的有效密钥块（EKB_M）。例如 EKB_1 使用于生成将内容 C1 加密了的内容密钥 Kcon1，例如 EKB_2 使用于生成将内容 C2 加密了的内容密钥 Kcon2。在这个示例中，版本 M 的有效密钥块（EKB_M）被存储于记录媒体，因为内容 C3、C4 与有效密钥块（EKB_M）相关联，所以通过有效密钥块（EKB_M）的解密可以取得内容 C3、C4 的内容密钥。因为 EKB_1、EKB_2 没有存储于磁盘中，所以为通过新的提供手段如网络发布或记录媒体的发布解密各个内容密钥，必须取得必要的 EKB_1、EKB_2。

其次，说明有关使用了有效密钥块（EKB）的取消实体（ex.非法装置）的检测处理。首先，用图 11 说明使用了公钥加密方式的相互认证方法。在图 11 中，A 具有本身的私钥[Apri-Key]、公钥[Apub-Key]、有认证局署名的公钥证明书[Acert]，更具有公钥证明书的署名实体的认证局的公钥和 EKB 的署名实体的 EKB 发行局的公钥，B 具有本身的私钥[Bpri-Key]、公钥[Bpub-Key]、有认证局署名的公钥证明书[Bcert]、认证局的公钥、EKB 发行局的公钥。

用图 12 说明有关图 11 中表示的 A、B 分别具有的公钥证明书的结构。公钥证明书是在公钥加密方式中由认证局（CA: Certificate Authority 或 IA: Issuer Authority）发行的证明书，是通过用户向认证局提示出本身的 ID、公钥等，认证局方附加认证局的 ID 和有效期限等的信息，进而附加认证局的署名而制成的证明书。

图 12 所示的公钥证明书 51 包括含有证明书版本的号码、认证局对证明书利用者分配的证明书的通用号、用于电子署名的算法及参数、认证局的名称、证明书的有效期限、证明书利用者的 ID、证明书利用者的公钥的全部说明书信息 52 和认证局的电子署名 53。

电子署名 53 是对证明书的版本号、认证局对证明书利用者分配的

证明书的通号、用于电子署名的算法及参数、认证局的名称、证明书的有效期限、证明书利用者的姓名和证明书利用者的公钥全部，应用散列函数而生成散列值，并对其散列值使用认证局的私钥生成了的数据。

公钥证明书的证明书利用者的ID包含作为表示上述的密钥发布树结构的节点、叶位置的识别值的叶ID。如果是图3的树结构，那么装置0为[ID=0000]、装置1为[ID=0001]、装置15为[ID=1111]等等。基于这样的ID可以识别其装置等的实体是在树结构的哪个位置(叶或节点）的实体（ex.装置）。

图11的相互认证处理使用上述的公钥证明书进行。首先，B生成B的公钥证明书Bcert和随机数Rb，并发送给A。接收了这些的A，用认证局的公钥验证B的公钥证明书（B.Cert）。验证如果是NG，因为判定出公钥证明书是无效的，所以在此时刻中止认证处理，认证不成立。B的公钥证明书（B.Cert）的验证如果是OK，接着用B的公钥证明书（B.Cert）内的B的叶ID追寻保持于本装置中的EKB。

从前面说明的有关图7的说明可理解，存储于EKB内的标记用0、1表示着本节点的左面及右面的节点的密钥数据的有无。即有数据时设为0，没有数据时设为1。基于叶ID的EKB的跟踪处理，即追寻方法，使用基于这样的条件设定的标记进行。

用图13说明关于基于叶ID的EKB的跟踪（追寻方法）。如图13A所示，具有叶密钥K1001的装置作为取消装置[1001]。这时，EKB具有如图13B所示的加密密钥和标记的结构。图13B中表示的EKB，为取消图13A的一个装置[1001]，而成为更新了KR，K1、K10、K100的EKB。

通过处理这个EKB，取消装置[1001]以外的叶都可以取得被更新了的根密钥K（t）R。即，与节点密钥K0的下位关联的叶，因为将没有被更新的节点密钥K0保持在装置内，所以通过K0解密Enc（K0，K（t）R）可取得更新根密钥K（t）R。而且，K11以下的叶使用没有被更新的K11，通过K11解密Enc（K11，K（t）1）取得更新节点密钥K（t）1，进而，通过K（t）1解密Enc（K（t）1，K（t）R）可取得更新根密钥。既使对于K101的下位叶仅稍微增加解密步骤，就可以同样取得更新根密钥。

而且，具有没有被取消的叶密钥K1000的装置[1000]，用本身的

叶密钥解密 Enc（K1000，K（t）100），取得 K（t）100 后，顺序解密上位的节点密钥，可以取得更新根密钥。

因为只有被取消的装置[1001]，不能通过 EKB 处理取得本身的叶的上一层的更新节点密钥 K（t）100，所以终究不能取得更新根密钥 K（t）R。

具有图 13B 所示的数据部和标记的 EKB，从 EKB 发行局发布给没被取消的合法的装置，并存储于装置内。

在相互认证中，如果进行图 13A 中表示的取消装置[ID＝1001]，和例如某些内容提供商之间图 11 中表示的公钥方式的相互认证，则内容提供商就从图 13A 的取消装置[ID＝1001]接收公钥证明书，验证公钥证明书之后，从公钥证明书取得 ID。这个 ID 是[1001]，表示 EKB 发布树结构的叶位置。

接收了 ID[1001]的内容提供商，验证与 ID＝1001 的叶对应的装置，在 EKB 中是否是作为有效的叶装置而设定着。这个验证，即是作为判定叶[1001]可否取得被更新了的根密钥 K（t）R 的处理而实行的。

例如，如果是属于非更新节点密钥（图 13A 中的 K0，K11 等）的下位的叶，则可以明确没有被取消，可判定出是合法装置，是属于更新节点密钥的下位的叶时，通过可取得其更新节点密钥的加密数据是否存储于 EKB，可判定其实体是否被取消了。

作为判定处理的一个示例，说明基于 EKB 中存储了的标记进行 EKB 跟踪处理的示例。EKB 跟踪处理是判定从上位的根密钥可否追寻密钥发布树的处理。例如，图 13A 中的叶[1001]的 ID 的[1001]为[1]、[0]、[0]、[1]的 4 位，按照从最上位的位到下位位的顺序追寻树。位如果为 1 则进入右侧，如果为 0 则进入左侧。

ID[1001]的最上位位是 1，从图 13A 的根，进入右侧。EKB 内的最初的标记是 0：｛0，0｝，判定出两枝有数据，进入右侧追寻到 K1。接着进入 K1 的下位的节点。ID[1001]的第 2 位是 0，进入左侧。表示 K1 的下位有无数据的标记如图 13A 及图 13B 所示的 2：｛0，0｝，判定出在两枝有数据，进入左侧追寻到 K10。进而，ID[1001]的第 3 位是 0，进入左侧。表示 K10 的下位有无数据的标记如图 13A 及图 13B 所示的 3：｛0，0｝，判定出两枝有数据，进入左侧追寻到 K100。进而，ID[1001]的最下位位是 1，进入右侧。表示 K100 的下位有无数据

的标记如图 13A 及图 13B 所示的 5: {0, 1}，在右侧没有数据。从而，判定不追寻到节点[1001]，并判定出 ID[1001]的装置是不能通过 EKB 取得更新根密钥的装置，即是取消装置。

例如，有图 13A 的叶密钥 K1000 的装置 ID 是[1000]，如果实行基于和上述同样的 EKB 内的标记的 EKB 跟踪处理，即追寻树的处理，因为可以追寻到节点[1000]，所以判定出是可通过 EKB 取得更新根密钥的没有被取消的合法的装置。

而且，例如对没有被更新的节点密钥如 K0、K11 等的下位的叶，也不能追寻到叶本身，但这时，追寻到没有被更新的终端节点是可能的。没有被更新的节点的下位的叶使用没有被更新的节点密钥可进行 EKB 的处理，因为可以取得更新根密钥，所以是合法的装置。是否是没有被更新的节点密钥，通过与该节点对应的标记可判定。与没有被更新的节点密钥 K0、K11、K101 对应的标记为 1: {1, 1}、4: {1, 1}、6: {1, 1}，它们存在更下位的节点或叶，但在 EKB 内表示着没有加密密钥数据，并判定出它们下位的叶的装置是没有被取消的有效的合法装置。

图 13 中表示的示例是仅对于一个装置的取消状态，如图 14 所示一并取消某节点下面的所有的叶装置也是可能的。此时的 EKB 的数据（加密密钥）、标记如图 14B 所示。

例如，如果内容提供商从对应已被取消的 K1000 的叶装置，接收公钥证明书取得了 ID[1000]，则基于这个 ID[1000]、基于 EKB 的标记实行追寻树的处理。

ID[1000]的最上位位是 1，从图 14A 的根，进入右侧。EKB 内的最初的标记是 0: {0, 0}，判定在两枝有数据，进入右侧追寻到 K1。接着进入 K1 的下位的节点。ID[1000]的第 2 位是 0，进入左侧。表示 K1 的下位有无数据的标记是图 13A 及图 13B 中表示的 2: {1, 0}，在左侧没有数据。从而，不追寻到节点[1000]。对应此时的终端节点 K1 的标记是{1, 0}，不是没有下位数据的{1, 1}。

标记{1, 0}表示仅在 K1 的右侧的下位的节点或叶中，为取得可解密的已被更新的 K1（t）的加密密钥数据已被存储于 EKB 中。

这样，基于叶 ID 追寻到的最终地点是节点，其最终节点的对应标记具有{1, 1}以外的值时，表示在 EKB 内有更下位的加密密钥数据。

这时，具有该 ID 的叶装置，因为不能通过 EKB 的处理取得已被更新的根密钥，所以判定出是已被取消的装置。

如此，在认证处理中基于从通信对方取得的公钥证明书中存储的叶 ID，使判定通信对方是否是已被取消成为可能。

返回图 11，继续有关认证处理顺序的说明。A 基于从由 B 接收的公钥证明书取出的 B 的叶 ID，实行追寻基于上述那样的 EKB 的标记的树的处理，判定 ID 表示的叶位置是否是通过 EKB 处理的可取得更新根密钥的位置，是可进行 EKB 处理的位置时，判定出是没有被取消的合法装置。是不可进行 EKB 处理的叶位置时，判定出是被取消的非法的装置，并作为认证不成立而中止处理。

判定出是基于 ID 的可进行 EKB 处理的装置时，用 A 的私钥给从 B 接收了的随机数 Rb 署名并生成 Sig_A(Rb)，进而生成随机数 Ra。A 在这些的 Sig_A(Rb)、Ra 中，将自己的装置内存储的 EKB 和公钥证明书 A.Cert 发送给 B。

B 用认证局的公钥验证 A 的公钥证明书（A.Cert），如果验证 OK，就用 EKB 发布机关的公钥进行接收 EKB 的验证。EKB 如上述那样，为防止涂改，用 EKB 发布机关的公钥制成署名，B 使用 EKB 的公钥进行验证处理。如果验证 OK，取得 A 的公钥证明书（A.Cert）内的 A 的叶 ID，基于用上述的图 13、14 的说明同样的叶 ID 追寻 EKB。

追寻不到时，判定出 A 是被取消的装置，认证不成立，中止其后面的处理。其中，A 不局限于装置，也可以是内容提供商、服务提供商，也可以是具有不是图 13、图 14 中表示的树结构的最下层的叶的中途节点的密钥。例如，是与图 13、图 14 中表示的 K10 的节点密钥位置对应的节点时，其内容提供商或服务提供商的 ID 为[10]，基于 ID[10]实行追寻利用了 EKB 的标记的 EKB 的处理，进行是否已被取消的判定。

通过追寻 EKB 的处理能追寻时，用 A 的公钥证明书（A.Cert）内的公钥 A.Pub-Key 验证从 A 接收的 Sig_A(Rb)。验证如果 OK，就用 B.pri-.Key(B 的私钥)给 Ra 署名，生成 Sig_B(Ra)，将生成的 Sig_B(Ra)发送给 A。

接收了 Sig_B(Ra)的 A，使用从 B 的公钥证明书（B.Cert）取得的 B 的公钥，验证 Sig_B(Ra)。验证如果 OK，则判定认证成立。

图 15 中表示利用了 EKB 的取消装置判定处理的处理流程。说明关

于流程的各步骤。步骤 S101 中，从通信对方（认证对方）的公钥证明书取得 ID。步骤 S102 中，基于使用取得了的 ID 的 EKB 的标记，实行以 ID 表示的叶或节点为目标的跟踪处理。

跟踪处理使用上述的图 13、图 14 说明了的顺序实行。判定跟踪处理的结果、能否追寻到 ID 表示的叶或节点，既使是不能追寻到的情况，在 ID 表示的叶或节点中能否进行 EKB 处理，即能否取得更新根密钥（S103）。

如果判定出是在可进行 EKB 处理的位置，就进入步骤 S104，判定出与 ID 对应的装置是没有被取消的合法的装置。另一方面，如果判定出是在不可进行 EKB 处理的位置，就进入步骤 S105，判定出与 ID 对应的装置是被取消的非法的装置。

其次，说明伴随使用了有效密钥块（EKB）的取消装置（非法装置）的判定处理的内容利用处理示例。图 16 中表示的示例是提供商 A 将内容加密并发布给装置（ID = 00xx）的示例。

内容提供商 A，对装置[00xx]发送将 A 的公钥证明书[A.Cert]、用本身的私钥署名了内容密钥的数据[Sig_A(Kcon)]、将有效密钥块[EKB]、用更新根密钥加密了的内容密钥的数据[Enc(K(t)root，Kcon)]，进而将用内容密钥加密了的内容的数据[Enc(Kcon，Content)]。

接收了这些的数据的装置[00xx]，首先用认证局的公钥验证接收了的 A 的公钥证明书[A.Cert]。验证如果 OK，从 A 的公钥证明书[A.Cert]取得 A 的公钥和 A 的 ID。

其次，使用从 A 的公钥证明书[A.Cert]取出的 A 的公钥验证用 A 的私钥署名了的内容密钥的数据[Sig_A(Kcon)]。验证如果 OK，更进一步，基于从公钥证明书[A.Cert]取出的 A 的 ID 实行上述的 EKB 跟踪处理，判定在 A 的 ID 表示的叶或节点位置中能否进行 EKB 处理。

通过 EKB 的跟踪处理，如果判定出 A 不是与被取消了的节点或叶相当的，装置[00xx]就从领受了的有效密钥块通过使用了本身保有的叶密钥、节点密钥的解密处理，取得更新根密钥 K(t)root。其次，通过更新根密钥(K(t) root)的解密，进一步取得内容密钥 Kcon。进而，通过取得的内容密钥 Kcon，进行内容的解密。通过这些的处理，装置[00xx]成为可以利用内容。

在上述的处理中，在取得的内容的发布者的公钥证明书之后，实行公钥证明书的验证，在取得了内容发布者的公钥和 ID 之后，因为进行 EKB 的处理、内容的解密，所以基于 ID 内容发布者的特定是可能的，使防止流通发布者不明确的内容成为可能。

其中，图 16 中表示的示例是提供商 A 给装置（ID = 00xx），加密并发布内容的示例，是提供商 A 实行对内容密钥的署名，在装置中进行提供商 A 的公钥的署名验证处理的示例，这样不是在来自于其他的提供商的发布内容的装置中的存储、再生处理中，例如，当将用户生成的或取得的内容记录于装置的记录媒体中时，也可以使用装置本身的私钥进行署名，并记录于记录媒体。如果实行作为对这样的记录媒体的存储内容的加密密钥的内容密钥的署名的结构，在内容再生时，就必须使用装置的公钥实行内容密钥的署名验证，取消非法的内容的存储再生成为可能。

说明了有关以加密密钥作为根密钥、节点密钥、叶密钥等图 3 的分层树结构而构成的，将内容密钥等和有效密钥块（EKB）一起加密并发布的结构，以下说明关于将定义着节点密钥等的分层树结构分类给各装置的每个类别，实行有效的密钥更新处理的结构。

图 17 中表示分层树结构的类别分类的一个示例。在图 17 中，分层树结构的最上层设定根密钥 Kroot2301，在下面的中间层设定节点密钥 2302，在最下层设定叶密钥 2303。各装置保有各自的叶密钥和从叶密钥至根密钥的一系列的节点密钥、根密钥。

在此，作为一个示例，以从最上层到第 M 层的某节点作为类别节点 2304 而设定。即以第 M 层的各个节点作为特定类别的装置设定节点。以第 M 层的一个节点作为顶点之下、M + 1 层之下的节点、叶，作为与其类别中包含的装置有关的节点及叶。

例如，在图 17 的第 M 层的一个节点 2305 中可设定类别[记忆棒(商标)]，与这个节点之下关联的节点、叶是作为包含使用了记忆棒的各种各样的装置的类别专用的节点或叶而设定。即，以节点 2305 之下作为被记忆棒的类别定义的装置的关联节点及叶的集合而定义。

进而，可以将 M 层的数层之下的下位层作为子类别节点 2306 而设定。例如如图中表示的，在类别[记忆棒]节点 2305 的 2 层之下的节点中，作为使用了记忆棒的装置的类别中包含的子类别节点，设定[再生

专用器]的节点。进而，在子类别节点的再生专用器的节点 2306 之下，设定再生专用器的类别中包含的附带音乐再生功能的电话的节点 2307，进而在它的下位，可以设定附带音乐再生功能的电话的类别中包含的[PHS]节点 2308 和[便携式电话]节点 2309。

进而，类别、子类别不仅是装置的种类，例如可以在某制造商、内容提供商、清算机关等独立管理的节点，即处理单位、管辖单位或提供服务单位等任意的单位（以下总称这些为实体）上设定。例如，如果以一个类别节点作为游戏机制造商销售的游戏机 XYZ 的专用顶点节点而设定，则在制造商销售的游戏机 XYZ 中可以存储其顶点节点之下的下层的节点密钥、叶密钥并进行销售，之后，生成通过其顶点节点密钥之下的节点密钥、叶密钥构成加密内容的发布或各种密钥的发布、更新处理的有效密钥块（EKB）并发布，使仅对顶点节点以下的装置发布可利用的数据成为可能。

这样以一个节点作为顶点，通过将之下的节点作为在其顶点节点中被定义的类别或子类别的关联节点而设定的结构，管理类别层或子类别层的一个顶点节点的制造商、内容提供商等，独立生成以其节点为顶点的有效密钥块（EKB），给属于顶点节点以下的装置发布的结构成为可能，完全不会给不属于顶点节点的、属于其他的类别的节点的装置带来影响，而可以实行密钥更新。

这样，随着在类别单位上的 EKB 的密钥更新，在类别单位或特定组上的一揽子的取消，也是可能的，在包含很多的取消·叶或取消·节点的情况下，通过上述的 EKB 跟踪处理的取消判定特别有效。原因是，在给各装置发布了将所有的取消装置的 ID 全都记录了的清单时，会产生清单的存储利用域的问题，同时也加重了花费于 ID 的对照处理的负担。基于上述的 ID 的 EKB 跟踪处理是基于 EKB 内的标记的跟踪处理，其处理负担极小，可立刻实行是否被取消的判定。

在上述这样的 EKB 中，制成了 EKB 发行机关的署名，可检查窜改，通过署名验证可验证是合法的 EKB，实现确实的取消判定。

以上，参照几个的实施示例，对本发明进行了说明，但本发明在不偏离它的要点的范围内，从业者能完成上述的实施示例的修改和代用是当然的。即，上述的实施示例是以称为示例的方式明示了本发明，不应该是限定地被解释。为了判断本发明的要点，应参考权利要求的

记载。

产业上的可利用性

涉及本发明的信息处理装置及方法，使基于利用了内容密钥等的发布所应用的分层密钥发布树的有效密钥块(EKB)，判定作为取消(排除）实体的装置或服务提供商等成为可能，因此没有必要向装置发布存储有取消实体的 ID 的取消清单，各装置存储清单。

而且，涉及本发明的信息处理装置及方法，由于将可识别分层密钥发布树的位置的 ID 存储于公钥证明书，基于从公钥证明书取得的 ID 来实行采用了有效密钥块（EKB）的标记的跟踪处理，所以 ID 的可靠性在公钥证明书中被保证，取消实体（装置）的确切判定成为可能。

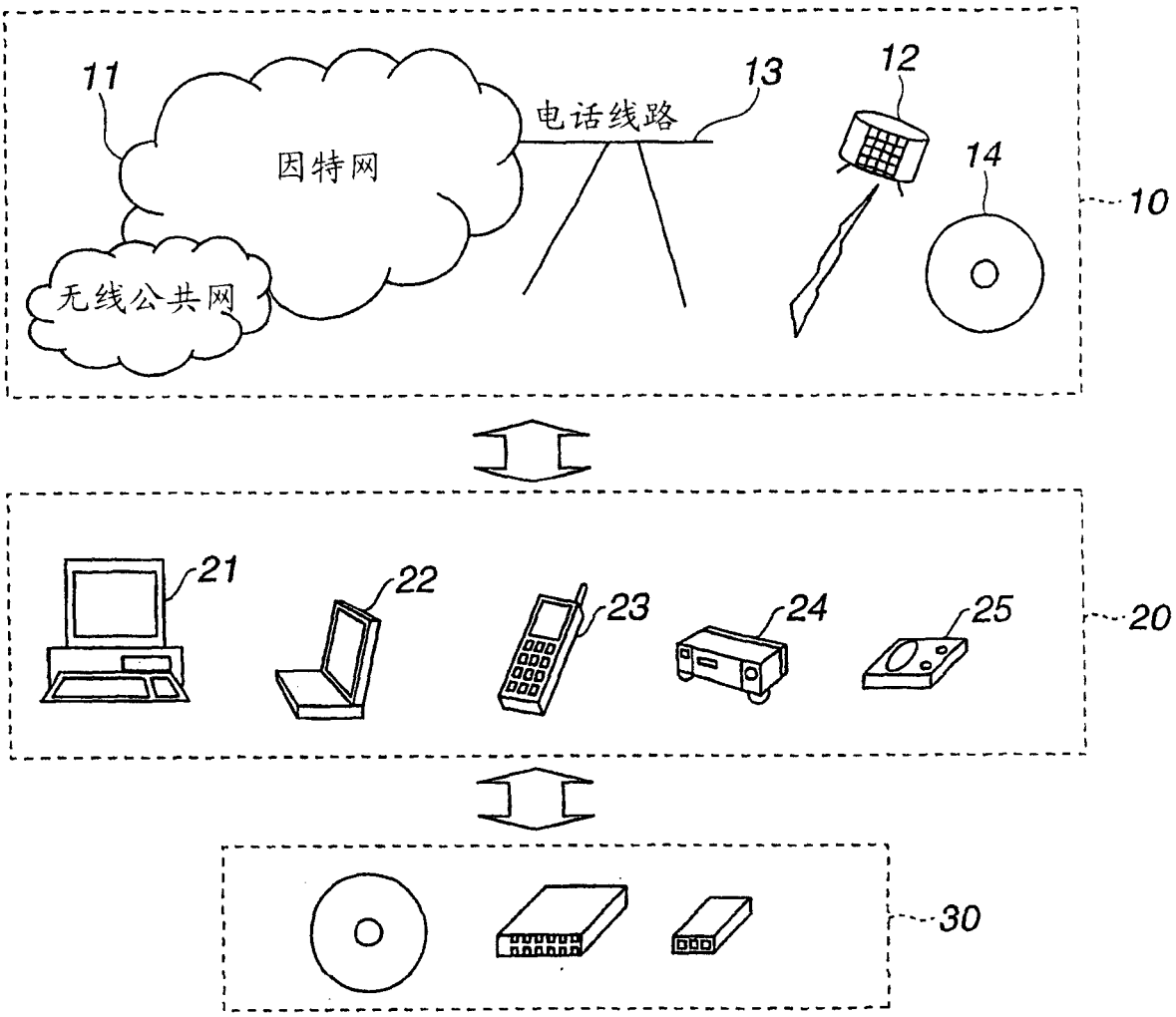


图 1

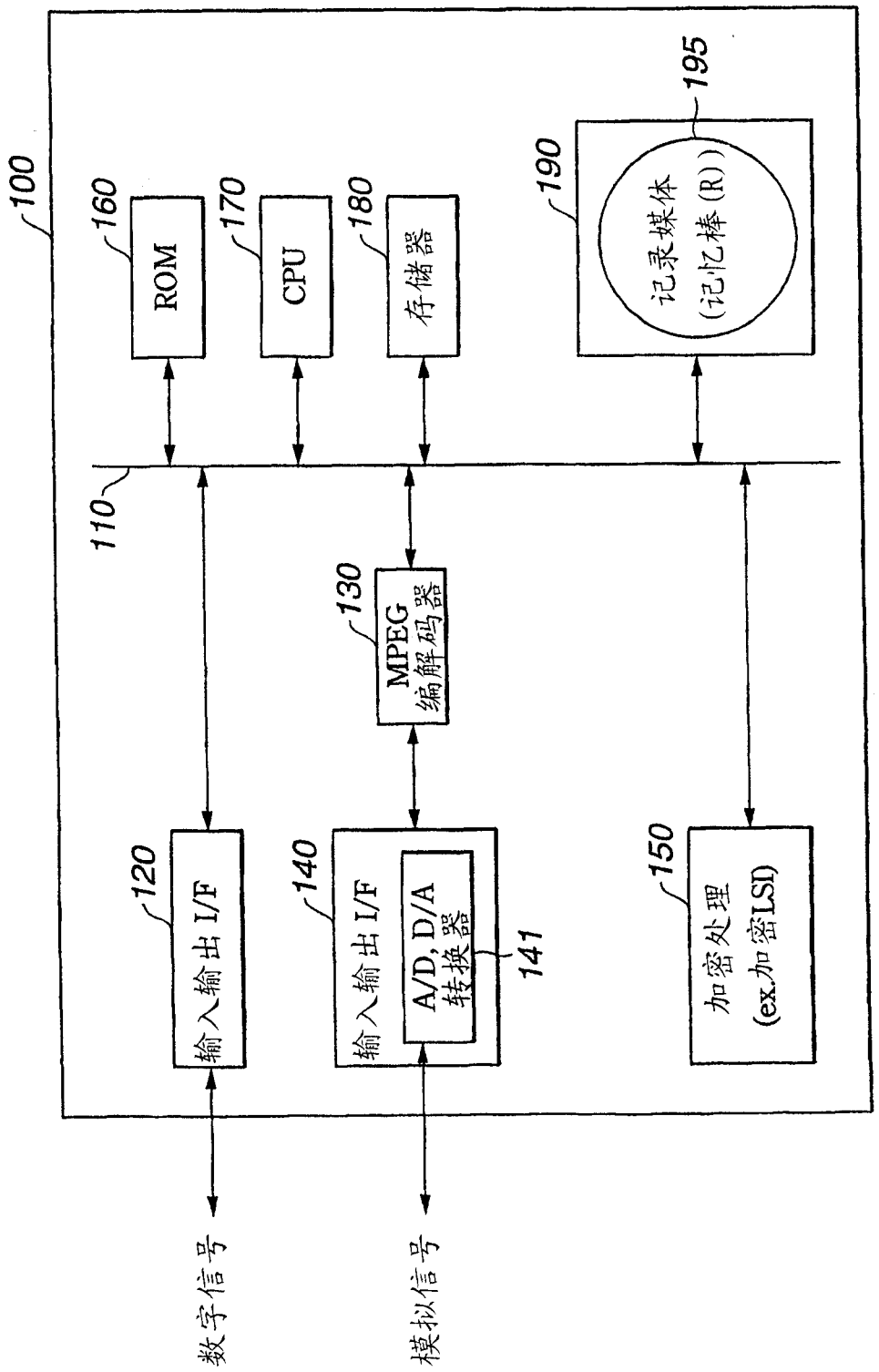

100
160
ROM
170
CPU
180
存储器
190
记录媒体
(记忆棒(R))
195
110
130
MPEG
编解码器
120
输入输出 I/F
140
输入输出 I/F
A/D, D/A
转换器
141
150
加密处理
(ex.加密LSI)
数字信号
模拟信号

图 2

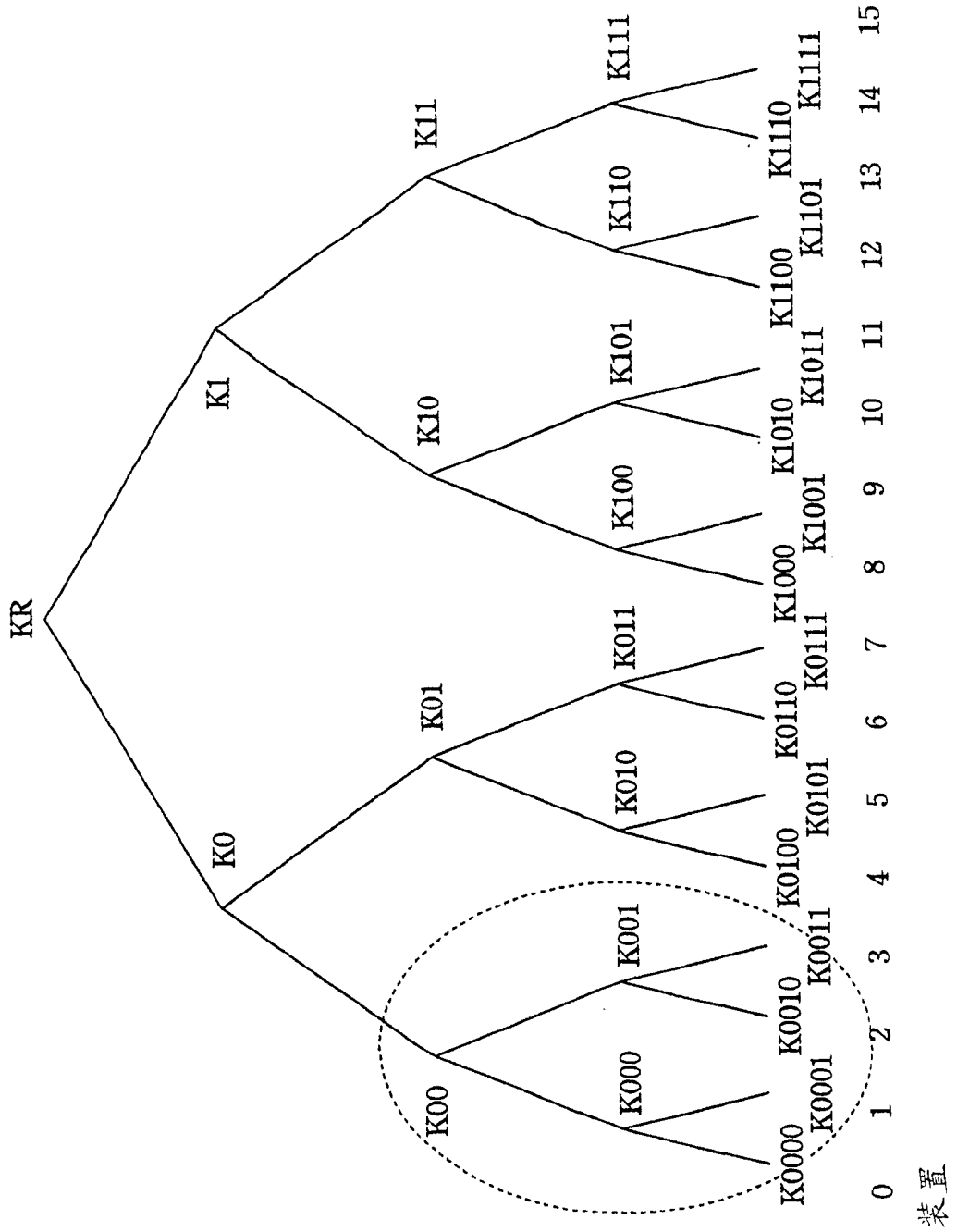

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
装置

图 3

版本 (Version) : t	
索引	加密密钥
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

图 4A

版本 (Version) : t	
索引	加密密钥
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

图 4B

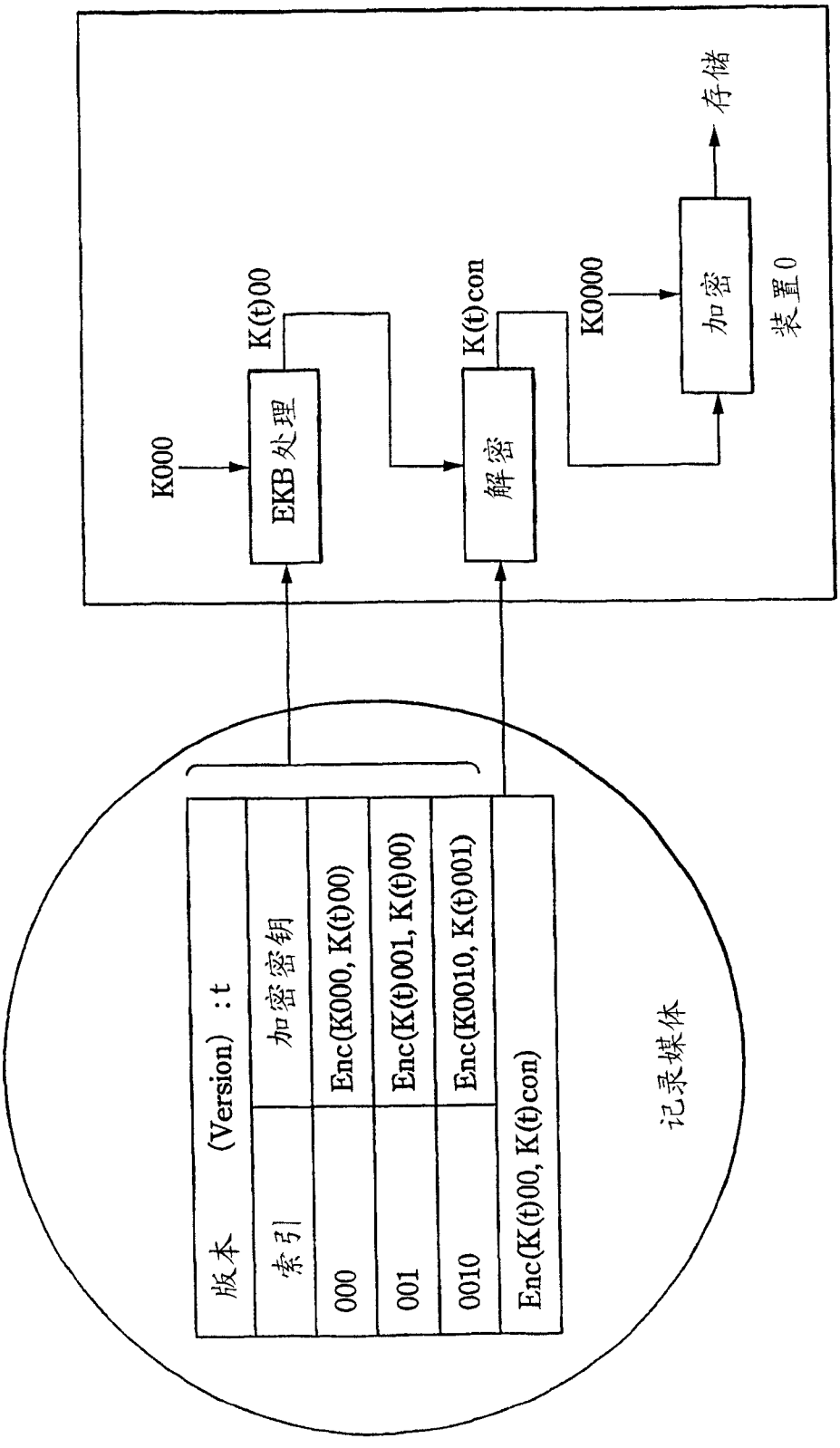

记录媒体
版本 (Version) : t
索引
加密密钥
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
装置0
K000
EKB 处理
K(t)00
解密
K(t)con
K0000
加密
存储

图 5

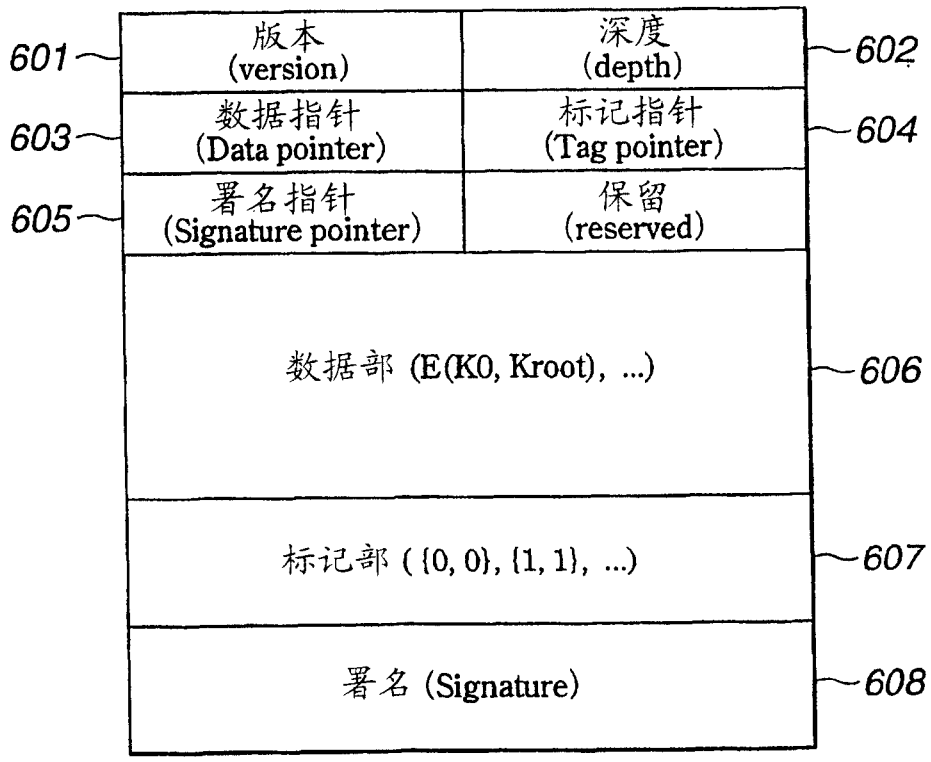

601
版本
(version)
深度
(depth)
602
603
数据指针
(Data pointer)
标记指针
(Tag pointer)
604
605
署名指针
(Signature pointer)
保留
(reserved)
数据部 (E(K0, Kroot), ...)
606
标记部 ({0, 0}, {1, 1}, ...)
607
署名 (Signature)
608

图 6

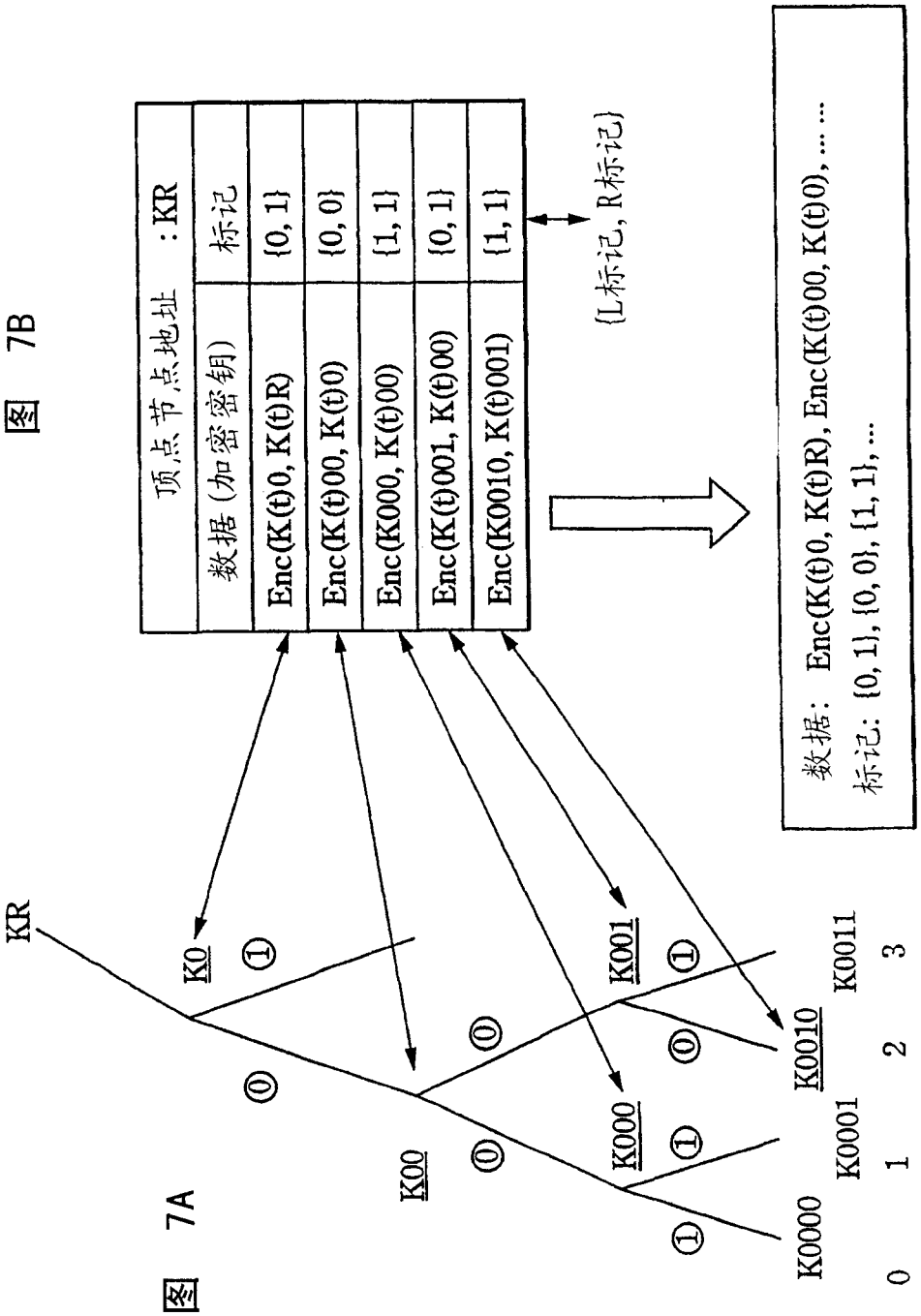


图 7A

顶点节点地址 :KR	
数据（加密密钥）	标记
Enc(K(t)0, K(t)R)	{0, 1}
Enc(K(t)00, K(t)0)	{0, 0}
Enc(K(t)000, K(t)00)	{1, 1}
Enc(K(t)001, K(t)00)	{0, 1}
Enc(K(t)0010, K(t)001)	{1, 1}

{L标记, R标记}

图 7B

数据： Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0),……
标记：{0, 1}, {0, 0}, {1, 1}, ...

图 7C

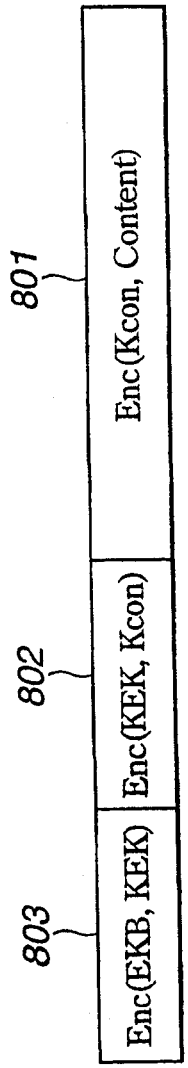

801
Enc(Kcon, Content)
802
Enc(KEK, Kcon)
803
Enc(EKB, KEK)

图 8A

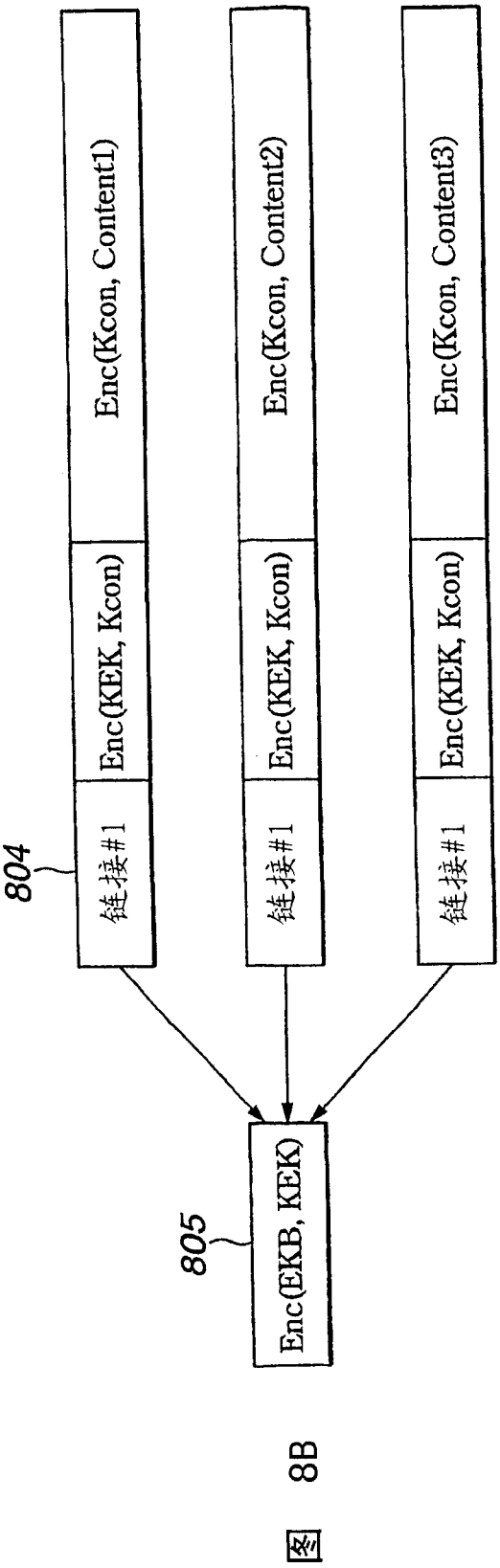

804
链接#1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
链接#1
Enc(KEK, Kcon)
Enc(Kcon, Content2)
链接#1
Enc(KEK, Kcon)
Enc(Kcon, Content3)
805
Enc(EKB, KEK)

图 8B

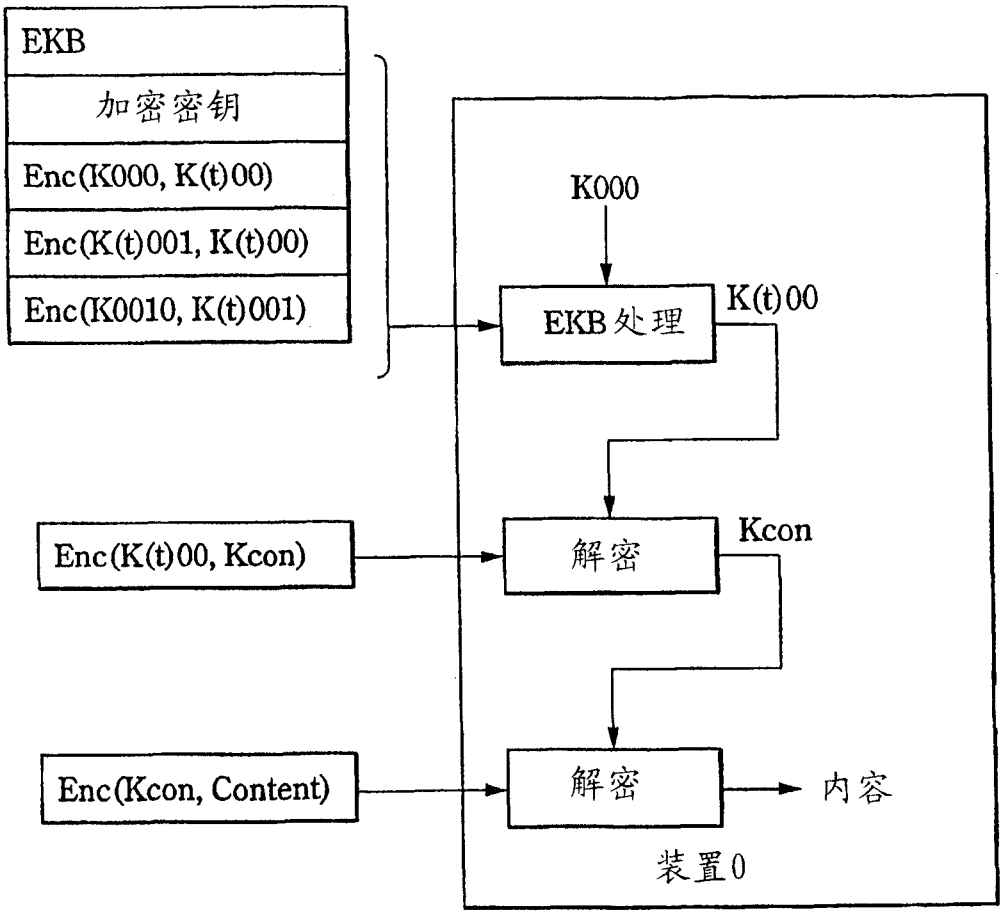

EKB
加密密钥
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K000
EKB处理
K(t)00
Enc(K(t)00, Kcon)
解密
Kcon
Enc(Kcon, Content)
解密
内容
装置0

图 9

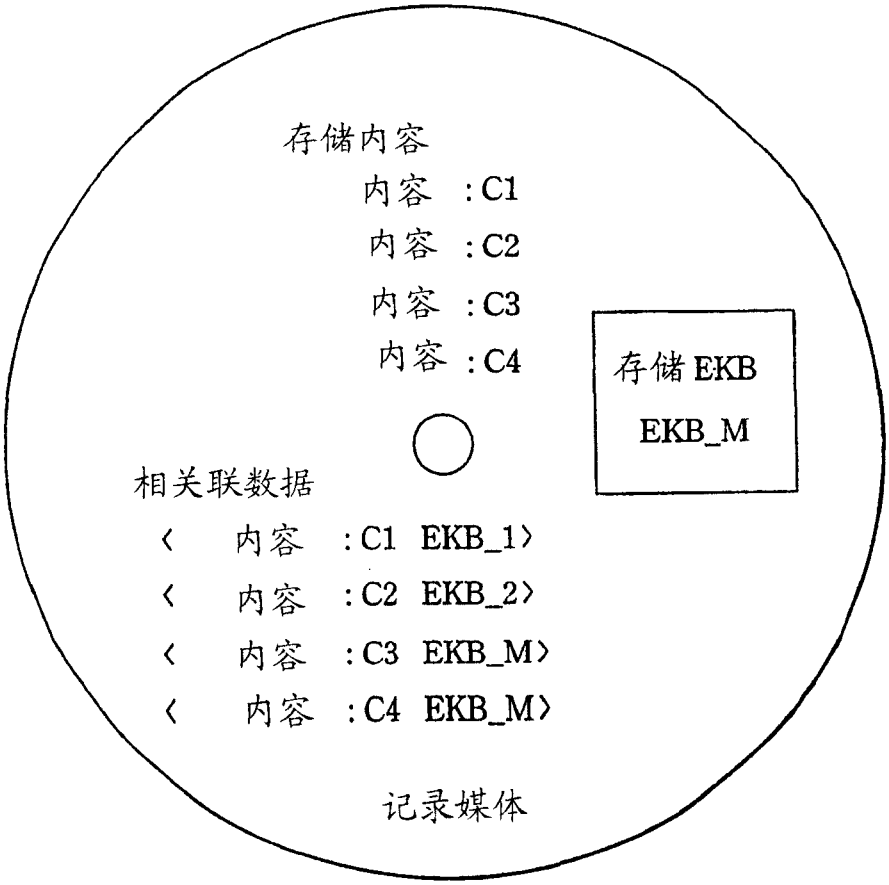

存储内容
内容 :C1
内容 :C2
内容 :C3
内容 :C4
存储 EKB
EKB_M
相关联数据
〈 内容 :C1 EKB_1〉
〈 内容 :C2 EKB_2〉
〈 内容 :C3 EKB_M〉
〈 内容 :C4 EKB_M〉
记录媒体

图 10

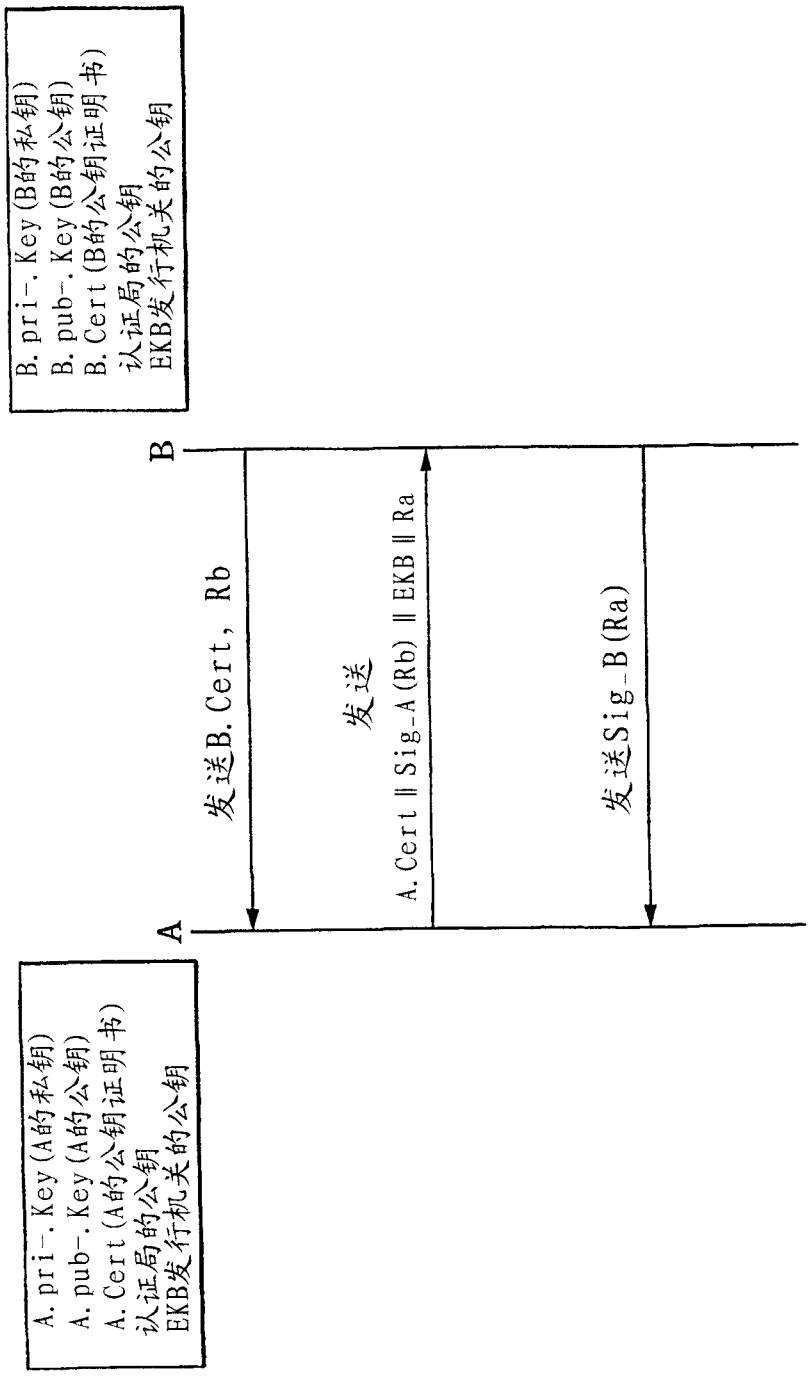

A. pri-. Key(A的私钥)
A. pub-. Key(A的公钥)
A. Cert(A的公钥证明书)
认证局的公钥
EKB发行机关的公钥
B. pri-. Key(B的私钥)
B. pub-. Key(B的公钥)
B. Cert(B的公钥证明书)
认证局的公钥
EKB发行机关的公钥
A
B
发送B. Cert, Rb
发送
A. Cert ‖ Sig_A(Rb) ‖ EKB ‖ Ra
发送Sig_B(Ra)

图 11

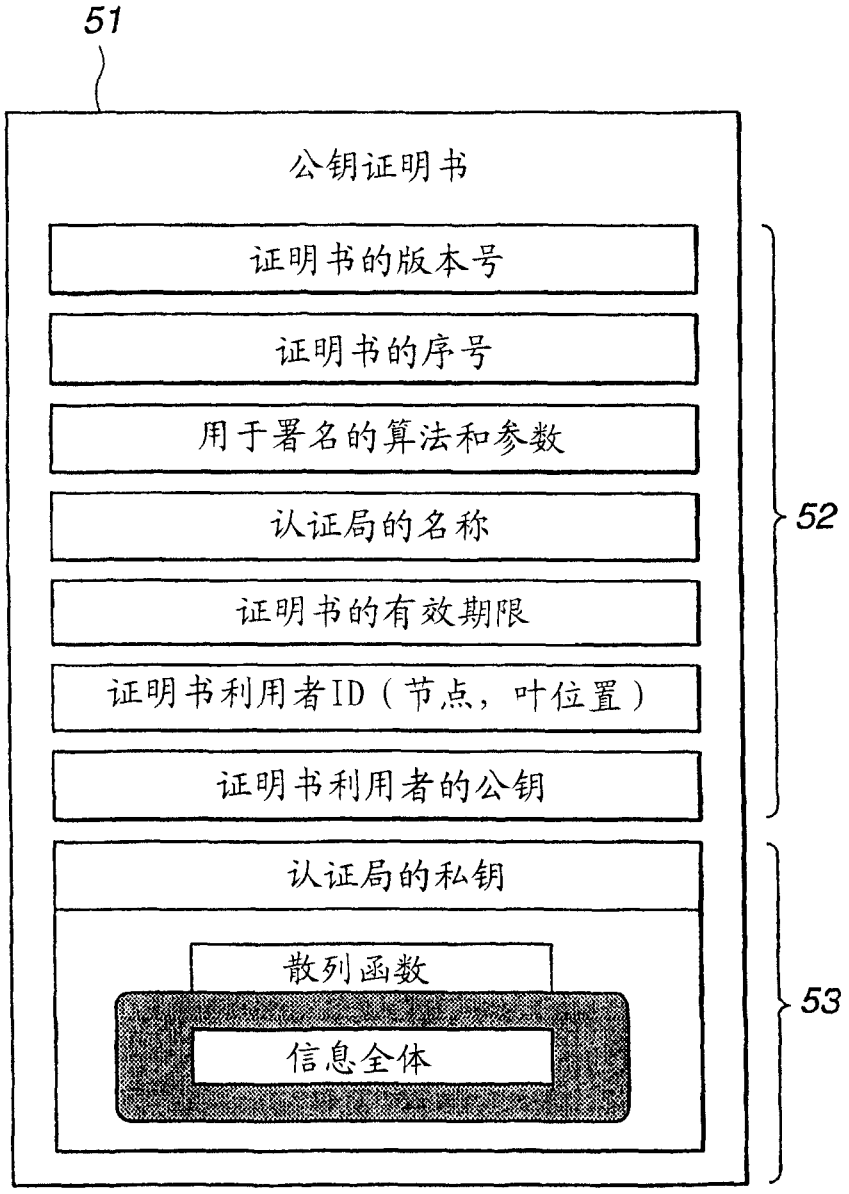

51
公钥证明书
证明书的版本号
证明书的序号
用于署名的算法和参数
认证局的名称
证明书的有效期限
证明书利用者ID（节点，叶位置）
证明书利用者的公钥
52
认证局的私钥
散列函数
信息全体
53

图 12

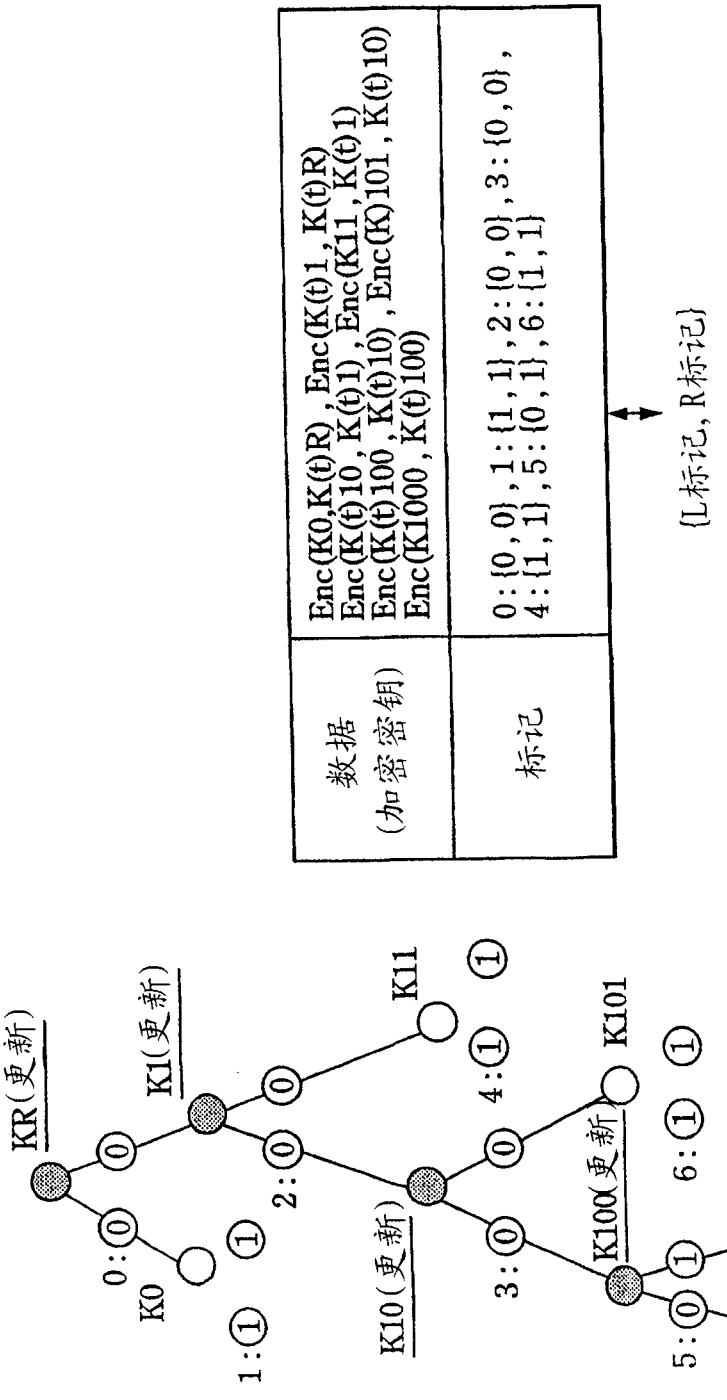


图 13A

数据 (加密密钥)	Enc(K0,K(t)R) , Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1) , Enc(K11, K(t)1) Enc(K(t)100 , K(t)10) , Enc(K)101 , K(t)10) Enc(K1000 , K(t)100)
标记	0:{0,0} , 1:{1,1} , 2:{0,0} , 3:{0,0} , 4:{1,1} , 5:{0,1} , 6:{1,1}

{L标记, R标记}

图 13B

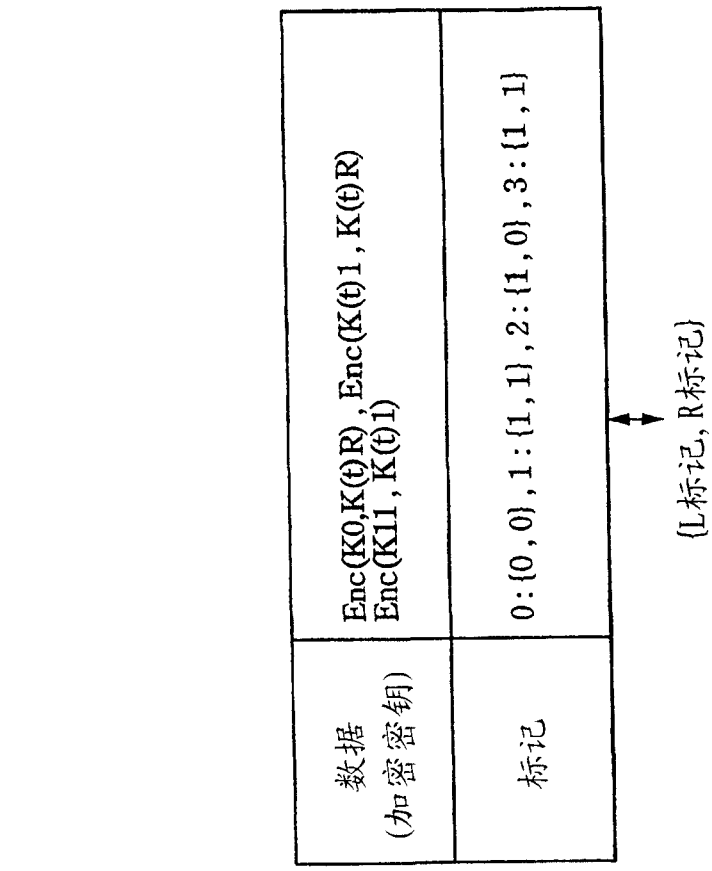


图 14A

数据 （加密密钥）	Enc(K0,K(t)R), Enc(K(t)1, K(t)R) Enc(K11, K(t)1)
标记	0:{0, 0}, 1:{1, 1}, 2:{1, 0}, 3:{1, 1}

{L标记, R标记}

图 14B

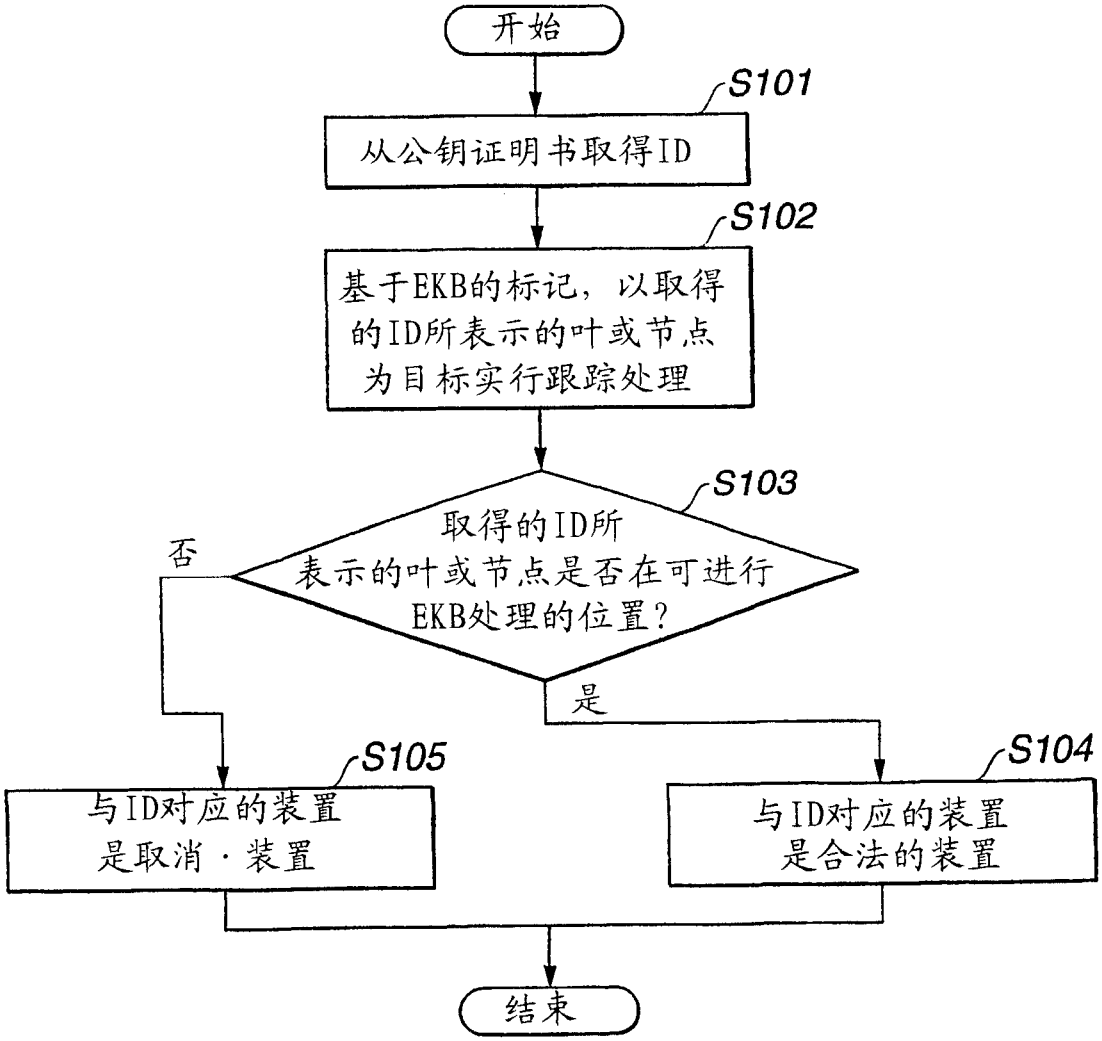

开始
S101
从公钥证明书取得ID
S102
基于EKB的标记，以取得的ID所表示的叶或节点为目标实行跟踪处理
S103
取得的ID所表示的叶或节点是否在可进行EKB处理的位置？
否
是
S105
与ID对应的装置是取消·装置
S104
与ID对应的装置是合法的装置
结束

图 15

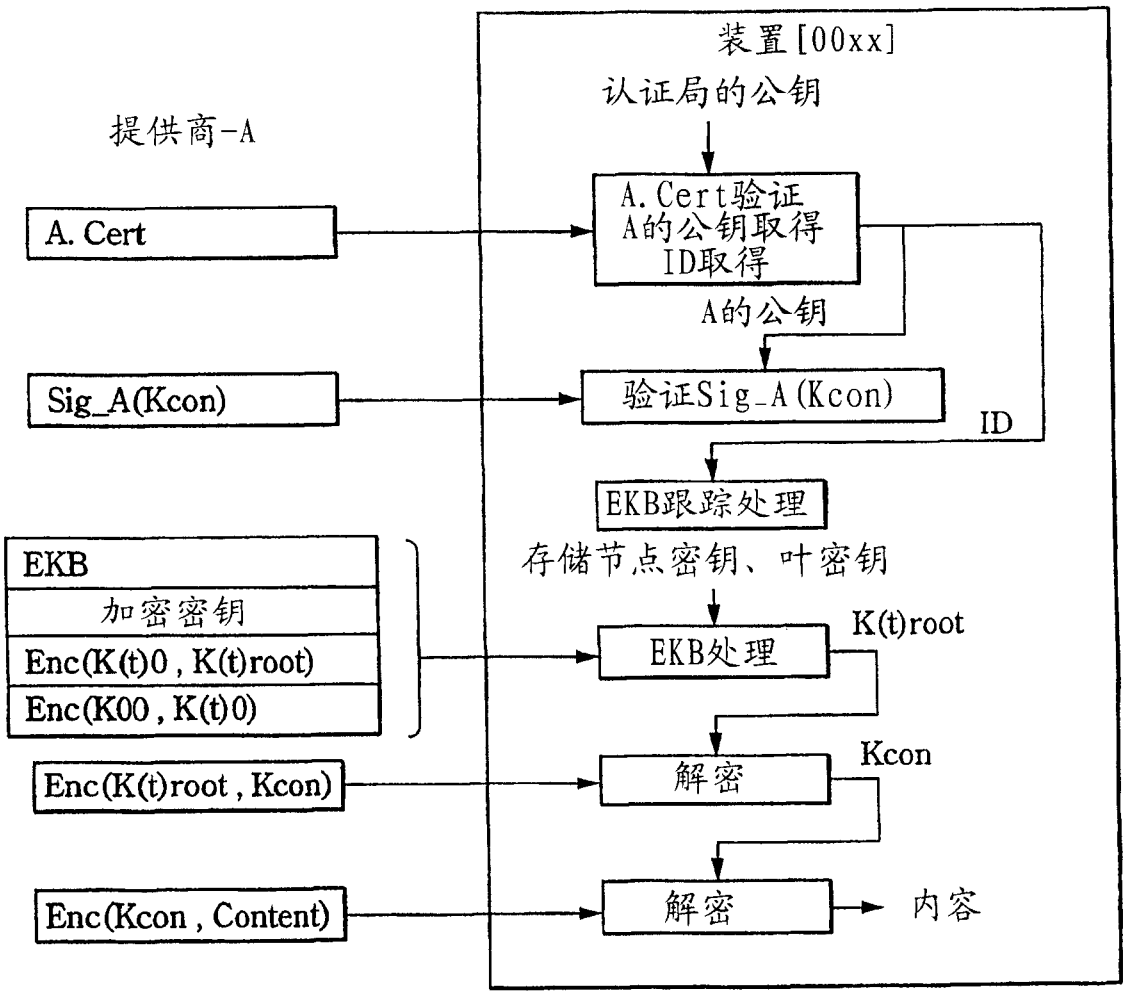

装置[00xx]
认证局的公钥
提供商-A
A. Cert
A. Cert验证
A的公钥取得
ID取得
A的公钥
Sig_A(Kcon)
验证Sig_A(Kcon)
ID
EKB跟踪处理
EKB
加密密钥
Enc(K(t)0 , K(t)root)
Enc(K00 , K(t)0)
存储节点密钥、叶密钥
EKB处理
K(t)root
Enc(K(t)root , Kcon)
解密
Kcon
Enc(Kcon , Content)
解密
内容

图 16

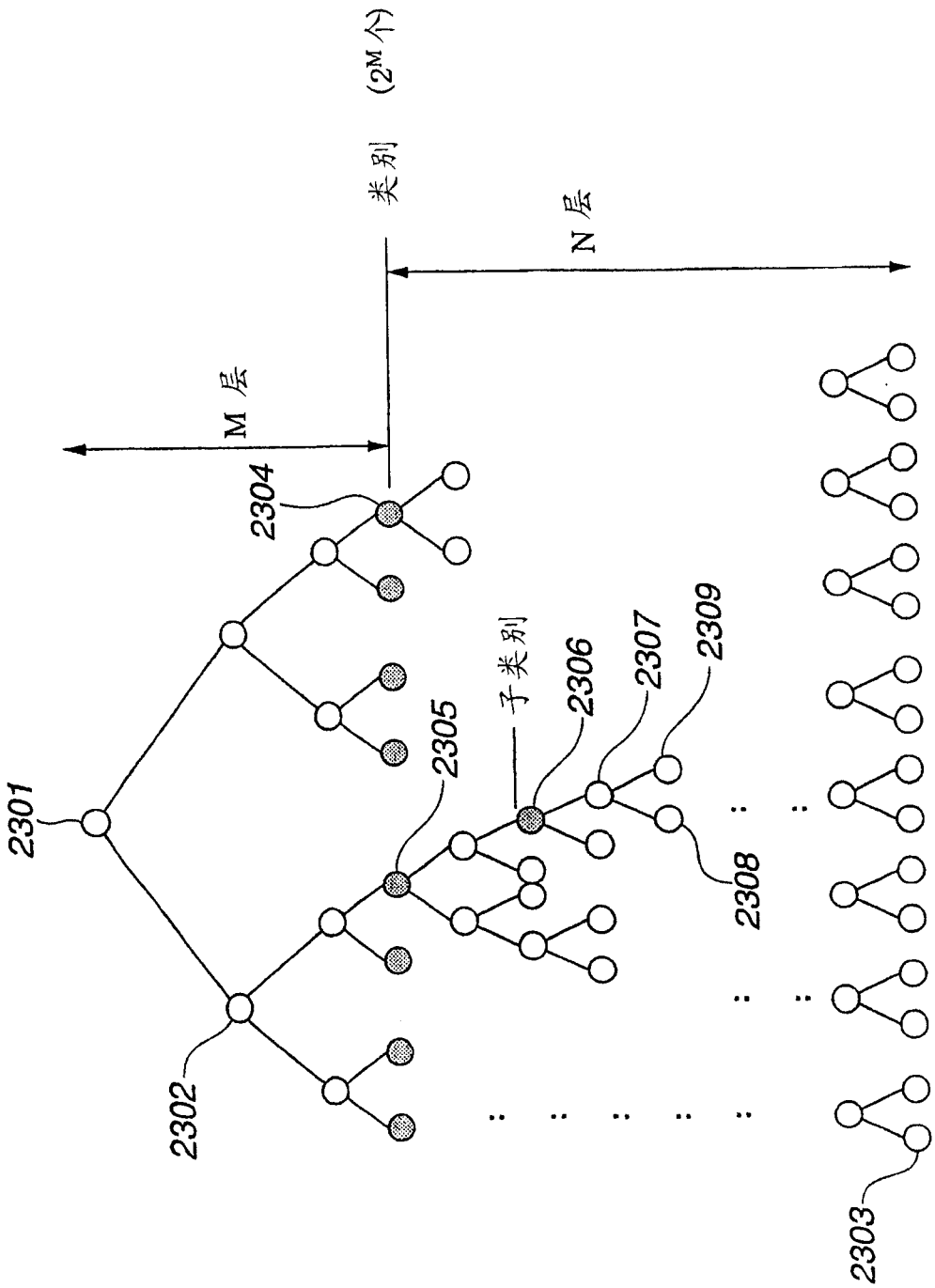


图 17