[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00
G06F 12/14 G06F 15/00
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 01808671.3

[43] 公开日 2003 年 6 月 25 日

[11] 公开号 CN 1426644A

[22] 申请日 2001.12.21 [21] 申请号 01808671.3
[30] 优先权
[32] 2000.12.26 [33] JP [31] 396098/2000
[86] 国际申请 PCT/JP01/11237 2001.12.21
[87] 国际公布 WO02/052781 日 2002.7.4
[85] 进入国家阶段日期 2002.10.25
[71] 申请人 索尼公司
地址 日本东京都
[72] 发明人 浅野智之 大泽义知 大石丈于
石黑隆二 泷隆太

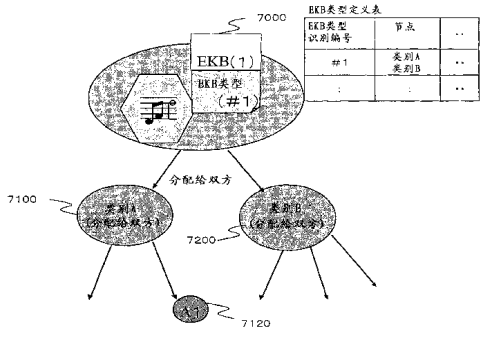
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 刘宗杰 王忠忠

权利要求书 3 页 说明书 68 页 附图 64 页

[54] 发明名称 信息管理系统和方法

[57] 摘要

本发明实现了下述的信息管理系统和方法，该信息管理系统和方法实现了使用有效化密钥块(EKB)的处理中的高效率的处理，上述有效化密钥块(EKB)采用进行了类别区分的树结构。 在生成由具有多个作为根据类别区分的、由类别实体管理的密钥树的选择通路上的低位密钥进行的高位密钥的加密处理数据的 EKB 并将其提供给装置的结构中，作成对 EKB 利用实体进行关于能处理被 EKB 类型定义表定义的 EKB 的类别树中的因排除等引起的状态变化发生的通知的结构，EKB 请求者能常时地进行基于最新的 EKB 的处理。



ISSN1008-4274

1. 一种信息管理系统，其中，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述信息管理系统具有对装置提供有效化密钥块（EKB）的结构，上述有效化密钥块（EKB）选择构成该密钥树的通路并具有由选择通路上的低位密钥产生的高位密钥的加密处理数据，上述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于:

上述密钥树是具有多个作为根据类别区分的、由类别实体管理的子树的类别树的结构，

上述信息管理系统具有生成并发行能在类别树中共同地进行解密处理的 EKB 的密钥发行中心（KDC），

上述密钥发行中心（KDC）具有使 EKB 类型识别符与能进行 EKB 处理的类别树的识别数据相对应的 EKB 类型定义表，

上述密钥发行中心（KDC）具有对于至少作为能处理状态变化发生的类别树而设定的 EKB 的利用实体进行关于能处理被上述 EKB 类型定义表定义的 EKB 的类别树中的上述状态变化发生的通知处理的结构。

2. 如权利要求 1 中所述的信息管理系统，其特征在于:

上述类别树中的状态变化是伴随该类别树中的排除（装置排除）的发生的状态变化。

3. 如权利要求 1 中所述的信息管理系统，其特征在于:

上述类别树中的状态变化是伴随属于该类别树的装置的装置存储密钥的变更的状态变化。

4. 如权利要求 1 中所述的信息管理系统，其特征在于:

上述 EKB 的利用实体包含作为对于上述密钥发行中心(KDC)的 EKB 生成要求实体的 EKB 请求者。

5. 如权利要求 1 中所述的信息管理系统，其特征在于:

上述 EKB 的利用实体包含作为能处理在上述 EKB 类型定义表中被定义的 EKB 的类别树的管理实体的类别实体。

6. 如权利要求 1 中所述的信息管理系统，其特征在于:

上述密钥发行中心（KDC）对于全部作为对于上述 EKB 类型定义

表的利用实体、即上述密钥发行中心(KDC)的EKB生成要求实体的EKB请求者和作为类别树的管理实体的类别实体进行关于上述状态变化的发生的通知处理。

7. 如权利要求1中所述的信息管理系统，其特征在于:

上述密钥发行中心（KDC）具有从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息并根据来自该类别实体的状态变化发生信息来进行关于状态变化发生的通知处理的结构。

8. 一种信息处理方法，该信息处理方法是下述的系统中的信息处理方法，该系统具有多个作为根据类别区分的、由类别实体管理的子树的类别树，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述系统具有对装置提供有效化密钥块（EKB）的结构，上述有效化密钥块（EKB）选择构成该密钥树的通路并具有由选择通路上的低位密钥进行的高位密钥的加密处理数据，上述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于:

生成并发行能在类别树中共同地进行解密处理的EKB的密钥发行中心（KDC）对于至少作为能处理状态变化发生的类别树而设定的EKB的利用实体进行关于能处理被使EKB类型识别符与能进行EKB处理的类别树的识别数据相对应的EKB类型定义表定义的EKB的类别树中的上述状态变化发生的通知处理。

9. 如权利要求8中所述的信息处理方法，其特征在于:

上述类别树中的状态变化是伴随该类别树中的排除（装置排除）的发生的状态变化。

10. 如权利要求8中所述的信息处理方法，其特征在于:

上述类别树中的状态变化是伴随属于该类别树的装置的装置存储密钥的变更的状态变化。

11. 如权利要求8中所述的信息处理方法，其特征在于:

上述EKB的利用实体包含作为对于上述密钥发行中心(KDC)的EKB生成要求实体的EKB请求者。

12. 如权利要求8中所述的信息处理方法，其特征在于:

上述EKB的利用实体包含作为能处理在上述EKB类型定义表中被定义的EKB的类别树的管理实体的类别实体。

13. 如权利要求 8 中所述的信息处理方法，其特征在于:

上述密钥发行中心（KDC）对于作为对于上述 EKB 类型定义表的利用实体、即上述密钥发行中心（KDC）的 EKB 生成要求实体的 EKB 请求者和作为类别树的管理实体的全部类别实体进行关于上述状态变化的发生的通知处理。

14. 如权利要求 8 中所述的信息处理方法，其特征在于:

上述密钥发行中心（KDC）具有从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息并根据来自该类别实体的状态变化发生信息来进行关于状态变化发生的通知处理的结构。

15. 一种程序记录媒体，该程序记录媒体是记录了在计算机系统上进行下述的系统中的信息处理的计算机程序的程序记录媒体，该系统具有多个作为根据类别区分的、由类别实体管理的子树的类别树，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述系统具有对装置提供有效化密钥块（EKB）的结构，上述有效化密钥块（EKB）选择构成该密钥树的通路并具有由选择通路上的低位密钥进行的高位密钥的加密处理数据，上述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于:

上述计算机程序具有:

从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息的步骤；以及

根据来自该类别实体的状态变化发生信息的接收、对于至少作为能处理状态变化发生的类别树而设定的 EKB 的利用实体进行关于状态变化发生的通知处理的步骤。

信息管理系统和方法

技术领域

本发明涉及信息管理系统和信息处理方法以及程序记录媒体，特别是涉及伴随对正当的用户提供内容（content）和各种数据的加密处理的信息分配系统和方法。特别是涉及使用树结构的分级的密钥信息分配方式、使用根据信息分配装置生成的密钥块、例如能进行作为内容的加密密钥的内容密钥信息分配或保持其它各种安全性的信息管理系统和信息处理方法以及程序记录媒体。

背景技术

迄今为止，经互联网等的网络或 DVD、CD 等的可流通的记录媒体来分配游戏程序、声音数据、图像数据等各种各样软件数据（以下，将其称为内容（content））的做法越来越盛行。这些流通内容由用户所有的 PC（个人计算机）、游戏机进行数据接收或存储媒体的安装来进行播放，或被存储在附属于 PC 等的记录播放装置内的记录装置、例如存储卡、硬盘等中，利用来自存储媒体的新的播放而加以利用。

在视频游戏机、PC 等的信息装置中，由于从网络来接收流通内容，或在 DVD、CD 等中具有进行存取用的接口，故还具有作为存储区使用的 RAM、ROM 等，用来存储在内容的播放方面所必要的控制手段、程序、数据。

根据来自作为播放装置利用的游戏机、PC 等的信息装置本体的用户指示、或经已连接的输入装置传送的用户的指示，从存储媒体调出音乐数据、图像数据或程序等的各种各样的内容，通过信息装置本体或已被连接的显示器、扬声器等进行播放。

关于游戏机程序、音乐数据、图像数据等多种软件内容，一般来说由其制作者、销售者保有其颁布权。因而，在这些内容的发布时，一般采取下述的结构：即，在一定的利用限制下、即只对正规的用户才许诺软件的使用，不使其进行不许可的复制、即考虑了安全性。

实现对于用户的利用限制的 1 种方法是发布内容的加密处理。即，作成下述的结构：在例如经互联网等发布已被加密的声音数据、图像数据、游戏机程序等各种内容的同时，只对被确认为正规的用户的人

赋予对已被发布的加密内容进行解密的方法、即解密密钥。

利用由规定的手续进行的解密处理，可将加密数据恢复为可利用的解密数据（平文）。迄今为止，大家都知道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、解密的方法的形态中有各种各样的种类，但作为其一例，有被称为共同密钥加密方式的方式。在共同密钥加密方式中，使数据的加密处理中使用的加密密钥和在数据的解密处理中使用解密密钥成为共同的密钥，对正规的用户赋予在这些加密处理、解密处理中使用的共同密钥，排除由不具有密钥的不正当用户进行的数据存取。在该方式的代表性的方式中，有 DES（数据密码标准）方式。

在上述的加密处理、解密处理中使用的加密密钥、解密密钥，例如可根据某个口令并应用杂乱（hash）函数等单一方向性函数来得到。所谓单一方向性函数，指的是从其输出反过来求其输入是非常困难的函数。例如将用户确定的口令作为输入来应用单一方向性函数，根据其输出来生成加密密钥、解密密钥。从这样得到的加密密钥、解密密钥反过来求作为其原来的数据的口令实质上是不可能的。

此外，使在加密时使用的加密密钥的处理与在解密时使用的解密密钥的处理成为不同的算法的方式是被称为所谓的公开密钥加密方式的方式。公开密钥加密方式是使用不特定的用户可使用的公开密钥的方式，使用特定个人发行的公开密钥进行对于该特定个人的加密文书的加密处理。由该公开密钥进行了加密的文书只能由与该加密处理中使用的公开密钥对应的秘密密钥进行解密处理。由于秘密密钥由发行了公开密钥的个人所有，故只能由具有秘密密钥的个人对由该公开密钥进行了加密的文书进行解密。公开密钥加密方式的代表性的方式中有 RSA（Rivest-Shamir-Adleman）密码。通过利用这样的加密方式，可实现只对正规用户来说才能对加密内容进行解密的系统。

在上述的那样的内容分配系统中，大多采用下述的结构：对内容进行加密并存储在网络或 DVD、CD 等的记录媒体中以提供给用户，只对正当的用户提供对加密内容进行解密的内容密钥。为了防止内容密钥本身的不正当的复制等，提出了将内容密钥加密后提供给正当的用

户、使用只有正当的用户具有的解密密钥对加密内容密钥进行解密后才能使用内容密钥的结构。

一般来说，通过例如在作为内容的发送者的内容提供者与用户装置间在内容或内容密钥的分配前进行认证处理，可进行是否是正当的用户的判定。在一般的认证处理中，在进行对方的确认的同时，生成只在该通信中有效的对话密钥，在认证成立了的情况下，使用已生成的对话密钥对数据、例如内容或内容密钥进行加密来进行通信。在认证方式中，有使用了共同密钥加密方式的相互认证和使用了公开密钥方式的认证方式，但在使用共同密钥的认证中，必须有在整个系统中共同的密钥，这在更新处理等时是不方便的。此外，在公开密钥方式中，计算负担增大、此外必要的存储量也变大，在各装置中设置这样的处理方法不能说是所希望的结构。

发明的公开

在本发明中，提出了下述的结构：不依赖于上述那样的数据的发送者、接收者间的相互认证处理，能只对正当的用户安全地发送数据，同时形成以分级密钥分配树为类别单位的子树、即类别树，使用能在多个类别树内应用（解密处理）的加密密钥块。

再者，其目的在于提供下述的信息管理系统和信息处理方法以及程序记录媒体，其中，生成作为能在 1 个以上的已被选择的类别树中进行解密的加密密钥数据块的有效化密钥块（EKB）并在属于各类别树的装置中可共同地使用，同时通过使用表示在哪个类别树中能处理、即能解密的 EKB 类型定义表，可实现 EKB 生成、管理处理的高效率。

再者，其目的在于提供下述的信息管理系统和信息处理方法以及程序记录媒体，其中，通过对 EKB 利用实体进行关于能处理被 EKB 类型定义表定义的 EKB 的类别树中的状态变化发生的通知，能进行基于最新的 EKB 类型定义信息的处理。

本发明的第 1 方面是一种信息管理系统，其中，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述信息管理系统具有对装置提供有效化密钥块（EKB）的结构，上述有效化密钥块（EKB）选择构成该密钥树的通路并具有由选择通路上的低位密钥进行的高位密钥的加密处理数据，上

述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于:

上述密钥树是具有多个作为根据类别区分的、由类别实体管理的子树的类别树的结构，

上述信息管理系统具有生成并发行能在类别树中共同地进行解密处理的 EKB 的密钥发行中心（KDC），

上述密钥发行中心（KDC）具有使 EKB 类型识别符与能进行 EKB 处理的类别树的识别数据相对应的 EKB 类型定义表，

上述密钥发行中心（KDC）具有对于至少作为能处理状态变化发生的类别树而设定的 EKB 的利用实体进行关于能处理被上述 EKB 类型定义表定义的 EKB 的类别树中的上述状态变化发生的通知处理的结构。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述类别树中的状态变化是伴随该类别树中的排除（装置排除）的发生的状态变化。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述类别树中的状态变化是伴随属于该类别树的装置的装置存储密钥的变更的状态变化。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述 EKB 的利用实体包含作为对于上述密钥发行中心（KDC）的 EKB 生成要求实体的 EKB 请求者。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述 EKB 的利用实体包含作为能处理在上述 EKB 类型定义表中被定义的 EKB 的类别树的管理实体的类别实体。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述密钥发行中心（KDC）对于作为对于上述 EKB 类型定义表的利用实体、即上述密钥发行中心（KDC）的 EKB 生成要求实体的 EKB 请求者和作为类别树的管理实体的全部类别实体进行关于上述状态变化的发生的通知处理。

再者，在本发明的信息管理系统的一个实施形态中，其特征在于:上述密钥发行中心（KDC）具有从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息并根据来自该类别实体的状态变

化发生信息来进行关于状态变化发生的通知处理的结构。

再者，本发明的第 2 方面是一种信息处理方法，该信息处理方法是下述的系统中的信息处理方法，该系统具有多个作为根据类别区分的、由类别实体管理的子树的类别树，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述系统具有对装置提供有效化密钥块（EKB）的结构，上述有效化密钥块（EKB）选择构成该密钥树的通路并具有由选择通路上的低位密钥进行的高位密钥的加密处理数据，上述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于：生成并发行能在类别树中共同地进行解密处理的 EKB 的密钥发行中心（KDC）对于至少作为能处理状态变化发生的类别树而设定的 EKB 的利用实体进行关于能处理被使 EKB 类型识别符与能进行 EKB 处理的类别树的识别数据相对应的 EKB 类型定义表定义的 EKB 的类别树中的上述状态变化发生的通知处理。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：上述类别树中的状态变化是伴随该类别树中的排除（装置排除）的发生的状态变化。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：上述类别树中的状态变化是伴随属于该类别树的装置的装置存储密钥的变更的状态变化。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：上述 EKB 的利用实体包含作为对于上述密钥发行中心（KDC）的 EKB 生成要求实体的 EKB 请求者。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：上述 EKB 的利用实体包含作为能处理在上述 EKB 类型定义表中被定义的 EKB 的类别树的管理实体的类别实体。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：上述密钥发行中心（KDC）对于全部作为对于上述 EKB 类型定义表的利用实体、即上述密钥发行中心（KDC）的 EKB 生成要求实体的 EKB 请求者和作为类别树的管理实体的类别实体进行关于上述状态变化的发生的通知处理。

再者，在本发明的信息处理方法的一个实施形态中，其特征在于：

上述密钥发行中心（KDC）具有从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息并根据来自该类别实体的状态变化发生信息来进行关于状态变化发生的通知处理的结构。

再者，本发明的第 3 方面是一种程序记录媒体，该程序记录媒体是记录了在计算机系统上进行下述的系统中的信息处理的计算机程序的程序记录媒体，该系统具有多个作为根据类别区分的、由类别实体管理的子树的类别树，构成使密钥分别与将多个装置作为叶构成的树的从根到叶为止的通路上的根、节点和叶相对应的密钥树，上述系统具有对装置提供有效化密钥块(EKB)的结构，上述有效化密钥块(EKB)选择构成该密钥树的通路并具有由选择通路上的低位密钥进行的高位密钥的加密处理数据，上述有效化密钥块（EKB）使得只在能利用与上述选择通路对应的节点密钥组的装置中才能解密，其特征在于：上述计算机程序具有：从作为该类别树的管理实体的类别实体接收类别树中的状态变化发生信息的步骤；以及根据来自该类别实体的状态变化发生信息的接收、对于至少作为能处理状态变化发生的类别树而设定的 EKB 的利用实体进行关于状态变化发生的通知处理的步骤。

在本发明的结构中，作成下述的结构：使用树结构的分级结构的加密密钥分配结构，使用在使各装置 n 分支的各叶上配置的结构的密钥分配方法，经记录媒体或通信线路与有效化密钥块一起分配例如作为内容数据的加密密钥的内容密钥或认证处理中使用的认证密钥或程序代码等。

再者，利用加密密钥数据部和表示加密密钥的位置的标志部来构成有效化密钥块，可减少数据量，可准备且迅速地进行装置中的解密处理。利用本结构，能只对正当的装置安全地分配能解密的数据。

再者，通过生成作为能在 1 个以上的已被选择的类别树中进行解密的加密密钥数据块的有效化密钥块（EKB）并在属于各类别树的装置中可共同地使用，同时通过使用表示在哪个类别树中能处理、即能解密的 EKB 类型定义表，可实现 EKB 生成、管理处理的高效率。

再有，本发明的程序记录媒体例如是对于能实现各种各样的程序代码的通用的计算机系统以计算机可读的形式提供的媒体。媒体是 CD 或 FD、MO 等的记录媒体或网络等的传送媒体等，其形态不作特别限定。

这样的程序记录媒体中定义了在计算机系统上实现规定的计算机程序的功能用的计算机程序与记录媒体的结构上或功能上的协同的关系。换言之，通过经该记录媒体将计算机程序安装在计算机系统上，可在计算机系统上发挥协同的作用，可得到与本发明的另一方面同样的作用和效果。

再有，所谓本发明的说明中的系统，指的是多个装置的逻辑的集合结构，各结构的装置不限于处于同一框体内。

通过基于后述的本发明的实施例或附加的附图的更详细的说明，可了解本发明的另外的目的、特征或优点。

附图的简单的说明

图 1 是说明本发明的信息管理系统的结构例的图。

图 2 是示出可应用在本发明的信息管理系统中的记录播放装置的结构例的框图。

图 3 是说明本发明的信息管理系统中的各种密钥、数据的加密处理的树结构图。

图 4 是示出本发明的信息管理系统中的各种密钥、数据的发布中使用的有效化密钥块（EKB）的例子的图。

图 5 是示出使用了本发明的信息管理系统中的内容密钥的有效化密钥块（EKB）的发布例和解密处理例的图。

图 6 是示出本发明的信息管理系统中的有效化密钥块（EKB）的格式例的图。

图 7 是说明本发明的信息管理系统中的有效化密钥块（EKB）的标志的结构的图。

图 8 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、内容密钥和内容的数据结构例的图。

图 9 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、内容密钥和内容时的装置中的处理例的图。

图 10 是说明在存储媒体中存储了本发明的信息管理系统中的有效化密钥块（EKB）和内容时的对应关系的图。

图 11 是将发送本发明的信息管理系统中的有效化密钥块（EKB）和内容密钥的处理与现有的发送处理进行比较的图。

图 12 是示出本发明的信息管理系统中可应用的共同密钥加密方

式的认证处理顺序的图。

图 13 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、认证密钥的数据结构和在装置中的处理例的图（其 1）。

图 14 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、认证密钥的数据结构和在装置中的处理例的图（其 2）。

图 15 是示出本发明的信息管理系统中可应用的公开密钥加密方式的认证处理顺序的图。

图 16 是示出在本发明的信息管理系统中使用公开密钥加密方式的认证处理同时分配有效化密钥块（EKB）、内容密钥的处理的图。

图 17 是示出在本发明的信息管理系统中同时分配有效化密钥块（EKB）、加密程序数据的处理的图。

图 18 是示出本发明的信息管理系统中可应用的内容完整性检验值（ICV）的生成中使用的 MAC 值生成例的图。

图 19 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、ICV 生成密钥的数据结构和在装置中的处理例的图（其 1）。

图 20 是示出同时分配本发明的信息管理系统中的有效化密钥块（EKB）、ICV 生成密钥的数据结构和在装置中的处理例的图（其 2）。

图 21 是说明在媒体中存储了本发明的信息管理系统中可应用的内容完整性检验值（ICV）时的防止复制功能的图。

图 22 是说明与内容存储媒体分开地管理本发明的信息管理系统中可应用的内容完整性检验值（ICV）的结构的图。

图 23 是说明本发明的信息管理系统中的分级树结构的类别分类的例子的图。

图 24 是说明本发明的信息管理系统中的简化有效化密钥块（EKB）的生成过程的图。

图 25 是说明本发明的信息管理系统中的简化有效化密钥块（EKB）的生成过程的图。

图 26 是说明本发明的信息管理系统中的简化有效化密钥块（EKB）（例 1）的图。

图 27 是说明本发明的信息管理系统中的简化有效化密钥块（EKB）（例 2）的图。

图 28 是说明本发明的信息管理系统中的分级树结构的类别树管

理结构的图。

图 29 是说明本发明的信息管理系统中的分级树结构的类别树管理结构的细节的图。

图 30 是说明本发明的信息管理系统中的分级树结构的类别树管理结构的图。

图 31 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的排除节点的图。

图 32 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的新的类别树登录处理顺序的图。

图 33 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的新的类别树与高位类别树的关系的图。

图 34 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中使用的子 EKB 的图。

图 35 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的装置排除处理的图。

图 36 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的装置排除处理顺序的图。

图 37 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的装置排除时的更新子 EKB 的图。

图 38 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的类别树排除处理的图。

图 39 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的类别树排除处理顺序的图。

图 40 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的排除类别树与高位类别树的关系的图。

图 41 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的性能设定的图。

图 42 是说明本发明的信息管理系统中的分级树结构的类别树管理结构中的性能设定的图。

图 43 是说明本发明的信息管理系统中的有效化密钥块（EKB）所管理的性能管理表结构的图。

图 44 是基于本发明的信息管理系统中的有效化密钥块（EKB）所

管理的性能管理表的 EKB 生成处理流程图。

图 45 是说明本发明的信息管理系统中新的类别树登录时的性能通知处理的图。

图 46 是说明本发明的信息管理系统中的类别树的结构的图。

图 47 是说明本发明的信息管理系统中的 EKB 请求者、密钥发行中心与顶级类别实体（TLCE）的关系、处理例的图。

图 48 是说明本发明的信息管理系统中的 EKB 请求者、密钥发行中心与顶级类别实体（TLCE）的硬件例的图。

图 49 是说明本发明的信息管理系统中的装置所保有的装置节点密钥（DNK）的图。

图 50 是说明本发明的信息管理系统中 EKB 类型定义表的数据结构的图。

图 51 是示出本发明的信息管理系统中 EKB 类型登录处理流程的图。

图 51 是示出本发明的信息管理系统中 EKB 类型登录处理流程的图。

图 52 是示出本发明的信息管理系统中 EKB 类型无效化处理流程的图。

图 53 是示出本发明的信息管理系统中树变更通知处理流程的图。

图 54 是示出本发明的信息管理系统中 EKB 类型表要求处理流程的图。

图 55 是说明本发明的信息管理系统中的子 EKB 的生成处理的图。

图 56 是说明本发明的信息管理系统中的子 EKB 的生成处理的图。

图 57 是说明从本发明的信息管理系统中的子 EKB 生成合成的 EKB 的处理的图。

图 58 是说明存在本发明的信息管理系统中的排除装置时的子 EKB 的生成处理的图。

图 59 是说明从存在本发明的信息管理系统中的排除装置时的子 EKB 生成合成的 EKB 的处理的图。

图 60 是说明从本发明的信息管理系统中的子 EKB 合成的 EKB 的数据结构的图。

图 61 是说明从本发明的信息管理系统中的子 EKB 合成的 EKB 的

数据结构的图。

图 62 是说明从存在本发明的信息管理系统中的排除装置时的子 EKB 合成的 EKB 的数据结构的图。

图 63 是说明本发明的信息管理系统中的数据分配型的系统中的排除处理的图。

图 64 是说明本发明的信息管理系统中的自己记录型的系统中的排除处理的图。

用于实施发明的最佳形态

〔系统概要〕

图 1 中示出本发明的信息管理系统可应用的内容分配系统例。内容的分配一侧 10 将内容或内容密钥加密后发送给内容接收侧 20 所具有的各种各样的可播放内容的装置。在内容分配侧 10 中的装置中，对已接收的加密内容或加密内容密钥进行解密以取得内容或内容密钥，进行图像数据、声音数据的播放或各种程序的执行等。内容分配侧 10 与内容接收侧 20 之间的数据交换经互联网等的网络或经 DVD、CD 等的可流通的记录媒体来进行。

作为内容分配侧 10 的数据分配装置，有互联网 11、卫星广播 12、电话线路 13、DVD、CD 等的媒体 14 等，另一方面，作为内容接收侧 20 的装置，有个人计算机（PC）21、携带装置（PD）22、携带电话、PDA（个人数字助理）等的携带装置 23、DVD、CD 播放器等的记录播放器 24、游戏机终端等的播放专用器 25 等。这些内容接收侧 20 的各装置从网络等的通信装置或媒体 30 取得由内容分配侧 10 提供的内容。

〔装置结构〕

在图 2 中示出记录播放装置 100 的结构框图，作为图 1 中示出的内容接收侧 20 的装置的一例。记录播放装置 100 具有：输入输出 I/F（接口）120；MPEG（运动图像专家组）编码、解码电路组合 130；具备 A/D、D/A 变换器 141 的输入输出 I/F（接口）140；密码处理装置 150；ROM（只读存储器）160；CPU（中央处理单元）170；存储区 180；以及记录媒体 195 的驱动器 190，由总线 110 互相连接这些部分。

输入输出 I/F120 接收构成从外部供给的图像、声音、程序等各种内容的数字信号，在输出给总线 110 的同时，接收总线 110 上的数字信号，输出给外部。MPEG 编码、解码电路组合 130 对经总线 110 供

给的以 MPEG 方式进行了编码的数据以 MPEG 方式进行译码，在输出给输入输出 I/F140 的同时，对从 I/F140 供给的数字信号以 MPEG 方式进行编码，输出给总线 110。输入输出 I/F140 内置了 A/D、D/A 变换器 141。输入输出 I/F140 接收从外部供给的作为内容的模拟信号，通过用 A/D、D/A 变换器 141 进行 A/D（模数）变换，在作为数字信号输出给 MPEG 编码、解码电路组合 130 的同时，通过用 A/D、D/A 变换器 141 对来自 MPEG 编码、解码电路组合 130 的数字信号进行 D/A（数模）变换，作为模拟信号输出给外部。

密码处理装置 150 例如由 1 个芯片的 LSI（大规模集成电路）构成，进行作为经总线 110 供给的内容的数字信号的加密、解密处理或认证处理，具有对总线 110 输出加密数据、解密数据等的结构。再有，密码处理装置 150 不限于 1 个芯片的 LSI，也可利用组合了各种软件或硬件的结构来实现。在后面说明作为软件结构的处理装置的结构。

ROM160 存储由记录播放装置处理的程序数据。CPU170 通过执行在 ROM160、存储区 180 中存储的程序，来控制 MPEG 编码、解码电路组合 130 或密码处理装置 150。存储区 180 例如用非易失性存储器来存储 CPU170 执行的程序或 CPU170 的工作方面必要的数据、进而是由装置执行的密码处理中使用的密钥组。在后面说明密钥组。驱动器 190 通过驱动能记录播放数字数据的记录媒体 195，从记录媒体 195 读出数字数据（播放），在输出给总线 110 的同时，对记录媒体 195 供给经总线 110 供给的数字数据并使其记录。

记录媒体 195 例如是 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存储数字数据的媒体，在本实施形态中，假定是对驱动器 190 来说可装卸的结构。但是，也可作成将记录媒体 195 内置于记录播放装置 100 中的结构。

再有，图 2 中示出的密码处理装置 150 可作为 1 个单片 LSI 来构成，此外，也可作成由组合了软件、硬件的结构来实现的结构。

〔关于作为密钥分配结构的树结构〕

其次，说明从图 1 中示出的内容分配侧 10 对内容接收侧 20 的各装置分配解密数据时的各装置中的密码处理密钥的保有结构和数据分配结构。

图 3 的最下面示出的编号 0～15 是内容接收侧 20 的各个装置。

即，图 3 中示出的分级树结构的各叶（leaf）相当于各个装置。

关于各装置 0～15，在制造时或出厂时或在其后，在存储器中存储对图 3 中示出的分级树结构中的从自身的叶到根为止的节点分配的密钥（节点密钥）和各叶的叶密钥。在图 3 的最下面示出的 K0000～K1111 是分别对各装置 0～15 分配的叶密钥，将从最下面的 KR（根密钥）到从最下面算起的第 2 个节点上记载的密钥：KR～K111 定为节点密钥。

在图 3 中示出的结构中，例如装置 0 具有叶密钥 K0000 和节点密钥：K000、K00、K0、KR。装置 5 具有叶密钥 K0101、K010、K01、K0、KR。装置 15 具有叶密钥 K1111、K111、K11、K1、KR。再有，在图 3 的树中，只记载了 0～15 这 16 个装置，树结构也采取 4 级结构的均衡的左右对称的结构来示出，但可在树中构成更多的装置，此外，在树的各部分中可具有不同的段数结构。

此外，在图 3 的树结构中包含的各装置中包含了使用各种记录媒体、例如固定于装置中的或对于装置来说可自由装卸地构成的 DVD、CD、MD、闪速存储器等的各种类型的装置。再者，可与各种应用服务程序共存。将图 3 中示出的内容或密钥发布结构、即分级树结构应用于这样的不同的装置、不同的应用程序的共存结构。

在这样的各种不同的装置、应用程序共存的系统中，例如将用图 3 的点线包围的部分、即装置 0、1、2、3 作为使用同一记录媒体的 1 个组来设定。例如进行下述的处理：对于用该点线包围的组内包含的装置来说，对共同的内容进行加密后，由提供者将其集中地发送给上述装置，或发送各装置共同地使用的内容密钥，或对内容收费的支付数据进行了加密后，从各装置对提供者或批准机关输出该加密的支付数据。内容提供者或批准处理机关等进行与各装置的数据接收发送的机关将用图 3 的点线包围的部分、即装置 0、1、2、3 作为 1 个组，进行一并地发送数据的处理。在图 3 的树中存在多个这样的组。内容提供者或批准处理机关等进行与各装置的数据接收发送的机关起到消息（message）数据分配装置的功能。

再有，可由某一个密钥管理中心一并地管理节点密钥、叶密钥，也可作成由进行对于各组的各种数据接收发送的提供者或批准机关等的消息数据分配装置管理各个组的结构。关于这些节点密钥、叶密钥，

例如在密钥的泄漏等的情况下进行更新处理，密钥管理中心、提供者、批准机关等进行该更新处理。

在该树结构中，如从图 3 可明白，1 个组中包含的 3 个装置 0、1、2、3 保有共同的密钥 K00、K0、KR 作为节点密钥。通过利用该节点密钥共有结构，例如可只对装置 0、1、2、3 提供共同的内容密钥。例如，如果将共同保有的节点密钥 K00 作为内容密钥来设定，则可只对装置 0、1、2、3 进行共同的内容密钥的设定而不进行新的密钥发送。此外，如果经网络或存储在存储媒体中对装置 0、1、2、3 发布用节点密钥 K00 对新的内容密钥 Kcon 进行了加密的值 Enc（K00，Kcon），则只有装置 0、1、2、3 使用在各自的装置中保有的共有节点密钥 K00 才能对密码 Enc（K00，Kcon）进行解密来得到内容密钥 Kcon。再有，Enc（Ka，Kb）表示用 Ka 对 Kb 进行了加密的数据。

此外，在某个时刻 t 处发现了装置 3 所具有的密钥：K0011、K001、K00、KR 被攻击者（黑客）解析出来而暴露了的情况下，为了在此之后保护在系统（装置 0、1、2、3 的组）中发送接收的数据，必须将装置 3 与系统断开。为此，必须将节点密钥 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，对装置 0、1、2 发送该更新密钥。在此，K（t）aaa 表示密钥 Kaaa 这一代 t 的更新密钥。

以下说明更新密钥的发布处理。通过例如将由图 4（A）中示出的被称为有效化密钥块（EKB）的块数据构成的表存储在网络或记录媒体中供给装置 0、1、2 来进行密钥的更新。再有，利用对与构成图 3 中示出的树结构的各叶对应的装置发布新的更新了的密钥用的加密密钥来构成有效化密钥块（EKB）。有效化密钥块（EKB）有时也被称为密钥更新块（KRB）。

在图 4（A）中示出的有效化密钥块（EKB）中，作为具有只有节点密钥的更新的必要的装置才能更新的数据结构的块数据来构成。图 4 的例子是在图 3 中示出的树结构中的装置 0、1、2 中以发布代 t 的更新节点密钥为目的而形成的块数据。如从图 3 可明白的那样，装置 0、装置 1 必须有 K（t）00、K（t）0、K（t）R 作为更新节点密钥，装置 2 必须有 K（t）001、K（t）00、K（t）0、K（t）R 作为更新节点密钥。

如图 4（A）的 EKB 中所示那样，在 EKB 中包含多个加密密钥。最下面的一段的加密密钥是 Enc（K0010，K（t）001）。这是用装置 2 所具有的叶密钥 K0010 进行了加密的更新节点密钥 K（t）001，装置 2 利用自身具有的叶密钥对该加密密钥进行解密，可得到 K（t）001。此外，利用解密得到的 K（t）001，可对从图 4（A）下面算起第 2 段的加密密钥 Enc（K（t）001，K（t）00）进行解密，可得到更新节点密钥 K（t）00。以下，依次对从图 4（A）上面算起第 2 段的加密密钥 Enc（K（t）00，K（t）0）进行解密，可得到更新节点密钥 K（t）0，对从图 4（A）上面算起第 1 段的加密密钥 Enc（K（t）0，K（t）R）进行解密，可得到 K（t）R。另一方面，关于装置 K0000，K0001，节点密钥 K000 没有包含在更新的对象中，作为更新节点密钥所需要的是 K（t）00、K（t）0、K（t）R。装置 K0000，K0001 对从图 4（A）上面算起第 3 段的加密密钥 Enc（K000，K（t）00）进行解密，取得 K（t）00，对从图 4（A）上面算起第 2 段的加密密钥 Enc（K（t）00，K（t）0）进行解密，取得更新节点密钥 K（t）0，对从图 4（A）上面算起第 1 段的加密密钥 Enc（K（t）0，K（t）R）进行解密，得到 K（t）R。这样，装置 0、1、2 可得到更新了的密钥 K（t）R。再有，图 4（A）的索引表示作为解密密钥使用的节点密钥、叶密钥的绝对地址。

在不需要进行图 3 中示出的树结构的高位段的节点密钥：K（t）0、K（t）R 的更新、只需要进行节点密钥 K00 的更新处理的情况下，通过使用图 4（B）的有效化密钥块（EKB），可对装置 0、1、2 发布更新节点密钥 K（t）00。

在例如发布在特定的组中共有的新的内容密钥的情况下可利用图 4（B）中示出的 EKB。作为具体例，假定图 3 中用点线示出的组内的装置 0、1、2、3 使用了某个记录媒体，必须有新的共同的内容密钥 K（t）con。此时，与图 4（B）中示出的 EKB 一起发布使用更新了装置 0、1、2、3 的共同的节点密钥 K00 的 K（t）00 对新的共同的内容密钥 K（t）con 进行了加密的数据 Enc（K（t），K（t）con）。利用该发布，可实现作为装置 4 等其它的组的装置中不能解密的数据的发布。

即，如果装置 0、1、2 使用处理 EKB 得到的 K（t）00 对上述密码文进行解密，则可得到在 t 时刻的内容密钥 K（t）con。

〔使用了 EKB 的内容密钥的发布〕

在图 5 中，作为得到 t 时刻的内容密钥 K（t）con 的处理例，示出经记录媒体接受了使用 K（t）00 对新的共同的内容密钥 K（t）con 进行了加密的数据 Enc（K（t）00，K（t）con）和图 4（B）中示出的 EKB 的装置 0 的处理。即，这是将由 EKB 得到的加密消息数据作为内容密钥 K（t）con 的例子。

如图 5 中所示，装置 0 使用在存储媒体中存储了的代：t 时刻的 EKB 和自身预先存储了的节点密钥 K000 并利用与上述同样的 EKB 处理，生成节点密钥 K（t）00。再者，使用已解密的更新节点密钥 K（t）00 对更新内容密钥 K（t）con 进行解密，为了其后使用该内容密钥 K（t）con，用自身具有的节点密钥 K0000 对其进行加密并存储。

〔EKB 的格式〕

在图 6 中示出有效化密钥块（EKB）的格式例。版本 601 是表示有效化密钥块（EKB）的版本的识别符。再有，版本具有表示识别最新的 EKB 的功能与内容的对应关系的功能。深度（depth）表示对于有效化密钥块（EKB）的发布目的地的装置的分级树的分段数。数据指针 603 是表示有效化密钥块（EKB）中的数据部的位置的指针，标识符指针 604 表示标识符部的位置，署名指针 605 是表示署名的位置的指针。

数据部 606 例如存储对更新的节点密钥进行了加密的数据。例如存储关于图 5 中示出的已被更新的节点密钥的各加密密钥等。

标识符部 607 是表示在数据部中已被存储的加密了的节点密钥与叶密钥的位置关系的标识符。使用图 7 说明该标识符的赋予规则。在图 7 中，示出了发送前面在图 4（A）中已说明的有效化密钥块（EKB）作为数据的例子。此时的数据如图 7 的表（b）中所示那样。将此时的加密密钥中包含的顶部节点的地址定为顶部节点地址。此时，由于包含了根密钥的更新密钥 K（t）R，故顶部节点地址为 KR。此时，例如最上段的数据 Enc（K（t）0，K（t）R）位于图 7 的（a）中示出的分级树中示出的位置上。在此，下一个数据是 Enc（K（t）00，K（t）0），在树上位于前一个数据的左下的位置上。在有数据的情况下，将标识符设定为 0，在没有数据的情况下，将标识符设定为 1。将标识符作为{左（L）标识符，右（R）标识符}来设定。由于在最上段的数

据（K（t）0，K（t）R）的左边有数据，故 L 标识符 = 0，在右边没有数据，故 R 标识符 = 1。以下，对全部的数据设定标识符，构成图 7（c）中示出的数据列和标识符列。

标识符是为了表示数据 Enc（Kxxx，Kyyy）位于树结构的何处而设定的。由于在数据部中已被存储的密钥数据 Enc（Kxxx，Kyyy）…不过是单纯地已被加密的密钥的罗列数据，故利用上述的标识符可判别作为数据已被存储的加密密钥的在树上的位置。在不使用上述的标识符的情况下，如在前面的图 4 中已说明的结构那样，使用与加密数据对应的节点索引，也可作成例如

0：Enc（K（t）0，K（t）root）

00：Enc（K（t）00，K（t）0）

000：Enc（K（t）000，K（t）00）

…那样的数据结构，但如果作成使用这样的索引的结构，则成为冗余的数据，数据量增大，在经网络的信息分配中是不理想的。与此不同，通过使用上述的标识符作为表示上述的密钥位置的索引数据，可用少的数据量来进行密钥位置的判别。

返回到图 6，进一步说明 EKB 格式。署名（Signature）是发行了有效化密钥块（EKB）的例如密钥管理中心、内容提供者、批准机关等进行的电子署名。接受了 EKB 的装置根据署名验证来确认是正当的有效化密钥块（EKB）发行者发行的有效化密钥块（EKB）。

〔使用了 EKB 的内容密钥和内容的分配〕

在上述的例子中，说明了与 EKB 一起只发送内容密钥的例子，但以下说明同时发送用内容密钥进行了加密的内容、用内容密钥加密密钥进行了加密的内容密钥和利用 EKB 进行了加密的内容密钥加密密钥的结构。

在图 8 中说明该数据结构。在图 8(a)中示出的结构中，Enc(Kcon，content）801 表示是用内容密钥（Kcon）对内容（content）进行了加密的数据，Enc（KEK，Kcon）802 表示是用内容密钥加密密钥（KEK）对内容密钥（Kcon）进行了加密的数据，Enc（EKB，KEK）803 表示是用有效化密钥块（EKB）对内容密钥加密密钥 KEK 进行了加密的数据。

在此，内容密钥加密密钥 KEK 可以是在图 3 中示出的节点密钥（K000，K00…）或根密钥（KR）本身，此外，也可以是用节点密钥

（K000，K00…）或根密钥（KR）进行了加密的密钥。

图 8（b）示出在媒体上记录了多个内容、各自利用了相同的 Enc（EKB，KEK）805 情况的结构例，在这样的结构中，在不对各数据附加相同的 Enc（EKB，KEK）的情况下，可作成将表示链接到 Enc（EKB，KEK）上的链接目的地的数据附加到各数据上的结构。

图 9 中示出将内容密钥加密密钥 KEK 作为更新了图 3 中示出的节点密钥 K00 的更新节点密钥 K（t）00 而构成的情况的例子。此时，在用图 3 的点线框包围的组中，假定装置 3 例如因密钥的泄漏的缘故而被排除了，通过对其它的组的成员、即装置 0、1、2 分配图 9 中示出的（a）有效化密钥块（EKB）、（b）用内容密钥加密密钥（KEK = K（t）00）对内容密钥（Kcon）进行了加密的数据和（c）用内容密钥（Kcon）对内容（content）进行了加密的数据，装置 0、1、2 可得到内容。

在图 9 的右侧，示出了装置 0 中的解密顺序。装置 0 首先利用使用了自身所保有的节点密钥 K000 从已接受的有效化密钥块取得内容密钥加密密钥（KEK = K（t）00）。其次，利用由 K（t）00 进行的解密来取得内容密钥 Kcon，再利用内容密钥 Kcon 取得内容的解密。利用这样的处理，装置 0 可利用内容。在装置 1、2 中，也通过用各自不同的处理顺序来处理 EKB，可取得内容密钥加密密钥（KEK = K（t）00），同样可利用内容。

即使图 3 中示出的其它的组的装置 4、5、6…接受了该同样的数据（EKB），也不能使用自身所保有的叶密钥、节点密钥来取得内容密钥加密密钥（KEK = K（t）00）。同样，即使在被排除了的装置 3 中，也不能使用自身所保有的叶密钥、节点密钥来取得内容密钥加密密钥（KEK = K（t）00），只有具有正当的权利的装置才能对内容进行解密来利用。

这样，如果采用利用了 EKB 的内容密钥的发送，则可减少数据量，而且可安全地分配只有正当的权利者才能解密的加密内容。

再有，有效化密钥块（EKB）、内容密钥、加密内容等是可经网络安全地分配的结构，但也可将有效化密钥块（EKB）、内容密钥、加密内容存储在 DVD、CD 等的记录媒体中来提供给用户。此时，在记录媒体中已被存储的加密内容的解密中，如果构成为使用由在同一记录媒

体中已被存储的有效化密钥块（EKB）的解密得到的内容密钥，则可用简单的结构来实现只有用正当的权利者预先保有的叶密钥、节点密钥才能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。

在图 10 中示出在记录媒体中与加密内容一起存储了有效化密钥块（EKB）的结构例。在图 10 中示出的例子中，在记录媒体中存储了内容 C1～C4，还存储了与有效化密钥块（EKB）对应的数据，该有效化密钥块（EKB）与各存储内容相对应，还存储了版本 M 的有效化密钥块（EKB－M）。例如，EKB_1 在生成对内容 C1 进行了加密的内容密钥 Kcon1 时被使用，例如，EKB_2 在生成对内容 C2 进行了加密的内容密钥 Kcon2 时被使用。在该例子中，版本 M 的有效化密钥块（EKB－M）存储在记录媒体中，由于内容 C3、C4 与有效化密钥块（EKB－M）相对应，故利用有效化密钥块（EKB－M）的解密可取得内容 C3、C4 的内容密钥。由于 EKB_1、EKB_2 未存储在盘中，故必须利用新的提供装置、例如网络分配或由记录媒体进行的分配，来取得为了对各自的内容密钥进行解密所必要的 EKB_1、EKB_2。

在图 11 中示出利用了内容在多个装置间流通时的 EKB 的内容密钥的分配与现有的内容密钥分配处理的比较例。上半部分（a）是现有的结构，下半部分（b）是利用了本发明的有效化密钥块（EKB）的例子。再有，在图 11 中，Ka（Kb）表示是用 Ka 对 Kb 进行了加密的数据。

如（a）中所示，以往，为了确认数据发送接收者的正当性及共有在数据发送的加密处理中使用的对话密钥 Kses，在各装置间进行认证处理和密钥交换处理（AKE），以认证成立为条件，用对话密钥 Kses 对内容密钥 Kcon 进行了加密后进行发送处理。

例如在图 11（a）的 PC 中，用对话密钥对用已接受的对话密钥进行了加密的对话密钥 Kses（Kcon）进行解密，可得到 Kcon，再用 PC 自身保有的保存密钥 Kstr 对已取得的 Kcon 进行了解密后，可保存在自身的存储器中。

在图 11（a）中，即使在内容提供者打算用只在图 11（a）的记录装置 1101 中能利用的形态来分配的情况下，在其间存在 PC、播放装置的情况下，如图 11（a）中所示，也必须进行认证处理，进行用

各自的对话密钥对内容密钥进行了加密后分配的处理。此外，即使在介于其间的 PC、播放装置中，通过使用在认证处理中生成并共有的对话密钥对加密内容密钥进行解密，也能取得内容密钥。

另一方面，在利用了图 11（b）的下半部分中示出的有效化密钥块（EKB）的例子中，通过从内容提供者分配有效化密钥块（EKB）、利用有效化密钥块（EKB）的处理得到的节点密钥或利用根密钥对内容密钥 Kcon 进行了加密的数据（在图的例子中，Kroot（Kcon）），可只在能进行已分配的 EKB 的处理的装置中对内容密钥 Kcon 进行解密并取得内容密钥 Kcon。

因而，例如生成只在 图 11（b）的右端能利用的有效化密钥块（EKB），通过同时发送该有效化密钥块（EKB）、由该 EKB 处理得到的节点密钥或由根密钥对内容密钥 Kcon 进行了加密的数据，其间存在的 PC、播放装置等不能利用自身所具有的叶密钥、节点密钥进行 EKB 的处理。因而，可不进行在数据发送接收装置间的认证处理、对话密钥的生成、由对话密钥进行的内容密钥 Kcon 的加密处理那样的处理，可安全地分配只对于正当的装置来说能利用的内容密钥。

在打算分配在 PC、记录播放器中也能利用的内容密钥的情况下，通过生成并分配在各自的装置中能处理的有效化密钥块（EKB），可取得共同的内容密钥。

〔使用了有效化密钥块（EKB）的认证密钥的分配（共同密钥方式）〕

在使用了上述的有效化密钥块（EKB）的数据或密钥的分配中，由于在装置间被传送的有效化密钥块（EKB）和内容或内容密钥维持常时地相同的加密形态，故因偷窃和记录数据传送路径、之后再次传送的所谓的重放攻击的缘故，存在生成不正当复制的可能性。作为防止该情况的结构，在数据传送装置间进行与以往同样的认证处理和密钥交换处理是有效的方法。在此，说明通过使用上述的有效化密钥块（EKB）对装置发送进行该认证处理和密钥交换处理时使用的认证密钥 Kake、具有共有的认证密钥作为安全的秘密密钥并进行按照共同密钥方式的认证处理的结构。即，是将由 EKB 得到的加密消息数据作为认证密钥的例子。

图 12 中示出使用了共同密钥加密方式的相互认证方法（ISO/IEC

9798－2)。在图 12 中，使用了 DES 作为共同密钥加密方式，但只要是共同密钥加密方式，也可使用其它的方式。在图 12 中，首先，生成 B 为 64 位的随机数 Rb，将 Rb 和作为自己的 ID 的 ID（b）发送给 A。接受了 Rb 和 ID（b）的 A 生成新的 64 位的随机数 Ra，按 Ra、Rb、ID（b）的顺序，用 DES 的 CBC 模式并使用密钥 Kab 对数据进行加密，返回给 B。再有，密钥 Kab 是作为共同的秘密密钥在各自的记录元件内存储的密钥。关于由使用了 DES 的 CBC 模式的密钥 Kab 进行的加密处理，在例如使用了 DES 的处理中，对初始值与 Ra 进行异或（EXOR）运算，在 DES 加密部中，使用密钥 Kab 进行加密，生成密码文 E1，接着，对密码文 E1 与 Rb 进行异或运算，在 DES 加密部中，使用密钥 Kab 进行加密，生成密码文 E2，再者，对密码文 E2 与 ID（b）进行异或运算，在 DES 加密部中，使用密钥 Kab 进行加密，生成密码文 E3，由此来生成发送数据（Token-AB)。

接受了该信息的 B 用在各自的记录元件内存储的密钥 Kab（认证密钥）作为共同的秘密密钥对接收数据进行解密。关于接收数据的解密方法，首先用认证密钥 Kab 对密码文 E1 进行解密，得到随机数 Ra。其次，用认证密钥 Kab 对密码文 E2 进行解密，对其结果与 E1 进行异或运算，得到 Rb。最后，用认证密钥 Kab 对密码文 E3 进行解密，对其结果与 E2 进行异或运算，得到 ID（b)。验证这样得到的 Ra、Rb、ID（b）中的 Rb 和 ID（b）是否与 B 发送的 Rb 和 ID（b）一致。在通过了该认证的情况下，B 将 A 认证为正当的。

其次，B 生成在认证后使用的对话密钥（Kses)(生成方法是使用随机数)。然后，按 Ra、Rb、ID（b）的顺序，用 DES 的 CBC 模式并使用密钥 Kab 进行加密，返回给 A。

接受了该信息的 A 用认证密钥 Kab 对接收数据进行解密。由于接收数据的解密方法与 B 的解密处理相同，故在此省略其细节。验证这样得到的 Rb、Ra、Kses 中的 Rb 和 Ra（b）是否与 A 发送的 Rb 和 Ra 一致。在通过了该认证的情况下，A 将 B 认证为正当的。在互相认证了对方后，将对话密钥 Kses 作为认证后的秘密通信用的共同密钥来利用。

再有，在接收数据的验证时，在发现了不正当、不一致的情况下，相互认证失败，中断处理。

在上述的认证处理中，A、B 共有共同的认证密钥 Kab。使用上述的有效化密钥块（EKB），对装置分配该共同密钥 Kab。

例如，在图 12 的例子中，也可作成 A 或 B 的某一方生成另一方可解密的有效化密钥块（EKB）、利用已生成的有效化密钥块（EKB）对认证密钥 Kab 进行加密从而发送给另一方的结构。或者，也可作成第 3 者生成对装置 A、B 来说两者可利用的有效化密钥块（EKB）、利用对于装置 A、B 生成的有效化密钥块（EKB）对认证密钥 Kab 进行加密从而进行发送的结构。

在图 13 和图 14 中示出利用有效化密钥块（EKB）对多个装置分配共同的认证密钥 Kake 的结构例。图 13 是分配对装置 0、1、2、3 来说可解密的认证密钥 Kake 的例子，图 14 是排除对装置 0、1、2、3 中的装置 3、分配只对装置 0、1、2 来说可解密的认证密钥的例子。

在图 13 的例子中，与利用更新节点密钥 K（t）00 对认证密钥 Kake 进行了加密的数据（b）一起，生成并分配在装置 0、1、2、3 中使用各自具有的节点密钥、叶密钥能对已被更新的节点密钥 K（t）00 进行解密的有效化密钥块（EKB）。各自的装置，如图 13 的右侧中所示，首先，通过对 EKB 进行处理（解密），取得已被更新的节点密钥 K（t）00，其次，使用已取得的节点密钥 K（t）00 对已被加密的认证密钥 Enc（K（t）00，Kake）进行解密，可得到认证密钥 Kake。

由于其它的装置 4、5、6、7…即使接受同一有效化密钥块（EKB）也不能用自身保有的节点密钥、叶密钥处理 EKB 而取得已被更新的节点密钥 K（t）00，故可安全地只对正当的装置发送认证密钥。

另一方面，图 14 的例子是假定用图 3 的点线框包围的组中装置 3 因例如密钥的泄漏的缘故而被排除、生成和分配只对其它的组的成员、即装置 0、1、2 能解密的有效化密钥块（EKB）的例子。分配用节点密钥 K（t）00 对图 14 中生成的（a）有效化密钥块（EKB）和（b）认证密钥 Kake 进行了加密的数据。

在图 14 的右侧，示出了解密顺序。装置 0、1、2 首先利用使用了自身保有的节点密钥、叶密钥的解密处理，从已接受的有效化密钥块取得更新节点密钥 K（t）00。其次，利用由 K（t）00 得到的解密，取得认证密钥 Kake。

图 3 中示出的其它的组的装置 4、5、6…即使接受同样的数据（EKB）

也不能用自身保有的叶密钥、节点密钥取得更新节点密钥 K（t）00。同样，装置 3 也不能使用自身所保有的叶密钥、节点密钥来取得更新节点密钥 K（t）00，只有具有正当的权利的装置才能对认证密钥进行解密而利用。

这样，如果使用利用了 EKB 的认证密钥的发送，则可减少数据量，而且可分配只有正当的权利者才能解密的认证密钥。

〔公开密钥认证和使用了有效化密钥块（EKB）的内容密钥的分配〕

其次，说明公开密钥认证和使用了有效化密钥块（EKB）的内容密钥的分配处理。首先，使用图 15 说明使用了作为公开密钥加密方式的 160 位长的椭圆曲线密码的相互认证方法。在图 15 中，使用了 E 信息处理方法作为公开密钥加密方式，但只要是同样的公开密钥加密方式，则可使用任一种方式。此外，密钥尺寸也可不是 160 位。在图 15 中，首先 B 生成 64 位的随机数 Rb，发送给 A。接受了该随机数 Rb 的 A 新生成 64 位的随机数 Ra 和比素数 p 小的随机数 Ak。然后，求出将基点 G 乘以 Ak 的点 Av = Ak × G，生成对于 Ra、Rb、Av（X 坐标和 Y 坐标）的电子署名 A.Sig，与 A 的公开密钥证明书一起返回给 B。在此，由于 Ra 和 Rb 发布是 64 位，Av 的 X 坐标和 Y 坐标发布是 160 位，故生成合计对于 448 位的电子署名。

接受了 A 的公开密钥证明书、Ra、Rb、Av、电子署名 A.Sig 的 B 验证 A 发送来的 Rb 是否与 B 生成的 Rb 一致。其结果，在一致的情况下，用认证局的公开密钥验证 A 的公开密钥证明书内的电子署名，之后取出 A 的公开密钥。然后，使用已取出的 A 的公开密钥验证电子署名 A.Sig。

其次，B 生成比素数 p 小的随机数 Bk。然后，求出将基点 G 乘以 Bk 的点 Bv = Bk × G，生成对于 Ra、Rb、Bv（X 坐标和 Y 坐标）的电子署名 B.Sig，与 B 的公开密钥证明书一起返回给 A。

接受了 B 的公开密钥证明书、Ra、Rb、Bv、电子署名 B.Sig 的 A 验证 B 发送来的 Ra 是否与 A 生成的 Ra 一致。其结果，在一致的情况下，用认证局的公开密钥验证 B 的公开密钥证明书内的电子署名，之后取出 B 的公开密钥。然后，使用已取出的 B 的公开密钥验证电子署名 B.Sig。在电子署名的验证成功了后，A 将 B 认证为正当的。

在两者在认证中成功了的情况下，B 计算 Bk × Av（虽然 Bk 是随机数，但由于 Av 是椭圆曲线上的点，故必须计算椭圆曲线上的点的标量倍），A 计算 Ak × Bv，将中心的 X 坐标的低位 64 位作为对话密钥在以后的通信中使用（在将共同密钥密码定为 64 位密钥长度的共同密钥密码的情况下）。当然，可从 Y 坐标来生成对话密钥，也可不是低位 64 位。再有，在相互认证后的秘密通信中，发送数据不仅用对话密钥加密，而且有时也附以电子署名。

在电子署名的验证或接收数据的验证时，在发现了不正当、不一致的情况下，相互认证失败，中断处理。

在图 16 中示出使用了公开密钥认证和有效化密钥块（EKB）的内容密钥的分配处理例。首先，在内容提供者与 PC 间进行在图 15 中已说明的公开密钥方式的认证处理。内容提供者生成由作为内容密钥分配目的地的播放装置、记录媒体所具有的节点密钥、叶密钥能解密的 EKB，用在 PC 间的认证处理中生成的对话密钥 Kses 对进行了更新节点密钥的加密的内容密钥 E（Kcon）和有效化密钥块（EKB）进行加密后发送给 PC。

PC 用对话密钥对用对话密钥进行了加密的〔进行了更新节点密钥的加密的内容密钥 E（Kcon）和有效化密钥块（EKB)〕进行了解密后，发送给播放装置、记录媒体。

播放装置、记录媒体利用自身所保有的节点密钥或叶密钥，通过对〔进行了更新节点密钥的加密的内容密钥 E（Kcon）和有效化密钥块（EKB)〕进行解密，取得内容密钥 Kcon。

按照该结构，由于将内容提供者与 PC 间的认证作为条件，发送〔进行了更新节点密钥的加密的内容密钥 E（Kcon）和有效化密钥块（EKB)〕，故例如即使在存在节点密钥的泄漏的情况下，也能进行对于可靠的对方的数据发送。

〔使用了程序代码的有效化密钥块（EKB）的分配〕

在上述的例子中，说明了使用有效化密钥块（EKB）对内容密钥、认证密钥等进行了加密后分配的方法，但也可作成使用有效化密钥块（EKB）分配各种各样的程序代码的结构。即，这是将由 EKB 得到的加密消息数据作为程序代码的例子。以下，说明该结构。

在图 17 中示出利用有效化密钥块（EKB）的例如更新节点密钥对

程序代码进行了加密后在装置间发送的例子。装置 1701 将由装置 1702 所具有的节点密钥、叶密钥能解密的有效化密钥块（EKB）和用有效化密钥块（EKB）中包含的更新节点密钥进行了加密处理的程序代码发送给装置 1702。装置 1702 处理已接受的 EKB，取得更新节点密钥，再利用已取得的更新节点密钥进行程序代码的解密，得到程序代码。

在图 17 中示出的例子中，还示出了在装置 1702 中进行由已取得的程序代码进行的处理、将其结果返回给装置 1701、装置 1701 根据其结果再继续进行处理的例子。

通过以这种方式分配有效化密钥块（EKB）和用有效化密钥块（EKB）中包含的更新节点密钥进行了加密处理的程序代码，可对上述的图 3 中示出的特定的装置或组分配在特定的装置中可解读的程序代码。

〔与对于发送内容的检验值（ICV：完整性检验值）相对应的结构〕

其次，说明为了防止内容的篡改而生成内容的完整性检验值（ICV）、与内容相对应地利用 ICV 的计算来判定有无内容的篡改的处理结构。

例如使用对于内容的 hash 函数来计算完整性检验值（ICV），利用 ICV = hash（Kicv，C1，C2，…）来计算。Kicv 是 ICV 生成密钥。C1，C2 是内容的信息，内容的重要信息的消息认证代码（MAC）被使用。

在图 18 中示出使用了 DES 密码处理结构的 MAC 值的生成例。如图 18 的结构中所示，将成为对象的消息分割为 8 字节单位，（以下，将已被分割的消息定为 M1、M2、…、MN），首先，求初始值（以下，定为 IV）与 M1 的异或运算值（将其结果定为 I1）。其次，将 I1 输入到 DES 加密部中，使用密钥（以下，定为 K1）进行加密（将输出定为 E1）。接着，求 E1 与 M2 的异或运算值，将其输出 I2 输入到 DES 加密部中，使用密钥 K2 进行加密（输出为 E2）。以下，重复该过程，对全部的消息进行加密处理。最后得出的 EN 成为消息认证代码（MAC）。

将 hash 函数应用于这样的内容的 MAC 值和 ICV 生成密钥，来生成内容的完整性检验值（ICV）。对保证了没有篡改的例如内容生成时生成的 ICV 与根据内容新生成的 ICV 进行比较，如果能得到同一 ICV，

则可保证在内容中没有篡改，如果 ICV 不同，则判定为有篡改。

〔利用 EKB 来发布检验值（ICV）的生成密钥 Kicv〕

其次，说明利用上述的有效化密钥块来发送作为内容的完整性检验值（ICV）的生成密钥的 Kicv 的结构。即，这是将由 EKB 得到的加密消息数据作为内容的完整性检验值（ICV）的生成密钥的例子。

在图 19 和图 20 中示出在多个装置中发送共同的内容的情况下、利用有效化密钥块（EKB）分配验证有无这些内容的篡改用的完整性检验值生成密钥 Kicv 的结构例。图 19 示出分配对于装置 0、1、2、3 能解密的检验值生成密钥 Kicv 的例子，图 20 示出排除装置 0、1、2、3 的装置 3、分配只对装置 0、1、2 能解密的检验值生成密钥 Kicv 的例子。

在图 19 的例子中，与利用更新节点密钥 K（t）00 对检验值生成密钥 Kicv 进行了加密的数据（b）一起，生成并分配在装置 0、1、2、3 中使用各自具有的节点密钥、叶密钥能对已被更新的节点密钥 K（t）00 进行解密的有效化密钥块（EKB）。各自的装置，如图 19 的右侧中所示，首先，通过对 EKB 进行处理（解密），取得已被更新的节点密钥 K（t）00，其次，使用已取得的节点密钥 K（t）00 对已被加密的检验值生成密钥 Enc（K（t）00，Kicv）进行解密，可得到检验值生成密钥 Kicv。

由于其它的装置 4、5、6、7…即使接受同一有效化密钥块（EKB）也不能用自身保有的节点密钥、叶密钥处理 EKB 而取得已被更新的节点密钥 K（t）00，故可安全地只对正当的装置发送认证密钥。

另一方面，图 20 的例子是假定用图 3 的点线框包围的组中装置 3 因例如密钥的泄漏的缘故而被排除、生成和分配只对其它的组的成员、即装置 0、1、2 能解密的有效化密钥块（EKB）的例子。分配用节点密钥 K（t）00 对图 20 中生成的（a）有效化密钥块（EKB）和（b）用节点密钥 K（t）00 对检验值生成密钥（Kicv）进行了加密的数据。

在图 20 的右侧，示出了解密顺序。装置 0、1、2 首先利用使用了自身保有的节点密钥、叶密钥的解密处理，从已接受的有效化密钥块取得更新节点密钥 K（t）00。其次，利用由 K（t）00 得到的解密，取得检验值生成密钥 Kicv。

图 3 中示出的其它的组的装置 4、5、6…即使接受同样的数据（EKB）

也不能用自身保有的叶密钥、节点密钥取得更新节点密钥 K（t）00。同样，已被排除的装置 3 中，也不能使用自身所保有的叶密钥、节点密钥来取得更新节点密钥 K（t）00，只有具有正当的权利的装置才能对检验值生成密钥进行解密而利用。

这样，如果使用利用了 EKB 的检验值生成密钥的发送，则可减少数据量，而且可分配只有正当的权利者才能解密的检验值生成密钥。

通过使用这样的内容的完整性检验值（ICV），可排除 EKB 和加密内容的不正当的复制。例如，如图 21 中所示，有与能取得各自的内容密钥的有效化密钥块（EKB）一起存储了内容 C1 和内容 C2 的媒体 1，设想按原样将其复制到媒体 2 上的情况。EKB 和加密内容的复制是可能的，在能对 EKB 进行解密的装置中，可利用 EKB 和加密内容。

如图 21（b）中所示，作成与在各媒体中正当地存储了的内容相对应地存储完整性检验值（ICV（C1，C2））的结构。ICV（C1，C2）表示使用 hash 函数对内容 C1 和内容 C2 进行计算的内容的完整性检验值、即 hash（Kicv，C1，C2）。在图 21（b）的结构中，在媒体 1 中正当地存储内容 C1 和内容 C2，并存储根据内容 C1 和内容 C2 生成的完整性检验值（ICV（C1，C2））。此外，在媒体 2 中正当地存储内容 C1，并存储根据内容 C1 生成的完整性检验值（ICV（C1））。在该结构中，如果将在媒体 1 中已被存储的{EKB，内容 2}复制到媒体 2 中，而且如果在媒体 2 中新生成内容检验值，则就生成 ICV（C1，C2），与在媒体中存储了的 Kicv（C1）不同，很明显，进行了因内容的篡改或正当的复制导致的新的内容的存储。在播放媒体的装置中，在播放步骤的前一个步骤中，进行 ICV 检验，判别生成 ICV 与存储 ICV 的一致，通过作成在不一致的情况下不进行播放的结构，可防止不正当复制的内容的播放。

此外，为了提高安全性，也可作成改写内容的完整性检验值（ICV）、根据包含了计数器的数据来生成的结构。即，作成利用 hash（Kicv，counter + 1，C1，C2，…）来计算的结构。在此，计数器（counter + 1）在 ICV 的每次改写时作为加 1 的值来设定。再有，必须作成在安全的存储器中存储计数值的结构。

再者，在不能在与内容为同一的媒体中存储内容的完整性检验值（ICV）的结构中，也可作成在与内容不同的其它的媒体上存储内容

的完整性检验值（ICV）的结构。

例如，在读入专用媒体或通常的 MO 等的未采取防止复制的对策的媒体上存储内容的情况下，如果在同一媒体上存储完整性检验值（ICV），则存在由不正当的用户进行 ICV 的改写的可能性，存在 ICV 的安全性不能保证的担心。在这样的情况下，通过在主机上的安全的媒体上存储了 ICV、作成在内容的复制控制（例如，check-in/checkout、move）中使用 ICV 的结构，可进行 ICV 的安全的管理和内容的篡改检验。

在图 22 中示出该结构例。该例子是这样的：在图 22 中，在读入专用媒体或通常的 MO 等的未采取防止复制的对策的媒体上存储内容，在不许可用户自由地存取的主机上的安全的媒体 2202 上存储关于这些内容的完整性检验值（ICV），防止了因用户引起的不正当的完整性检验值（ICV）的改写。作为这样的结构，如果作成例如安装了媒体 2201 的装置在进行媒体 2201 的播放时在作为主机的 PC、服务器中进行 ICV 的检验来判定播放的可否的结构，则可防止不正当的复制内容或篡改内容的播放。

〔分级树结构的类别分类〕

已说明了将加密密钥作为根密钥、节点密钥、叶密钥等的图 3 的分级树结构来构成、与有效化密钥块（EKB）一起对内容密钥、认证密钥、ICV 生成密钥或程序代码、数据等进行加密来分配的结构，但以下说明将定义了节点密钥等的分级树结构分类为各装置的每个类别以进行高效率的密钥更新处理、加密密钥分配、数据分配的结构。

在图 23 中示出分级树结构的类别的分类的一例。在图 23 中，在分级树结构的最上面一段中设定根密钥 Kroot2301，在以下的中间一段中，设定节点密钥 2302，在最下面一段中设定叶密钥 2303。各装置保有各自的叶密钥、从叶密钥到根密钥的一系列的节点密钥和根密钥。

在此，作为一例，将从最上面一段到第 M 段的某个节点作为类别节点 2304 来设定。即，将第 M 段的节点的每一个定为特定类别的装置设定节点。将第 M 段的 1 个节点作为顶点，将以下的 M+1 段有效的节点、叶定为关于该类别中包含的装置的节点和叶。

例如，在图 23 的第 M 段的 1 个节点 2305 上设定类别〔存储器 stick

（商标）〕，将在该节点以下连接的节点、叶作为包含使用了存储器 stick 的各种各样的装置的类别专用的节点或叶来设定。即，将节点 2305 以下作为被定义为存储器 stick 的类别的装置的关联节点和叶的集合来定义。

再者，可将从 M 段算起的几段的低位的段作为类别节点 2306 来设定。例如，如图中所示，在类别〔存储器 stick〕节点 2305 的 2 段下的节点上设定〔专用播放器〕的节点，作为使用了存储器 stick 的装置的类别中包含的子类别节点。再者，在作为子类别节点的专用播放器的节点 2306 以下，设定专用播放器的类别中包含的带有音乐播放功能的电话的节点 2307，可再在其低位上设定带有音乐播放功能的电话的类别中包含的〔PHS〕节点 2308 和〔携带电话〕节点 2309。

再者，不仅可用装置的种类来设定类别、子类别，而且可用某个厂家、内容提供者、批准机关等独自管理的节点、即处理单位、管辖单位或提供服务单位等任意的单位（以下将其总称为实体）来设定类别、子类别。例如，如果将 1 个类别节点作为游戏机厂家销售的游戏机 XYZ 专用的顶点节点来设定，则可在厂家销售的游戏机 XYZ 上存储其顶点节点以下的下段的节点密钥、叶密钥来销售，其后，通过生成和分配由该顶点节点密钥以下的节点密钥、叶密钥构成的有效化密钥块（EKB），可分配只有顶点节点以下的装置可利用的数据，这样来进行加密内容的分配或各种密钥的分配、更新处理。

这样，通过作成以 1 个节点为顶点、将以下的节点作为被该顶点节点定义的类别、子类别的关联节点来设定的结构，管理类别段或子类别段的 1 个顶点节点的厂家、内容提供者等可独自生成已该节点为顶点的有效化密钥块（EKB），可实现对属于顶点节点以下的装置进行分配的结构，可进行密钥更新而对属于其它的不属于顶点节点的类别的节点的装置完全没有影响。

〔由简化 EKB 进行的密钥分配结构（1）〕

在前面已说明的例如图 3 的树结构中，在将密钥、例如内容密钥发送给规定的装置（叶）时，生成并提供使用密钥发布目的地的装置所具有的叶密钥、节点密钥可解密的有效化密钥块（EKB）。例如在图 24（a）中生成的树结构中，在对构成叶的装置 a、g、j 发送密钥、例如内容密钥的情况下，生成并分配在 a、g、j 的各节点中可解密的

有效化密钥块（EKB）。

例如，考虑用更新根密钥 K（t）root 对内容密钥 K（t）con 进行加密处理、与 EKB 一起分配的情况。此时，装置 a、g、j 分别使用图 24（b）中生成的叶和节点密钥，进行 EKB 的处理，取得 K（t）root，利用已取得的更新根密钥 K（t）root 进行对内容密钥 K（t）con 的解密处理，得到内容密钥。

此时所提供的有效化密钥块（EKB）的结构如图 25 中所示。图 25 中生成的有效化密钥块（EKB）按照在前面的图 6 中已说明的有效化密钥块（EKB）的格式来构成，具有与数据（加密密钥）对应的标识符。标识符如在前面使用图 7 已说明的那样，如果在左（L）、右（R）各自的方向上有数据，则表示为 0，如果没有数据，则表示为 1。

接受了有效化密钥块（EKB）的装置根据有效化密钥块（EKB）的加密密钥和标识符，依次进行加密密钥的解密处理，取得高位节点的更新密钥。如图 25 中所示，在有效化密钥块（EKB）中，从根到叶的段数（深度）越多，其数据量越增加。段数（深度）随装置（叶）数而增大，在成为密钥的分配目的地的装置数目多的情况下，EKB 的数据量进一步增大。

说明可削减这样的有效化密钥块（EKB）的数据量的结构。图 26 是示出根据密钥分配装置而简化了有效化密钥块（EKB）的结构的例子的图。

与图 25 同样，设想对构成叶的装置 a、g、j 发送密钥、例如内容密钥的情况。如图 26 的（a）中所示，构筑只由密钥分配装置构成的树。此时，根据图 24 的（b）中示出的结构构筑图 26 的（b）树结构作为新的树结构。从 Kroot 到 Kj 全部没有分支、只存在 1 个枝即可，为了从 Kroot 到 Ka 和 Kg，只在 K0 处构成分支点，构筑 2 分支结构的图 26（a）的树。

如图 26（a）中所示，生成只具有 K0 作为节点的简化了的树。根据这些简化树来生成更新密钥分配用的有效化密钥块（EKB）。图 26（a）中示出的树是通过选择构成将能对有效化密钥块（EKB）进行解密的末端节点或叶作为最下段的 2 分支型树的通路并省略不需要的节点以进行再构筑的再构筑分级树。只根据与该再构筑分级树的节点或叶对应的密钥来构成更新密钥分配用的有效化密钥块（EKB）。

在前面的图 25 中已说明的有效化密钥块（EKB）存储了对从各叶 a、g、j 到 Kroot 为止的全部的密钥进行了加密的数据，但简化 EKB 只存储关于构成简化了的树的节点的加密数据。如图 26（b）中所示，标识符具有 3 位结构。第 2 和第 3 位具有与图 25 的例子同样的意义，如果在左（L）、右（R）各自的方向上有数据，则表示为 0，如果没有数据，则表示为 1。第 1 位是表示在 EKB 内是否存储了加密密钥用的位，在存储了数据的情况下，设定为 1，在没有数据的情况下，设定为 0。

被存储在数据通信网或存储在存储媒体中并对装置（叶）提供的有效化密钥块（EKB），如图 26（b）中所示，如果与图 25 中示出的结构相比，则数据量被大幅度地被削减。接受了图 26 中示出的有效化密钥块（EKB）的各装置，通过依次只对标识符的第 1 位中存储了 1 的部分的数据进行解密，可实现规定的加密密钥的解密。例如，装置 a 用叶密钥 Ka 对 Enc（Ka，K（t）0）进行解密，取得节点密钥 K（t）0，利用节点密钥 K（t）0 对加密数据 Enc（K（t）0，K（t）root）进行解密，取得 K（t）root。装置 j 用叶密钥 Kj 对 Enc（Kj，K（t）root）进行解密，取得 K（t）root。

这样，通过构筑只由分配目的地的装置构成的简化了的新的树结构，只使用构成已被构筑的树的叶和节点的密钥来生成有效化密钥块（EKB），可生成数据量少的有效化密钥块（EKB）可有效地进行有效化密钥块（EKB）的数据分配。

〔由简化 EKB 进行的密钥分配结构（2）〕

说明可进一步简化根据图 26 中生成的简化了的树生成的有效化密钥块（EKB）、削减数据量、可进行有效的处理的结构。

使用凸 6 已说明的结构是通过选择构成将能对有效化密钥块（EKB）进行解密的末端节点或叶作为最下段的 2 分支型树的通路并省略不需要的节点以进行再构筑的再构筑分级树。只根据与该再构筑分级树的节点或叶对应的密钥来构成更新密钥分配用的有效化密钥块（EKB）。

图 26（a）中示出的再构筑分级树中，为了能在叶 a、g、j 中取得更新根密钥 K(t)root，分配图 26(b)中示出的有效化密钥块(EKB)。在图 26（b）的有效化密钥块（EKB）的处理中，叶 j 可利用 Enc（Kj，

K（t）root）的 1 次的解密处理取得根密钥：K（t）root。但是，叶 a、g 在利用 Enc（Ka，K（t）0）或 Enc（Kg，K（t）0）的解密处理得到了 K（t）0 后，还要进行 Enc（K（t）0，K（t）root）的解密处理来取得根密钥：K（t）root。即，叶 a、g 必须进行 2 次解密处理。

图 26 的简化了的再构筑分级树中，在节点 K0 作为其低位叶 a、g 的管理节点进行了独自的管理的情况下，例如在作为后述的子根节点进行了低位叶的管理的情况下，虽然在叶 a、g 确认取得了更新密钥的意义上是有效的，但在节点 K0 未进行低位叶的管理的情况下，或即使进行了管理、但在容许来自高位节点的更新密钥分配的情况下，也可进一步简化图 26（a）中示出的再构筑分级树，省略节点 K0 的密钥、生成并分配有效化密钥块（EKB）。

在图 27 中示出这样的有效化密钥块（EKB）的结构。与图 26 同样，设想对构成叶的装置 a、g、j 发送密钥、例如内容密钥的情况。如图 27（a）中所示，构筑直接连接了根 Kroot 与各叶 a、g、j 的树。

如图 27（a）中所示，由图 26（a）中示出的再构筑分级树生成省略了节点 K0 的简化树。根据这些简化树来生成更新密钥分配用的有效化密钥块（EKB）。图 27（a）中示出的树是利用直接连接可对有效化密钥块（EKB）进行解密的叶与根的通路进行再构筑的再构筑分级树。只根据与该再构筑分级树的叶对应的密钥来构成更新密钥分配用的有效化密钥块（EKB）。

再有，图 27（a）的例子是将末端作为叶的结构例，但在最高位节点对多个中位、低位节点分配密钥的情况下，也可根据直接连接了最高位节点与中位、低位节点的简化树生成有效化密钥块（EKB）来进行密钥分配。这样，再构筑分级树具有直接连接了构成简化了的树的顶点节点与构成简化了的树的末端节点或叶的结构。在该简化树中，来自顶点节点的分支不限于 2 个，可根据分配节点或叶的数目构成为具有 3 个以上的多分支的树。

在前面的图 25 中已说明的有效化密钥块（EKB）存储了对从各叶 a、g、j 到 Kroot 为止的全部的密钥进行了加密的数据，图 26 中已说明的有效化密钥块（EKB）是存储了叶 a、g、j 的叶密钥、作为 a、g 的共同节点的 K0 和根密钥的结构，但由于基于图 27（a）中示出的简化分级树的有效化密钥块（EKB）省略了节点 K0 的密钥，故如图 27（b）

中所示，成为进一步减少了数据量的有效化密钥块（EKB）。

图 27（b）的有效化密钥块（EKB）与图 26（b）的有效化密钥块（EKB）同样，具有 3 位结构的标识符。第 2 和第 3 位与图 26 中已说明的相同，如果在左（L）、右（R）各自的方向上有数据，则表示为 0，如果没有数据，则表示为 1。第 1 位是表示在 EKB 内是否存储了加密密钥用的位，在存储了数据的情况下，设定为 1，在没有数据的情况下，设定为 0。

在图 27（b）的有效化密钥块（EKB）中，各叶 a、g、j 利用 Enc（Ka，K（t）root）或 Enc（Kg，K（t）root）、Enc（Kj，K（t）root）的 1 次的解密处理可取得根密钥：K（t）root。

根据具有直接连接了以这种方式简化了的再构筑树的最高位节点与构成树的末端节点或叶的结构的树生成的有效化密钥块（EKB），如图 27（b）中所示，只根据与该再构筑分级树的顶点节点或末端节点或叶对应的密钥来构成。

如在图 26 或图 27 中已说明的有效化密钥块（EKB）那样，通过构筑只由分配目的地的装置构成的简化了的新的树结构，只使用构成已被构筑的树的叶或叶和共同节点的密钥来生成有效化密钥块（EKB），可生成数据量少的有效化密钥块（EKB），可有效地进行有效化密钥块（EKB）的数据分配。

再有，在后面说明的作为子树设定的类别树单位的 EKB 管理结构中，可特别有效地利用简化了的分级树结构。类别树是从构成作为密钥分配结构的树结构的节点或叶中选择的多个节点或叶的集合体块。类别树是根据装置的种类而被设定的集合，或作为装置提供厂家、内容提供者、批准机关等的管理单位等具有某个共同点的处理单位、管辖单位或提供服务单位等各种各样的形态的集合而被设定。在 1 个类别树中，集合了被分类为某个共同的类别的装置，例如通过利用多个类别树的顶点节点（子根）对与上述同样的简化了的树进行再构筑来生成 EKB，可实现在属于已被选择的类别树的装置中能解密的简化了的有效化密钥块（EKB）的生成、分配。在后面详细地说明类别树单位的管理结构。

再有，可作成在光盘、DVD 等的信息记录媒体上存储了这样的有效化密钥块（EKB）的结构。例如，可作成对各装置提供与包含由上

述的加密密钥数据构成的数据部和作为加密密钥数据的分级树结构中的位置识别数据的标识符部的有效化密钥块（EKB）一起存储了由更新节点密钥进行了加密的内容等的消息数据的信息记录媒体的结构。装置按照标识符部的识别数据依次抽出有效化密钥块（EKB）中包含的加密密钥数据进行解密，取得在内容的解密中必要的密钥，可进行内容的利用。当然，也可作成经互联网等的网络来分配有效化密钥块（EKB）的结构。

〔类别树单位的EKB管理结构〕

其次，说明用作为多个节点或叶的集合的块来管理构成作为密钥分配结构的树结构的节点或叶的结构。再有，以下将作为多个节点或叶的集合的块称为类别树。类别树是根据装置的种类而被设定的集合，或作为装置提供厂家、内容提供者、批准机关等的管理单位等具有某个共同点的处理单位、管辖单位或提供服务单位等各种各样的形态的集合而被设定。

使用图28说明类别树。图28（a）是说明以类别树单位来管理树的结构的图。在图中，1个类别树作为三角形来表示，例如在1个类别树2701内包含多个节点。表示1个类别树内的节点结构是（b）。1个类别树由以1个节点为顶点的多段2分支形树来构成。以下，将类别树的顶点节点2702称为子根。

树的末端，如（c）中所示，由叶、即装置来构成。将多个装置作为叶，装置属于由具有作为子根的顶点节点2702的树构成的某一个类别树。

从图28（a）可理解，类别树具有分级结构。使用图29说明该分级结构。

图29（a）是简化分级结构来说明用的图，从Kroot算起的几段下的段上构成类别树A01～Ann，在类别树A1～An的低位上设定了类别树B01～Bnk，进而，在其低位上设定了类别树C1～Cnq。如图29（b）、（c）中所示，各类别树具有由多段的节点、叶构成的树形状。

例如，类别树Bnk的结构，如（b）中所示，具有以子根2811为顶点节点并到达末端节点2812的多个节点。该类别树具有识别符Bnk，通过类别树Bnk独自地进行与类别树Bnk内的节点的节点密钥管理，进行以末端节点2812为顶点而被设定的低位（子）类别树的

管理。此外，另一方面，类别树 Bnk 处于以子根 2811 为末端节点而具有的高位（亲）类别树 Ann 的管理下。

类别树 Cn3 的结构，如（c）中所示，以子根 2851 为顶点节点，具有作为各装置的末端节点 2852、此时是到叶为止的多个节点、叶。该类别树具有识别符 Cn3，通过类别树 Cn3 独自进行与类别树 Cn3 内的节点、叶对应的节点密钥、叶密钥管理，来进行与末端节点 2852 对应的叶（装置）的管理。此外，另一方面，类别树 Cn3 处于以子根 2851 为末端节点而具有的高位（亲）类别树 Bn2 的管理下。所谓各类别树中的密钥管理，例如是密钥更新处理、排除处理等，但在后面详细地说明这些处理。

在作为最下段类别树的作为叶的装置中存储位于从装置所属的类别树的叶密钥到作为自己所属的类别树的子根节点的通路上的各节点的节点密钥和叶密钥。例如末端节点 2852 的装置存储从末端节点（叶）2852 到子根节点 2851 为止的各密钥。

使用图 30 进一步说明类别树的结构。类别树可具有由各种段数构成的树结构。段数、即深度（depth）是由类别树管理的与末端节点对应的低位（子）类别树的数目，或者可根据作为叶的装置数来设定。

如果交替地说明图 30 的（a）中生成的上下类别树，则成为（b）中示出的形态。根树是具有根密钥的最上段的树。在根树的末端节点上设定类别树 A、B、C 作为多个低位类别树，再者，设定类别树 D 作为类别树 C 的低位类别树。类别树 C2901 保持其末端节点的 1 个以上的节点作为保留节点 2950，在增加了自己管理的类别树的情况下，通过以保留节点 2950 作为顶点节点进一步新设置具有多段树结构的类别树 C′2902，可使管理末端节点 2970 增加，在管理末端节点上附加增加了的低位类别树。

再使用图 31 说明保留节点。类别树 A，3011 具有所管理的低位类别树 B、C、D、…，具有 1 个保留节点 3021。类别树在打算进一步增加管理对象的低位类别树的情况下，在保留节点 3021 上设定自己管理的低位类别树 A′，3012，在低位类别树 A′，3012 的末端节点上可进一步设定管理对象的低位类别树 F、G。自己管理的低位类别树 A′，3012 通过将其末端节点的至少 1 个设定为保留节点 3022，也可进一

步设定低位类别树 A''，3013，可进一步增加管理类别树。在低位类别树 A''，3013 的末端节点上也确保 1 个以上的保留节点。通过采取这样的保留节点保有结构，可没有限制地增加某个类别树所管理的低位类别树。再有，也可作成不仅将末端节点的 1 个节点设定为保留类别树、而且将末端节点的多个节点设定为保留类别树的结构。

在各自的类别树中，以类别树为单位构成有效化密钥块（EKB），进行以类别树为单位的密钥更新、排除处理。如图 31 中所示，在多个类别树 A、A'、A''上设定各类别树各自的有效化密钥块（EKB），但共同地管理类别树 A、A'、A''的例如某个装置厂家可一并地管理这些有效化密钥块（EKB）。

〔新的类别树的登录处理〕

其次，说明新的类别树的登录处理。在图 32 中示出登录处理顺序。按照图 32 的顺序来说明。新附加在树结构中的新的（子）类别树（N－En）对于高位（亲）类别树（P－En）进行新的登录要求。再有，各类别树保有依据公开密钥加密方式的公开密钥，新的类别树在登录要求时对高位（亲）类别树（P－En）发送自己的公开密钥。

接受了登录要求的高位（亲）类别树（P－En）将已接受的新的（子）类别树（N－En）的公开密钥转送给证明书发行局（CA），接受附加了 CA 的署名的新的（子）类别树（N－En）的公开密钥。这些手续作为高位（亲）类别树（P－En）与新的（子）类别树（N－En）的相互认证的手续来进行。

如果利用这些处理使新的登录要求类别树的认证结束，则高位（亲）类别树（P－En）许可新的（子）类别树（N－En）的登录，将新的（子）类别树（N－En）的节点密钥发送给新的（子）类别树（N－En）。该节点密钥是高位（亲）类别树（P－En）的末端节点的 1 个节点密钥，而且，与新的（子）类别树（N－En）的顶点节点、即子根密钥相对应。

如果该节点密钥的发送结束，则新的（子）类别树（N－En）构筑新的（子）类别树（N－En）的树结构，在已构筑的树的顶点上设定已接受的顶点节点的子根密钥，设定各节点、叶的密钥，生成类别树内的有效化密钥块（EKB）。将 1 个类别树内的有效化密钥块（EKB）称为子 EKB。

另一方面，高位（亲）类别树（P－En）根据新的（子）类别树（N－En）的附加，生成附加了有效化的末端节点的高位（亲）类别树（P－En）内的子 EKB。如果新的（子）类别树（N－En）生成由新的（子）类别树（N－En）内的节点密钥、叶密钥构成的子 EKB，则将其发送给高位（亲）类别树（P－En）。

从新的（子）类别树（N－En）接受了子 EKB 的高位（亲）类别树（P－En）将已接受的子 EKB 和高位（亲）类别树（P－En）的更新了的子 EKB 发送给密钥发行中心（KDC）。

密钥发行中心（KDC）根据全部的类别树的子 EKB，可生成各种形态的 EKB、即只有特定的类别树或装置能解密的 EKB。例如对内容提供者提供设定了以这种方式能解密的类别树或装置的 EKB，内容提供者根据 EKB 对内容进行加密，通过经网络或存储在记录媒体中来提供，可提供只有用特定的装置才能利用的内容。

再有，新的类别树的子 EKB 的对于密钥发行中心（KDC）的登录处理不限于经高位类别树依次转送子 EKB 来进行的方法，也可作成不经高位类别树、而是进行从新的登录类别树直接登录在密钥发行中心（KDC）上的处理的结构。

使用图 33 说明高位类别树与新附加到高位类别树上的低位类别树的对应关系。将高位类别树的末端节点的 1 个 3201 作为新附加的类别树的顶点节点，通过提供给低位类别树，低位类别树作为高位类别树管理下的类别树来附加。在后面详细地说明所谓高位类别树管理下的类别树，但它包含该结构是高位类别树能进行低位类别树的排除处理的结构的意义。

如图 33 中所示，如果在高位类别树上设定为低位类别树，则将作为高位类别树的叶的末端节点的 1 个节点 3201 和新附加的类别树的顶点节点 3202 作为等同的节点来设定。即，将作为高位类别树的 1 个叶的 1 个末端节点作为新附加的类别树的子根来设定。通过这样来设定，新附加的类别树在整体树结构下是有效的。

在图 34 中示出设定了新附加的类别树时高位类别树生成的更新 EKB 的例子。图 34 是示出了在（a）中示出的结构中、即在存在已经有效地存在的末端节点（node000）3301 和末端节点（node001）3302 的结构中对新附加的类别树赋予新的类别树附加末端节点（node100）

3303 时高位类别树生成的子 EKB 的例子的图。

子 EKB 具有图 34 的（b）中示出的结构。子 EKB 是包含下述部分的表，包含：利用分别有效地存在的末端节点密钥进行了加密的高位节点密钥、用高位节点密钥进行了加密的更高位的节点密钥、…进行到更高的高位、最后是子根密钥。利用该结构来生成子 EKB。各类别树与图 34（b）中示出的相同，具有由利用有效的末端节点或叶密钥进行了加密的高位节点密钥、用高位节点密钥对更高位的节点密钥进行加密、依次进入到更高位而达到子根的加密数据构成的 EKB，每个类别树的 EKB 由该类别树来管理。

〔类别树管理下的排除处理〕

其次，说明以密钥分配树结构作为类别树单位来管理的结构中的装置或类别树的排除处理。在前面的图 3、4 中，说明了分配只能由树结构整体中的特定的装置才能解密、被排除的装置不能解密的有效化密钥块（EKB）的处理。在图 3、4 中中已说明的排除处理是从树整体中排除作为特定的叶的装置的处理，但可在树的类别树管理的结构中对每个类别树进行排除处理。

使用图 35 以下的图，说明类别树管理下的树结构中的排除处理。图 35 是说明管理了构成树的类别树中的最下段的类别树、即各个装置的类别树的装置的排除处理的图。

图 35（a）示出了类别树管理的密钥分配树结构。在树的最高位上设定根节点，在其几段下构成了类别树 A01～Ann，在其低位的段上构成了 B01～Bnk 的类别树，在其更低位的段上构成了 C1～Cn 的类别树。最下的类别树的末端节点（叶）假定是各个装置、例如记录播放器、专用播放器等。

在此，说明在各类别树中独自进行排除处理。例如，在最下段的类别树 C1～Cn 中进行叶的装置的排除处理。在图 35（b）中，示出了作为最下段的类别树的 1 个的类别树 Cn，3430 的树结构。类别树 Cn，3430 是具有顶点节点 3431、在作为末端节点的叶上具有多个装置的结构。

如果假定在作为该末端节点的叶中存在成为排除对象的装置、例如装置 3432，则类别树 Cn，3430 生成由独自地更新了的类别树 Cn 内的节点密钥、叶密钥构成的有效化密钥块（EKB）。该有效化密钥块是

不能在排除装置 3432 中解密、只能在构成其它的叶的装置中才能解密的加密密钥构成的密钥块。类别树 Cn 的管理者生成该有效化密钥块（EKB）作为已被更新的子 EKB。具体地说，更新构成从子根连接到排除装置 3432 的通路的各节点 3431、3434、3435 的节点密钥，将作为排除装置 3432 以外的叶装置中才能对该更新节点密钥进行解密的加密密钥构成的块作为更新子 EKB。该处理与在前面的图 3、4 中已说明的排除处理结构中将根密钥置换为类别树的顶点密钥、即子根密钥的处理相对应。

这样，类别树 Cn，3430 将利用排除处理更新了的有效化密钥块（子 EKB）发送给高位类别树。此时，高位类别树是类别树 Bnk，3420，是具有类别树 Cn，3430 的顶点节点 3431 作为末端节点的类别树。

如果类别树 Bnk，3420 从低位类别树 Cn，3430 接受有效化密钥块（子 EKB），则将与该密钥块中包含的类别树 Cn，3430 的顶点节点 3431 对应的类别树 Bnk，3420 的末端节点 3431 设定为在低位类别树 Cn，3430 中已被更新的密钥，进行自身的类别树 Bnk，3420 的子 EKB 的更新处理。在图 35（c）中示出类别树 Bnk，3420 的树结构。在类别树 Bnk，3420 中，成为更新对象的节点密钥是从图 35（c）的子根 3421 到构成包含排除装置的类别树的末端节点 3431 的通路上的节点密钥。即，构成连接到发送了更新子 EKB 的类别树的节点 3431 上的通路的各节点 3421、3424、3425 的节点密钥成为更新对象。更新这些各节点的节点密钥来生成类别树 Bnk，3420 的新的更新子 EKB。

再者，将类别树 Bnk，3420 更新了的有效化密钥块（EKB）发送给高位类别树。此时，高位类别树是类别树 Ann，3410，是具有类别树 Bnk，3420 的顶点节点 3421 作为末端节点的类别树。

如果类别树 Ann，3410 从低位类别树 Bnk，3420 接受有效化密钥块（子 EKB），则将与该密钥块中包含的 Bnk，3420 的顶点节点 3421 对应的 Ann，3410 的末端节点 3421 设定为在低位类别树 Bnk，3420 中已被更新的密钥，进行自身的类别树 Ann，3410 的子 EKB 的更新处理。在图 35（d）中示出类别树 Ann，3410 的树结构。在类别树 Ann，3410 中，成为更新对象的节点密钥是构成从图 35（d）的子根 3411 连接到发送了更新子 EKB 的类别树的节点 3421 上的通路的各节点 3411、3414、3415 的节点密钥。更新这些各节点的节点密钥来生成类

别树 Ann，3410 的新的更新子 EKB。

在高位类别树中依次进行这些处理，进行到在图 30（b）中已说明的根类别树为止。利用该一系列的处理，结束装置的排除处理。再有，将在各自的类别树中已被更新的 EKB 最终发送给密钥发行中心（KDC）并由其进行保管。密钥发行中心（KDC）根据全部的类别树的更新子 EKB，生成各种各样的 EKB。更新 EKB 成为已被排除的装置中的不能解密的加密密钥块。

在图 36 中示出装置的排除处理的顺序图。按照图 36 的顺序图来说明处理次序。首先，为了排除装置管理类别树（D－En）内的排除对象的叶，处于树结构的最下段的装置管理类别树（D－En）进行必要的密钥更新，生成装置管理类别树（D－En）的新的子 EKB（D）。将更新子 EKB（D）发送给高位类别树。接受了更新子 EKB（D）的高位（亲）类别树（P1－En）生成更新了与更新子 EKB（D）的更新顶点节点对应的末端节点密钥和从其末端节点到子根的通路上的节点密钥的更新子 EKB（P1）。依次在高位类别树中进行这些处理，在密钥发行中心（KDC）中存储并管理最终被更新的全部的子 EKB。

在图 37 中示出高位类别树利用装置的排除处理进行更新处理而生成的有效化密钥块（EKB）的例子。

图 37 是说明在（a）的结构中在从包含排除装置的低位类别树接受了更新子 EKB 的高位类别树中生成的 EKB 的例子的图。包含排除装置的低位类别树的顶点节点与高位类别树的末端节点（node100）3601 相对应。

高位类别树更新从高位类别树的子根到末端节点（node100）3601 为止的通路上存在的节点密钥，生成新的更新子 EKB。更新子 EKB 如图 37（b）中所示。已被更新的密钥附以底线和〔′〕来示出。更新从以这种方式被更新了的末端节点到子根为止的通路上的节点密钥，作成该类别树中的更新子 EKB。

其次，说明将排除的对象作为类别树时的处理、即类别树的排除处理。

图 38（a）示出了类别树管理的密钥分配树结构。在树的最高位上设定根节点，在其几段下构成了类别树 A01～Ann，在其低位的段上构成了 B01～Bnk 的类别树，进而，在其低位的段上构成了类别树 C1～

Cn 的类别树。最下的类别树的末端节点（叶）假定是各个装置、例如记录播放器、专用播放器等。

在此，说明对类别树 Cn，3730 进行排除处理的情况。如图 38（b）中所示，最下段类别树 Cn，3730 是具有顶点节点 3431、在作为末端节点的叶上具有多个装置的结构。

通过排除类别树 Cn，3730，可进行属于类别树 Cn，3730 的全部的装置的与树结构脱离的一并排除。在作为类别树 Cn，3730 的高位类别树的类别树 Bnk，3720 中进行类别树 Cn，3730 的排除处理。类别树 Bnk，3720 是具有类别树 Cn，3730 的顶点节点 3731 作为末端节点的类别树。

类别树 Bnk，3720 在进行低位类别树 Cn，3730 的排除的情况下，更新与类别树 Cn，3730 的顶点节点 3731 对应的类别树 Bnk，3720 的末端节点 3731，再者，进行从该排除类别树 3730 到类别树 Bnk，3720 的子根为止的通路上的节点密钥的更新，生成有效化密钥块（EKB），生成更新子 EKB。程序更新对象的节点密钥是从图 38（c）的子根 3721 到构成排除类别树的顶点节点的末端节点 3731 的通路上的节点密钥。即，节点 3724、3725、3731 成为更新对象。更新这些各节点的节点密钥来生成类别树 Bnk，3720 的新的更新子 EKB。

或者，在类别树 Bnk，3720 在进行低位类别树 Cn，3730 的排除的情况下，也可不更新与类别树 Cn，3730 的顶点节点 3731 对应的类别树 Bnk，3720 的末端节点 3731，进行从该排除类别树 3730 到类别树 Bnk，3720 的子根为止的通路上的除了末端节点 3731 的节点密钥的更新，生成有效化密钥块，生成更新子 EKB。

再者，将类别树 Bnk，3720 更新了的有效化密钥块（子 EKB）发送给高位类别树。此时，高位类别树是类别树 Ann，3710，是具有类别树 Bnk，3720 的顶点节点 3721 作为末端节点的类别树。

如果类别树 Ann，3710 从低位类别树 Bnk，3720 接受有效化密钥块（子 EKB），则将与该密钥块中包含的 Bnk，3720 的顶点节点 3721 对应的 Ann，3710 的末端节点 3721 设定为在低位类别树 Bnk，3720 中已被更新的密钥，进行自身的类别树 Ann，3710 的子 EKB 的更新处理。在图 38（d）中示出类别树 Ann，3710 的树结构。在类别树 Ann，3710 中，成为更新对象的节点密钥是构成从图 38（d）的子根 3711

连接到发送了更新子 EKB 的类别树的节点 3721 上的通路的各节点 3711、3714、3715 的节点密钥。更新这些各节点的节点密钥来生成类别树 Ann，3710 的新的更新子 EKB。

在高位类别树中依次进行这些处理，进行到在图 30（b）中已说明的根类别树为止。利用该一系列的处理，结束类别树的排除处理。再有，将在各自的类别树中已被更新的 EKB 最终发送给密钥发行中心（KDC）并由其进行保管。密钥发行中心（KDC）根据全部的类别树的更新子 EKB，生成各种各样的 EKB。更新 EKB 成为属于已被排除的类别树的装置中的不能解密的加密密钥块。

在图 39 中示出类别树的排除处理的顺序图。按照图 39 的顺序图来说明处理次序。首先，为了排除类别树管理类别树（E－En）内的排除对象的末端节点，打算排除类别树的类别树管理类别树（E－En）进行必要的密钥更新，生成类别树管理类别树（E－En）的新的子 EKB（E）。将更新子 EKB（E）发送给高位类别树。接受了更新子 EKB（E）的高位（亲）类别树（P1－En）生成更新了与更新子 EKB（E）的更新顶点节点对应的末端节点密钥和从其末端节点到子根的通路上的节点密钥的更新子 EKB（P1）。依次在高位类别树中进行这些处理，在密钥发行中心（KDC）中存储并管理最终被更新的全部的子 EKB。密钥发行中心（KDC）根据全部的类别树的更新子 EKB，生成各种各样的 EKB。更新 EKB 成为属于已被排除的类别树的装置中的不能解密的加密密钥块。

在图 40 中生成说明已被排除的低位类别树与进行了排除的高位类别树的对应关系的图，高位类别树的末端节点 3901 由于类别树的排除而被更新，由于从高位类别树的树中的末端节点 3901 到子根为止的通路上存在的节点密钥的更新，生成新的子 EKB。其结果，已被排除的低位类别树的顶点节点 3902 的节点密钥与高位类别树的末端节点 3901 的节点密钥成为不一致。由于根据在高位类别树中被更新的末端节点 3901 的密钥来生成在类别树的排除后由密钥发行中心（KDC）生成的 EKB，故不保有该更新密钥的与低位类别树的叶对应的装置不能进行由密钥发行中心（KDC）生成的 EKB 的解密。

再有，在上述的说明中，说明了管理装置的最下段的类别树的排除处理，但处于高位的类别树也可利用与上述同样的过程进行排除处

于树的中段的类别树管理类别树的处理。通过排除中段的实体管理类别树，可一并地排除属于已被排除的类别树管理类别树的低位的全部的多个类别树和装置。

这样，通过进行以类别树为单位的排除，与以 1 个 1 个的装置为单位进行到排除处理相比，可用简单的过程进行排除处理。

〔类别树的性能（capability）管理〕

其次，说明在以类别树为单位的密钥分配树结构中管理各实体所容许的性能（capability）、进行与性能对应的内容分配的处理结构。在此，所谓性能，指的是例如能进行特定的压缩声音数据的解密的性能，或容许特定的声音播放方式的性能，或能处理特定的图像处理程序的性能，或装置是能处理怎样的内容或程序等的装置、即装置的数据处理能力的定义信息。

在图 41 中示出定义了性能的类别树结构例。是根节点位于密钥分配树结构的最高的顶点上、多个类别树连接到下层、各节点具有 2 分支的树结构。在此，例如将类别树 4001 作为具有声音播放方式 A、B、C 的某一种方式的性能的类别树来定义。具体地说，例如在分配了用某个声音压缩程序 A、B 或 C 方式压缩的音乐数据的情况下，属于在类别树 4001 以下被构成的类别树的装置能进行恢复压缩数据的处理。

同样，将类别树 4002 作为具有能处理声音播放方式 B 或 C 的性能的类别树来定义，将类别树 4003 作为具有能处理声音播放方式 A 或 B 的性能的类别树来定义，将类别树 4004 作为具有能处理声音播放方式 B 的性能的类别树来定义，将类别树 4005 作为具有能处理声音播放方式 C 的性能的类别树来定义。

另一方面，将类别树 4021 作为容许图像播放方式 p、q、r 的类别树来定义，将类别树 4022 作为具有能实现方式 p、q 的图像播放方式的性能的类别树来定义，将类别树 4023 作为具有能实现方式 p 的图像播放的性能的类别树来定义。

在密钥发行中心（KDC）中管理这样的各类别树的性能信息。在打算对各种各样的装置分配例如某个内容提供者用特定的压缩程序进行了压缩的音乐数据的情况下，密钥发行中心（KDC）可根据各类别树的性能信息来生成只对于能播放该特定的压缩程序的装置能解密的

有效化密钥块（EKB）。提供内容的内容提供者利用根据性能信息生成的有效化密钥块（EKB）分配进行了加密的内容密钥，对各装置提供用该内容密钥进行了加密的压缩声音数据。利用该结构，能可靠地只对能进行数据的处理的装置提供特定的处理程序。

再有，在图 41 中是对于全部的类别树定义了性能信息的结构，但不一定需要象图 41 的结构那样对全部的类别树定义性能信息，也可例如象图 42 中所示那样作成下述的结构：只对与装置所属的最下段的类别树定义性能，在密钥发行中心（KDC）中管理属于最下段的类别树的装置的性能，根据由最下段的类别树定义了的性能信息生成只能在能进行内容提供者希望的处理的装置中进行解密的有效化密钥块(EKB)。在图 42 中，是在末端节点上定义了装置的类别树 4101－4105 中的性能被定义、在密钥发行中心（KDC）中管理关于这些类别树的性能的结构。例如，关于声音播放能进行方式 B 的处理和关于图像播放能进行方式 r 的处理的装置属于类别树 4101。关于声音播放能进行方式 A 的处理和关于图像播放能进行方式 q 的处理的装置属于类别树 4102 等。

在图 43 中示出在密钥发行中心（KDC）中管理的性能管理表的结构例。性能管理表具有图 43（a）那样的数据结构。类别树 ID 是用来识别各类别树的识别符。性能表表示对由类别树 ID 表示的类别树定义的性能。如图 43（b）中所示，性能表由多个位组成，每个位表示各种性能是否有效。例如，如果能处理声音数据播放处理方式（A），则该位为〔1〕，如果不能处理，则该位为〔0〕，如果能处理声音数据播放处理方式（B），则该位为〔1〕，如果不能处理，则该位为〔0〕…等。再有，该性能信息的设定方法，不限于这样的形式，只要能识别类别树的关于管理装置的性能，也可以是其它的结构。

在性能管理表中还存储各类别树的子 EKB，或在另外的数据库中存储了子 EKB 的情况下，在性能管理表中存储子 EKB 的识别信息，再者，还存储各类别树的子根节点识别数据。

密钥发行中心（KDC）根据性能管理表，例如生成只有能播放特定的内容的装置才能解密的有效化密钥块（EKB）。在图 44 中，说明基于性能信息的有效化密钥块的生成处理。

首先，在步骤 S4301 中，密钥发行中心（KDC）从性能管理表选

择具有被指定的性能的类别树。具体地说，例如内容提供者打算分配能播放基于声音数据播放处理方式 A 的数据的情况下，从图 43（a）的性能表中选择例如将声音数据播放处理（方式 A）的项目设定为〔1〕的 Y。

其次，在步骤 S4302 中，生成由已被选择的类别树构成的选择类别树 ID 的表。其次，在步骤 S4303 中，在由选择类别树 ID 构成的树中选择必要的通路（密钥分配树结构的通路）。在步骤 S4304 中，判定选择类别树 ID 的表中包含的全部的通路选择是否结束，到结束为止，在步骤 S4303 中生成通路。这意味着在选择了多个类别树的情况下依次选择各自的通路的处理。

如果选择类别树 ID 的表中包含的全部的通路选择结束，则进到步骤 S4305，构筑只由已选择的通路和选择类别树构成的密钥分配树结构。

其次，在步骤 S4306 中，进行在步骤 S4305 中生成的树结构的节点密钥的更新处理，生成更新节点密钥。再者，从性能管理表中取出构成树的选择类别树的子 EKB，根据子 EKB 和在步骤 S4306 中生成的更新节点密钥，生成只在选择类别树的装置中才能解密的有效化密钥块（EKB）。以这种方式生成的有效化密钥块（EKB）成为只在基于特定的性能的装置中才能利用、即才能解密的有效化密钥块（EKB）。用该有效化密钥块（EKB）例如对内容密钥进行加密，通过用该内容密钥对根据特定程序压缩了的内容进行加密来提供内容，只在由密钥发行中心（KDC）选择的能进行特定的处理的装置中利用内容。

这样，密钥发行中心（KDC）根据性能管理表生成例如只有能进行特定的内容的播放的装置才能解密的有效化密钥块（EKB）。因而，在登录了新的类别树的情况下，必须预先取得该新登录类别树的才能。使用图 45 说明伴随该类别树的新的登录的性能通知处理。

图 45 是示出了新的类别树参与到密钥分配树结构中时的性能通知处理顺序的图。

新附加在树结构中的新的（子）类别树（N－En）对高位（亲）类别树（P－En）进行新的登录要求。再有，各类别树保有按照公开密钥加密方式的公开密钥，新的类别树在登录要求时对高位（亲）类别树（P－En）发送自己的公开密钥。

接受了登录要求的高位（亲）类别树（P－En）将已接受的新的（子）类别树（N－En）的公开密钥转送给证明书发行局（CA），接受附加了 CA 的署名的新的（子）类别树（N－En）的公开密钥。这些手续作为高位（亲）类别树（P－En）与新的（子）类别树（N－En）的相互认证的手续来进行。

如果利用这些处理使新的登录要求类别树的认证结束，则高位（亲）类别树（P－En）许可新的（子）类别树（N－En）的登录，将新的（子）类别树（N－En）的节点密钥发送给新的（子）类别树（N－En）。该节点密钥是高位（亲）类别树（P－En）的末端节点的 1 个节点密钥，而且，与新的（子）类别树（N－En）的顶点节点、即子根密钥相对应。

如果该节点密钥的发送结束，则新的（子）类别树（N－En）构筑新的（子）类别树（N－En）的树结构，在已构筑的树的顶点上设定已接受的顶点节点的子根密钥，设定各节点、叶的密钥，生成类别树内的有效化密钥块（子 EKB）。另一方面，高位类别树（P－En）根据新的（子）类别树（N－En）的附加，也生成附加了有效化的末端节点的高位类别树（P－En）内的子 EKB。

如果新的（子）类别树（N－En）生成由新的（子）类别树（N－En）内的节点密钥、叶密钥构成的子 EKB，则将其发送给高位类别树（P－En），再者，将由自己的类别树管理的关于装置的性能信息通知高位类别树。

从新的（子）类别树（N－En）接受了子 EKB 和性能信息的高位类别树（P－En）将已接受的子 EKB 和性能信息以及高位类别树（P－En）的已更新的子 EKB 发送给密钥发行中心（KDC）。

密钥发行中心（KDC）将已接受的类别树的子 EKB 和性能信息登录在图 43 中已说明的性能管理表上，更新性能管理表。密钥发行中心（KDC）根据已更新的性能管理表可生成各种形态的 EKB、即只有具有特定的性能的类别树或装置才能解密的 EKB。

〔使用了 EKB 类型定义表的 EKB 的管理结构〕

其次，说明在生成 1 个以上的已选择的类别树中能解密的 EKB 并提供在属于各类别树的装置中可共同地使用的 EKB 的结构中使用了表示用哪个类别树能处理、即能解密的 EKB 类型定义表的结构。

在本结构中，密钥发行中心（KDC）从内容提供者等的希望 EKB 的使用、发行的 EKB 请求者接受 EKB 发行要求。在 EKB 发行要求中包含被 EKB 类型定义表定义的表示 EKB 类型的 EKB 类型识别编号，密钥发行中心（KDC）按照 EKB 类型识别编号生成在 1 个或多个类别树中能处理（解密）的 EKB。

在 EKB 的生成时，密钥发行中心（KDC）根据与 EKB 类型定义表的 EKB 类型识别编号对应地设定了的各类别树的顶部节点识别符，对作为类别树管理者的顶级类别实体（TLCE）要求子 EKB 的生成，接受各 TLCE 已生成的子 EKB，进行多个子 EKB 的合成处理，生成在多个类别树中能处理的 EKB。

在本结构中，内容提供者（CP）等的 EKB 的发行要求者能根据 EKB 类型定义表进行特定的类别树的选择。内容提供者（CP）等的 EKB 的发行要求者参照 EKB 类型定义表对密钥发行中心（KDC）要求在特定类别树中能处理的 EKB 的发行。密钥发行中心（KDC）根据 EKB 发行要求，对已被选择的类别树的管理实体进行子 EKB 发行要求，各被选择的类别树的管理实体生成只在管理实体的未被排除的正当的装置中能处理的子 EKB，发送给密钥发行中心（KDC）。密钥发行中心（KDC）组合 1 个以上的子 EKB，生成只在 EKB 的发行要求者所要求的选择类别树中能处理的 EKB，提供给 EKB 的发行要求者。EKB 的发行要求者从密钥发行中心（KDC）接受 EKB，进行只由 EKB 的处理能取得的密钥才能解密的加密密钥或加密内容的分配。

首先，简单地说明以下的说明中的结构实体。

密钥发行中心（KDC）发行有效化密钥块（EKB），管理关于已发行的 EKB 的 EKB 类型定义表。

顶级类别实体（TLCE）是管理某个类别树的实体。例如是记录装置的格式持有者。它管理类别树，生成管理下的类别树内的装置中能处理（解密）的 EKB、即子 EKB，对密钥发行中心（KDC）提出。

EKB 请求者例如是进行电子内容提供（ECD）服务的内容提供者（CP）等的对用户装置提供图像、声音、程序等各种各样的内容的实体或记录媒体的格式持有者，作为使用由 EKB 处理在提供内容的加密密钥中能取得的密钥的设定，提供内容、媒体。对密钥发行中心（KDC）要求此时使用的 EKB 的发行要求。

例如内容提供者（CP）使用密钥发行中心（KDC）的已生成的 EKB 的根密钥，对自己的内容进行加密来分配。记录媒体的格式持有者在记录媒体的制造时写入 EKB 后发布，使用该 EKB 的根密钥对被记录的内容进行加密。

（TLCE 和类别库的树管理）

关于 TLCE 和类别库的树管理，在前面进行了叙述，现在使用图 46 来说明顶级类别实体（TLCE）与类别树的关系。

首先，类别，如以上所述，是具有相同的性质的装置的集合，具体地说，是相同的厂家制造的装置或是处理相同的代码格式的装置等。在图 46 中，A、B、C、D 分别表示类别树。

在图 46 中，最上段的根树例如是 8 段结构（节点段数），在根树的最下段上设定类别树的顶点节点。类别树的多个可成为高位、低位的关系，在图 46 中，类别树 C 与类别树 D 的高位相对应。

将直接连接到最上段的根树上的类别树称为顶级类别树，将管理顶级类别树的实体称为顶级类别实体（TLCE）。在图 46 中，A、B、C 是顶级类别树，管理该 A、B、C 的实体是顶级类别实体（TLCE）。顶级类别实体（TLCE）基本上具有管理自己的树以下的全部的责任。即，图 46 的管理树 C 的 TLCE 也进行关于与树 C 同样的树 D 的管理。如果在 D 以下还存在下层的类别树，则也进行该下层类别树的管理。但是，也可设置例如管理下层的类别树 D 的类别实体，对其委托该责任和权利。

进行内容的利用的记录播放装置的各装置被顶级类别实体（TLCE）分配给某个树的叶，具有从该叶到根的通路间的几个节点的密钥。将 1 个装置具有的节点密钥的组称为装置节点密钥（DNK）。装置节点密钥（DNK）决定各装置具有几个密钥（在 DNK 中包含几个密钥）。

在图 47 中示出说明密钥发行中心（KDC）、顶级类别实体（TLCE）、EKB 请求者各实体的对应、处理的概要的图。

密钥发行中心（KDC）4511 位于使用了树结构的 EKB 分配系统的管理实体 4510 中。在管理实体 4510 中有进行对于 EKB 的署名处理的认证局（CA）4512。

密钥发行中心（KDC）4511 进行顶级类别树等的子树的密钥管理，

进行后述的 EKB 类型定义表的管理、EKB 的生成。认证局（CA）4512 在密钥发行中心（KDC）生成的 EKB 中进行署名，同时将与进行了署名的秘密密钥对应的公开密钥作为署名验证用的密钥来发行。

对密钥发行中心（KDC）4511 进行 EKB 的发行要求的是 EKB 请求者 4520。EKB 请求者是关于提供存储了内容的 CD、DVD 等的媒体的内容存储媒体的内容提供者（CP）、进行电子内容的分配的内容提供者（CP）、提供关于闪速存储器等的存储系统的格式的许可证的存储系统发许可证者等。

这些 EKB 请求者 4520 在各自的提供的媒体、内容、许可证使用时，与内容、媒体、许可证格式等对应地提供将必要的密钥作为由 EKB 处理得到的密钥来设定的 EKB。密钥发行中心（KDC）4511 按照从 EKB 请求者 4520 对于密钥发行中心(KDC)4511 的 EKB 发行要求来生成 EKB。

EKB 请求者 4520 将作为对于密钥发行中心（KDC）4511 的发行要求的结果而接受的 EKB 提供给媒体制造者 4540、装置制造者 4550，可进行将存储了 EKB 的媒体或装置供给用户的处理。这些 EKB 作为例如在 1 个或多个类别树中能处理的 EKB 来生成。

在本系统中，成为生成并使用在多个、例如 2 个或 3 个以上的类别树中能共同地处理的 EKB、或只能在唯一的类别树中处理的 EKB 等各种各样的类型的 EKB 的状况。对于这样的各种各样的类型的 EKB 进行列表处理的是 EKB 类型定义表。密钥发行中心（KDC）管理 EKB 类型定义表。在后面详细地说明 EKB 类型定义表。EKB 请求者 4520 对密钥发行中心（KDC）4511 生成 EKB 类型定义表并取得表，此外，在有表的数据变更的情况下，从密钥发行中心（KDC）4511 对 EKB 请求者 4520 进行通知。

顶级类别实体（TLCE）4530 如以上所述，是连接到根树上的类别树的管理实体，管理子树的密钥管理、管理装置 ID 与在各装置中被存储的 EKB 处理用的节点密钥组、即装置节点密钥（DNK）的对应表。再者，对制造与管理下的装置对应的装置的装置制造者 4550 进行装置存储用的装置节点密钥（DNK）的生成、提供处理。

如果密钥发行中心（KDC）4511 从 EKB 请求者 4520 接受 EKB 发行要求，则密钥发行中心（KDC）4511 生成按照发行要求的 EKB。在所生成的 EKB 例如是在 2 个顶级类别树中能处理的 EKB 的情况下，对该

2 个顶级类别实体（TLCE）4530 发送子 EKB 的发行要求，接受了子 EKB 的发行要求的顶级类别实体（TLCE）4530 生成在各自的类别树内的正当的装置能取得根密钥的子 EKB，发送给密钥发行中心（KDC）4511。密钥发行中心（KDC）4511 根据从 TLCE 接受的 1 个或多个子 EKB 生成 EKB。在后面进一步说明基于子 EKB 的 EKB 生成处理。

顶级类别实体（TLCE）4530 与 EKB 请求者 4520 同样对密钥发行中心（KDC）4511 要求 EKB 类型定义表的生成以便能取得表。

顶级类别实体（TLCE）4530 还可对密钥发行中心（KDC）4511 要求删除关于 EKB 类型定义表的自己的树被定义的类型。例如要求从表中删除作为与其它的类别树共有的 EKB 被定义的 EKB 类型。再者，顶级类别实体（TLCE）4530 在有关于自己管理的树的变更的情况下，将变更信息通知密钥发行中心（KDC）4511。在后面，使用流程图来说明这些处理。

装置制造者 4550 被区分为 2 个种类的装置制造者。1 个是制造在所制造的装置中存储了装置节点密钥（DNK）和 EKB 这两种数据的装置的 DNKE 装置制造者 4551，另 1 个是制造在装置中只存储了装置节点密钥（DNK）的装置的 DNK 装置制造者 4552。

在图 48 中将在图 47 中生成的密钥发行中心（KDC）、EKB 请求者、顶级类别实体（TLCE）各自的结构例作为框图来示出。密钥发行中心（KDC）作为 EKB 发行信息处理装置来构成，EKB 请求者作为 EKB 要求信息处理装置来构成，顶级类别实体（TLCE）作为类别树管理信息处理装置来构成，基本上作为可进行密码通信的数据处理装置来构成。

构成各实体的信息处理装置具有分别承担与其它的实体的相互认证、数据通信时的密码处理整体的密码处理部。密码处理部内的控制部是进行关于认证处理、加密/解密处理等的密码处理整体的控制的控制部。内部存储器存储相互认证处理、加密、解密处理等各种处理中必要的密钥数据、识别数据等。在例如与其它实体的相互认证处理中使用识别数据。

加密/解密部进行使用了在内部存储器中存储的密钥数据等的数据传送时的认证处理、加密处理、解密处理、数据的验证、随机数的发生等的处理。

但是，在作为 EKB 请求者的信息处理装置中，也可作成在自身的

装置内不进行密钥的生成处理的结构。此时，可省略在密钥的生成中所必要的构成要素、例如随机数发生装置等。具体地说，作为自身生成在 EKB 中包含的根密钥、对密钥发行中心要求包含已生成的根密钥的 EKB 的生成的 EKB 请求者的信息处理装置必须有生成根密钥用的装置，但作为自身不生成在 EKB 中包含的根密钥、对密钥发行中心要求根密钥的生成处理、对密钥发行中心要求包含在密钥发行中心（KDC）中生成的根密钥的 EKB 生成的 EKB 请求者的信息处理装置可省略随机数发生装置等的伴随密钥生成处理的构成要素。

由于密码处理部的内部存储器保持了密码密钥等的重要的信息，故必须作成难以从外部不正当地读出的结构。因而，密码处理部作为用具有难以从外部进行存取的结构的例如半导体芯片构成的抗干扰存储器来构成。

各实体除了这些密码处理功能外，还具备中央运算处理装置（CPU）、RAM（随机存取存储器）、ROM（只读存储器）、输入部、显示部、数据库 I/F、数据库。

中央运算处理装置（CPU）、RAM（随机存取存储器）、ROM（只读存储器）是起到各实体本体的控制系统的功能的构成部。RAM 作为在 CPU 中的各种处理用的主存储器来使用，作为由 CPU 进行的处理用的操作区来使用。ROM 存储在 CPU 中的启动程序等。

在构成各实体的信息处理装置的数据库或其它的存储器中分别存储各实体所管理的数据，此外，在顶级类别实体（TLCE）的数据库中存储管理装置与装置节点密钥（DNK）的对应等属于类别树的装置的管理数据，在 EKB 请求者的数据库中存储使提供内容与对内容使用了的 EKB 的关系相对应的管理数据、关于内容的提供目的地的管理数据等。再有，最好将 EKB 类型定义表作成也存储在构成 EKB 请求者、顶级类别实体（TLCE）的信息处理装置中可参照的状态的结构。或者，也可作成放置于 EKB 请求者、顶级类别实体（TLCE）的可存取的密钥发行中心（KDC）管理的 Web 地点中的结构。

如上所述，装置为了 EKB 处理（解密）而使用装置节点密钥（DNK）。使用图 49 说明 1 个装置具有的装置节点密钥（DNK）。图 49 中生成的树表示 1 个类别树，最下段是与装置对应的叶，例如相当于顶级类别实体（TLCE）的管理树。根树（ex.8 段结构）连接到其上段上。在此，

装置如图 49 中所示，具有从装置到上段的通路上的节点密钥。将这些密钥组作为装置节点密钥（DNK）来保有，使用装置节点密钥（DNK）进行 EKB 的解密。

基本上说，以在 1 个叶上不重叠的方式来分配 1 个装置。作为例外，在例如使 PC 软件等的软件与叶相对应的情况下，也有将 1 个版本的软件包全部分配给 1 个叶的情况。这一点也由 TLCE 来决定。即，TLCE 决定怎样将装置分配给叶，使其具有哪个节点密钥。

也有顶级类别实体（TLCE）是装置自身的提供者的情况。对于制造装置来说，可预先存储装置节点密钥（DNK）来提供（销售）给用户。即，对记录播放装置等的装置来说，将某个特定的类别树的节点密钥组作为装置节点密钥（DNK）存储在存储器中来提供（销售）给用户。

（EKB 类型定义表）

关于以类别为单位的 EKB 分配，如已经说明的那样，但在生成并发行在多个类别中共同的 EKB、即在属于不同的类别树的装置中能处理的 EKB 的情况下，有时发生几个问题。

例如，作为某个可进行再次写入的媒体（记录媒体）、例如携带型闪速存储器的格式的许可证接收者，存在 A 公司和 B 公司不同的 2 个公司，作为媒体（携带型闪速存储器）的发许可证者（许可证许诺者）的厂家作为顶级类别而存在，在其下有 A 公司管理的类别树和 B 公司管理的类别树的结构中，A 公司和 B 公司使彼此的装置具有互换性，可共同地利用各种各样发布的内容，因此，在密钥发行中心（KDC）中生成并发行在 A 公司的类别树和 B 公司的类别树的 2 个类别树所属的装置中能处理（解密）的 EKB。

在这样的状况下，如果属于 A 公司管理的类别树的 1 个装置的装置节点密钥（DNK）泄漏了，则会发生利用该装置节点密钥（DNK）在 A 公司、B 公司的彼此的装置中可利用的发布内容全部被不正当地利用的可能性。为了排除该利用的可能性，必须进行作为排除处理的 EKB 更新处理，但此时，不单单是进行对于 A 公司的类别树的排除处理，由于在 A 公司和 B 公司这 2 个类别树中存在共同的 EKB，故必须对于 A 公司和 B 公司的 2 个类别树进行 EKB 更新处理。

这样，在对多个类别树生成并提供了共同的 EKB 的情况下，不仅

进行 1 个类别树内的排除处理、EKB 更新处理，而且必须在使用共同的 EKB 的全部的其它的类别树中进行伴随排除的 EKB 更新处理。以 B 公司来说，就受到与自己管理的装置不同的其它的管理类别树的影响，其处理负担加重了。

为了解决这样的状况，作成具有管理各自的类别的类别实体的结构，该类别实体被赋予在多个类别中能共同地使用的 EKB 的发行的许可权限。即，为了取得互换性，只在能容许因属于对方的类别的装置的不良情况引起的对自身的类别内装置的危险的情况下，才承认取得互换性的 EKB 的发行，在不能容许上述的危险的情况下，假定不承认能共同地使用的 EKB 的发行或使用。

如果打算进行这样的处理，则成为生成、使用在多个、例如 2 个或 3 个以上的类别树中能共同地处理的 EKB 或只能在唯一的类别树中处理的 EKB 等各种各样的 EKB。对于这样的各种各样的类型的 EKB 进行列表处理的是 EKB 类型定义表。在图 50 中示出 EKB 类型定义表的例子。密钥发行中心（KDC）在记录媒体上记录并管理 EKB 类型定义表。此外，根据需要，对于 EKB 请求者、TLCE，也处于能提供或阅览的状态。

如图 50 中所示，EKB 类型定义表具有「EKB 类型识别编号」、「节点」、「说明」的各区段，「EKB 类型识别编号」是识别被 EKB 类型定义表列出的各种形态的 EKB 的编号，如果识别号不同，则成为能处理该 EKB 的类别树或其组合不同的结构。

「节点」区段是记录能应用 EKB 的类别树的顶部节点 ID 的区段。例如记录 EKB 类型识别编号为 1 的 EKB 的 MS（存储器 stick）的类别树的顶部节点 ID。此外，记录 EKB 类型识别编号为 3 的 EKB 的 MS（存储器 stick）的类别树的顶部节点 ID 和 PHS 的类别树的顶部节点 ID。

「说明」区段是记录被 EKB 类型定义表列出的各种形态的 EKB 的说明的区段，例如示出了 EKB 类型识别编号为 1 的 EKB 是 MS（存储器 stick）用的 EKB。此外，示出了 EKB 类型识别编号为 3 的 EKB 是 MS（存储器 stick）和 PHS 的类别树的装置中能共同地使用的 EKB。

密钥发行中心（KDC）管理在图 50 中生成的 EKB 类型定义表。此外，打算进行由利用 EKB 的处理能取得的密钥进行了加密的加密密钥或加密内容等的加密数据分配的实体、例如内容提供者，参照图 50

中示出的 EKB 类型定义表，选择由包含成为内容的提供对象的装置的类别树能处理的 EKB 类型，指定其 EKB 类型识别编号，要求密钥发行中心（KDC）进行 EKB 生成处理。

但是，在对于 EKB 类型定义表的各种类型的 EKB 登录处理中，必须有成为登录对象的顶级类别实体（TLCE）的承认。例如，如果类别树 A 的 TLCE－A 拒绝与其它的类别共有的 EKB 的发行，则类别树 A 与其它的类别树共有的 EKB 的类型不登录在 EKB 类型定义表上。

例如，如果承认类别树 A 的 TLCE－A、类别树 B 的 TLCE－B、类别树 C 的 TLCE－C 分别共有的 EKB 的发行，则在 EKB 类型定义表上登录在这 3 个类别树中能处理的共同的 EKB 的类型，例如内容提供者指定表示该登录类型的 EKB 类型识别编号，可对密钥发行中心（KDC）要求 EKB 生成处理。

即，为了在 EKB 类型定义表上登录新的 EKB 类型，定义与该 EKB 类型对应的 EKB 类型识别编号，必须进行下述的处理。

（1）管理成为与打算定义的 EKB 类型识别编号对应的 EKB 的应用对象的类别的全部的 TLCE 将 EKB 类型定义表发送给密钥发行中心（KDC）。

（2）密钥发行中心（KDC）在确认了能处理成为有要求的登录对象的 EKB 的 1 个以上的顶级类别实体（TLCE）的全部发送了上述的 EKB 类型定义表后，定义新的 EKB 类型识别编号，将其增加到 EKB 类型定义表中。

（3）密钥发行中心（KDC）为了通知在 EKB 类型定义表中有变更这一点，将 EKB 类型定义表变更通知发送给全部的 TLCE 和 EKB 请求者。

再有，通过将 EKB 类型定义表发送给全部的 TLCE 和 EKB 请求者以及将其放置于 Web 地点上等，对全部的 TLCE 和 EKB 请求者公开 EKB 类型定义表。因而，TLCE 和 EKB 请求者可常时地区段登录在最新的 EKB 类型定义表上的 EKB 类型信息。

（EKB 类型登录处理）

在图 51 中示出说明在 EKB 类型定义表上登录新的 EKB 类型时密钥发行中心（KDC）进行的处理的处理流程。首先，密钥发行中心（KDC）接受（S101）来自进行新的 EKB 类型的登录要求的 TLCE 的 EKB 类型

登录请求。在来自 TLCE 的 EKB 类型登录请求中包含能共同地使用登录要求 EKB 的类别数。密钥发行中心（KDC）判定（S102）是否从对应于与要求内的类别数一致的数目的类别的 TLCE 接受了同样的 EKB 类型登录请求，以受理了来自对应于与要求内的类别数一致的数目的类别的 TLCE 的要求为条件，对于 EKB 类型定义表登录按照要求的新的 EKB 类型，进行表的更新处理、表的更新通知处理（S103）。对于 TLCE 和 EKB 请求者进行更新通知处理。

这样，密钥发行中心（KDC）在对于 EKB 类型定义表的 EKB 类型识别符的新的登录处理中，以管理作为能处理预定登录的 EKB 类型的已被选择的 1 个以上的类别树的全部的类别实体的承认为条件，进行登录。

再有，在这些处理中，在密钥发行中心（KDC）与 TLCE、EKB 请求者间的通信中，根据需要进行相互认证处理、发送数据的加密处理。此外，也可作成进行其它的消息加密处理、数字署名的生成、验证处理的结构。再有，在进行基于公开密钥密码方式的认证或密码通信的情况下，在各实体间预先进行互相保有公开密钥的手续。

（EKB 类型无效化处理）

例如，在必须排除属于某个类别的全部的装置时，顶级类别实体（TLCE）必须对密钥发行中心（KDC）提出使该类别成为要素的 EKB 类型无效化的要求。此外，顶级类别实体（TLCE）以例如停止某个服务等的理由对 KDC 提出使现在登录的 EKB 类型无效化的要求。

按照图 52 的处理流程署名该 EKB 类型无效化处理的流程。密钥发行中心（KDC）接受（S201）来自进行 EKB 类型的无效化要求的 TLCE 的 EKB 类型无效化请求。如果接受来自 TLCE 的 EKB 类型无效化请求，则密钥发行中心（KDC）在确认了管理成为被该请求而无效化的 EKB 类型的要素的类别的 TLCE 是该请求的发送者这一点的基础上，使与在 EKB 类型定义表内的无效化请求中被指定的类型对应的 EKB 类型识别编号无效化，更新 EKB 类型定义表，进行表的更新通知处理（S202）。对于 TLCE 和 EKB 请求者进行更新通知处理。

这样，密钥发行中心（KDC）在 EKB 类型定义表上登录的 EKB 类型识别符的无效化处理中，以管理作为能处理预定无效化的 EKB 类型的类别树而被选择的 1 个以上的类别树的至少 1 个的类别实体的无效

化要求为条件，进行无效化处理。此时，不需要其它的类别实体的承认。

再有，在这些处理中，在密钥发行中心（KDC）与 TLCE、EKB 请求者间的通信中，根据需要进行相互认证处理、发送数据的加密处理。此外，也可作成进行其它的消息加密处理、数字署名的生成、验证处理的结构。再有，在进行基于公开密钥密码方式的认证或密码通信的情况下，在各实体间预先进行互相保有公开密钥的手续。

（EKB 类型定义表变更通知处理）

例如在某个类别树内管理类别树的 TLCE 进行了装置排除或使将某个装置存储了的 DNK 更换为新的 DNK 的装置节点密钥（DNK）的更新等的树内的状态变化的处理的情况下，必须对使用了以这些装置为对象的 EKB 的 EKB 请求者或关联 TLCE 通知已进行了这些处理的情况。

之所以如此，是因为，如果不对其通知已进行了装置排除的情况，内容提供者（CP）就继续使用老的 EKB 对内容进行加密来分配，则即使在已被排除的装置中也能使用老的 EKB 进行 EKB 处理（解密），存在继续进行内容的不正当利用的可能性。此外，在进行了装置节点密钥（DNK）的更新的情况下，通常舍弃已被取代的老的 DNK，装置具有新的 DNK，但如果内容提供者不使用与该新的 DNK 对应的 EKB，则具有新的 DNK 的装置就不能对 EKB 进行处理（解密），不能对内容进行存取。

为了避免这样的弊病，

*作为装置排除等的结果，在 EKB 的标识符部分中产生了变更的情况下，

*作为装置节点密钥（DNK）的更新等的结果，在至少 1 个装置具有的 DNK 的值中产生了变更的情况下，

在这些情况下，TLCE 必须将树变更通知发送给密钥发行中心（KDC）。在树变更通知中包含在需要变更的 EKB 类型定义表上登录完的 EKB 类型识别编号、表示与 EKB 类型识别编号对应地被登录的哪个类别中引起了变更的信息和表示引起了排除、DNK 的更新的哪一个的信息。

按照图 53 的处理流程说明 EKB 类型定义表变更通知处理的流程。密钥发行中心（KDC）从 TLCE 接受（S301）树变更通知。如果接受来

自 TLCE 的树变更通知，则密钥发行中心（KDC）从 EKB 类型定义表抽出具有该类别作为要素的 EKB 类型识别编号，对于全部的 TLCE 和 EKB 请求者进行具有在哪个 EKB 类型识别编号中引起了怎样的变化（是排除还是 DNK 更新（替代））的信息的 EKB 类型定义表变更通知处理。再有，在这些处理中，在密钥发行中心（KDC）与 TLCE、EKB 请求者间的通信中，根据需要进行相互认证处理、发送数据的加密处理。此外，也可作成进行其它的消息加密处理、数字署名的生成、验证处理的结构。再有，在进行基于公开密钥密码方式的认证或密码通信的情况下，在各实体间预先进行互相保有公开密钥的手续。

（EKB 类型定义表要求）

顶级类别实体（TLCE）或 TLCE 以外的子类别实体（SCE）或内容提供者等的 EKB 请求者为了知道最新版的 EKB 类型定义表，可对密钥发行中心（KDC）要求 EKB 类型定义表的发送。密钥发行中心（KDC）对于该要求，将最新版的 EKB 类型定义表发送给要求者。

按照图 54 的处理流程说明 EKB 类型定义表要求处理的流程。密钥发行中心（KDC）从 TLCE、子类别实体或 EKB 请求者的某一个接受（S401）EKB 类型定义表要求。如果接受 EKB 类型定义表要求，则密钥发行中心（KDC）抽出最新的 EKB 类型定义表，对进行了要求处理的实体发送（S402）最新的 EKB 类型定义表。再有，在这些处理中，在密钥发行中心（KDC）与 TLCE、EKB 请求者间的通信中，根据需要进行相互认证处理、发送数据的加密处理。此外，也可作成进行其它的消息加密处理、数字署名的生成、验证处理的结构。再有，在进行基于公开密钥密码方式的认证或密码通信的情况下，在各实体间预先进行互相保有公开密钥的手续。

（EKB 发行处理）

根据 EKB 请求者的 EKB 发行要求来进行 EKB 发行处理。EKB 请求者是〔a〕CD、DVD 等的提供内容存储媒体的内容提供者（CP）、〔b〕提供电子信息分配（ECD）服务的内容提供者、〔c〕记录系统的格式持有者等使用由 EKB 的解密取得的密钥提供能进行内容的利用、格式的使用的服务、媒体、装置的实体。

在上述的〔c〕记录系统的格式持有者中，有〔c1〕例如在制造时在记录媒体中存储 EKB 那样的格式中，对记录媒体供给已取得的 EKB

的格式持有者、〔c2〕例如在制造时在记录装置中存储 EKB 那样的格式中，对记录装置供给已取得的 EKB 的格式持有者这 2 种格式持有者。

以下说明 EKB 发行处理的手续。

（1）内容密钥的作成

首先，内容提供者等的 EKB 请求者生成与自己提供的内容、装置、媒体对应地被使用的内容密钥。

例如在 EKB 请求者是〔a〕CD、DVD 等的提供内容存储媒体的内容提供者（CP）、〔b〕提供电子信息分配（ECD）服务的内容提供者的情况下，所生成的内容密钥作为在媒体上或电子信息分配（ECD）服务中保护内容（加密）的密钥来使用。

此外，在 EKB 请求者是〔c1〕例如在制造时在记录媒体中存储 EKB 那样的格式中对记录媒体供给已取得的 EKB 的格式持有者的情况下，内容密钥作为保护在该记录媒体上被记录的内容（加密）的密钥来使用。

再者，在 EKB 请求者是〔c2〕例如在制造时在记录装置中存储 EKB 那样的格式中对记录装置供给已取得的 EKB 的格式持有者的情况下，内容密钥作为保护在该记录装置上被记录的内容（加密）的密钥来使用。

再有，在各个格式中可任意地决定使用内容密钥来保护内容用的密码算法等的机理。

（2）根密钥的生成

EKB 请求者生成由 EKB 的解密处理能取得的根密钥。再有，EKB 请求者也可自身不生成根密钥、而是要求密钥发行中心（KDC）生成根密钥。根密钥是为了保护（加密）内容密钥而使用的。再有，在各个格式中可任意地决定使用根密钥来保护内容密钥用的密码算法等的机理。

（3）EKB 发行要求

EKB 请求者将 EKB 的发行要求发送给密钥发行中心（KDC）。

在该请求中包含上述的根密钥和由 EKB 将根密钥送给哪个类别的装置这样的在 EKB 类型定义表上被登录的 EKB 类型识别编号的一个。EKB 请求者根据自身的装置的存储器中已存储的 EKB 类型定义表或从网络上的可阅览的地点取得的 EKB 类型定义表，选择由包含成为提供

内容提供等的服务的对象的类别构成的 EKB 类型，将表示已选择的 EKB 类型的 EKB 类型识别编号包含在 EKB 发行要求中，发送给密钥发行中心（KDC）。

（4）EKB 发行处理

密钥发行中心（KDC）根据来自 EKB 请求者的 EKB 发行要求，在 EKB 发行要求中包含根密钥的情况下，进行包含该根密钥的 EKB 的生成，在 EKB 发行要求中不包含根密钥并进行了根密钥生成处理依赖的情况下，KDC 生成根密钥，生成包含生成根密钥的 EKB，发送给 EKB 请求者。

密钥发行中心生成的 EKB 有在单一的类别树中能处理的 EKB 的情况和在多个类别树中能共同地处理的 EKB 的情况。密钥发行中心（KDC）根据在 EKB 发行要求中包含的 EKB 类型识别编号，抽出在成为该 EKB 类型识别编号的构成要素的类别、即 EKB 类型定义表中被指定的 EKB 类型识别编号的节点区段中被记录的节点。在节点区段中记录了类别树的顶部节点 ID。这是与该类别树的管理实体对应的节点 ID。根据该节点 ID，对作为类别树的管理实体的顶级类别实体（TLCE）提出子 EKB 的发行要求。在子 EKB 的发行要求中包含表示根密钥和各类别的信息。

从密钥发行中心（KDC）接受了 EKB 发行要求的 TLCE 生成具有从被指定的 1 个以上的类别内的（未被排除）的各装置最终地能得到根密钥的结构的子 EKB，发送给密钥发行中心（KDC）。

顶级类别实体（TLCE）生成的子 EKB 是除了不具有版本编号或其验证用的信息（版本检验值）外具有与通常的 EKB（参照图 6）同样的结构的信息组。在此，可每个在生成子 EKB 的 TLCE（格式持有者）中任意地决定使用子 EKB 中的叶密钥或节点密钥对高位的节点密钥或根密钥进行加密的算法或密钥长度、模式。由此，可使用与其它的格式不同的独自的安全方式。此外，也可例如将密码算法决定为 FIPS46－1 的三次 DES，作成与其没有矛盾的 TLCE 应用三次 DES 算法的结构。即使在 TLCE 任意地决定密码算法或密钥长度的情况下，也决定用规定的长度、例如 16 字节的数据来表示一个一个的（被加密了的）密钥，以便即使在处于其它的 TLCE 的支配下的装置也能处理与另外的 TLCE 作成了的子 EKB 合成的 EKB。在以这种方式生成在多个类别树中

共同地 EKB 的情况下，通过按照规定的规则设定数据，不同的类别树的各装置可判断依据 EKB 的标识符自身需要第几个密钥数据。即，EKB 内包含的密钥数据的每一个只要是 16 字节，就可依次抽出用自身的装置能处理的密钥数据来处理，最终可取得根密钥。

即，根据子 EKB 生成的合成 EKB 具有多个密钥数据的每一个被存储在固定长度的数据区段内的结构。因而，即使根据分别具有独自的算法、独自的密钥数据长度的子有效化密钥块（子 EKB）生成的合成 EKB 根据密钥树中的节点或叶位置对子 EKB 内的多个加密密钥数据进行再次排列来生成，也可依据 EKB 的标识符依次取得必要的密钥数据。将这样的合成 EKB 经网络或存储在各种各样的记录媒体中，分配给或提供给用户（装置）。

密钥发行中心（KDC）根据需要对从 TLCE 发送来的子 EKB 进行重新组合、合成，附加版本编号和其验证用的信息，完成合成了的合成 EKB，发送给 EKB 请求者。但是，也有要求与密钥发行中心（KDC）不同的其它的认证局（CA）进行使用了公开密钥密码技术的数字署名的情况。

参照图，说明子 EKB 的生成、从子 EKB 到合成 EKB 的生成。图 55 是说明在生成在类别树 A，5100 和类别树 B，5200 中共同的合成 EKB 的处理中类别树 A，5100 的 TLCE 生成的子 EKB－（A）的结构的图。子 EKB－（A）作为类别树 A，5100 的各装置能取得根密钥的 EKB 而被生成。再有，在图中，根树区 5300 在上述的说明中作为 8 段结构来说明，但在此为了简化说明起见，作成 2 段结构。

在图 55 中，附加了树结构内记载的下线的 3 位的数值〔XXX〕表示 EKB 内的标识符（e、l、r），如上（参照图 26、27）所述，e＝1 表示有数据，e＝0 表示没有数据，l＝1 表示在左边没有分支，l＝0 表示在左边有分支，r＝1 表示在右边没有分支，r＝0 表示在右边有分支。

图 55 的类别树 A，5100 的各装置（叶）为了取得根密钥，生成存储了由各叶共同地存储了的节点密钥对根密钥进行了加密的数据的 EKB 即可。由于各装置保有了图 55 的类别树 A，5100 的装置节点密钥（DNK）区 5120 的树的各通路的节点密钥，故生成用 DNK 区 5120 的最上段的节点密钥对根密钥进行了加密的 EKB 即可。

因而，类别树 A，5100 的 TLCE 生成的子 EKB－（A）成为标识符部分为 101，010，000，111，111、密钥部分为 Enc（K010，Kroot），Enc（K011，Kroot）的子 EKB－（A）。类别树 A，5100 的 TLCE 将该子 EKB－（A）发送给密钥发行中心（KDC）。

其次，使用图 56 说明类别树 B，5200 生成的子 EKB－（B）。类别树 B，5200 的各装置（叶）为了取得根密钥，生成存储了利用各叶共同地存储了的节点密钥对根密钥进行了加密的数据的 EKB 即可。由于各装置保有了图 56 的类别树 B，5200 的装置节点密钥（DNK）区 5220 的树的各通路的节点密钥，故生成用 DNK 区 5220 的最上段的节点密钥对根密钥进行了加密的 EKB 即可。

因而，类别树 B，5200 的 TLCE 生成的子 EKB－（B）成为标识符部分为 110，010，000，111，111、密钥部分为 Enc（K110，Kroot），Enc（K111，Kroot）的子 EKB－（B）。类别树 B，5200 的 TLCE 将该子 EKB－（B）发送给密钥发行中心（KDC）。

密钥发行中心从各 TLCE 生成的子 EKB－（A）和子 EKB－（B）生成合成 EKB。使用图 57 说明合成 EKB 的生成。合成 EKB 作为属于类别树 A，5100 和类别树 B，5200 的各树的装置能取得根密钥的 EKB 来构成。基本上说，混合已接受的多个子 EKB 的密钥数据排列、利用从树的上段起进行对齐的操作来生成合成 EKB。再有，在同一段中，进行以左侧为开头的数据排列。

其结果，合成 EKB 作为具有下述的部分的 EKB 来生成：标识符部分为 100，010，010，000，000，111，111，111，111、密钥部分为 Enc（K010，Kroot），Enc（K011，Kroot），Enc（K110，Kroot），Enc（K111，Kroot）。各密钥部分的密钥数据通过如上所述分别例如作为 16 字节来设定，由于各类别树内的装置可检测出能利用自身的装置来处理的密钥数据位置，故能从合成 EKB 取得根密钥。

以上所述是在哪一个类别树中都没有被排除的装置的情况的子 EKB 的生成和合成 EKB 的生成处理结构，其次说明有排除装置的情况的子 EKB 的生成和合成 EKB 的生成。

图 58 是说明在类别树 A，5100 中存在排除装置（01101）5150 时的子 EKB 的生成。此时的子 EKB 作为只是不能处理排除装置（01101）5150 的子 EKB－（A′）来生成。

此时，就生成具有连接了用图的粗线示出的通路的密钥数据结构的子 EKB。因而，类别树 A，5100 的 TLCE 生成的子 EKB－（A′）成为标识符部分为 101，010，000，111，000，001，111，111、密钥部分为 Enc（K010，Kroot），Enc（K0111，Kroot），Enc（K01100，Kroot）的子 EKB－（A′）。类别树 A，5100 的 TLCE 将该子 EKB－（A′）发送给密钥发行中心（KDC）。

密钥发行中心从各 TLCE 生成的子 EKB－（A′）和从没有排除装置的子 EKB－（B）的 TLCE 接受了的子 EKB－（B）生成合成 EKB。使用图 59 说明合成 EKB 的生成。合成 EKB 作为属于类别树 A，5100 的除了排除装置（01101）5150 的装置和属于类别树 B，5200 的树的装置能取得根密钥的 EKB 来构成。基本上说，混合已接受的多个子 EKB 的密钥数据排列、利用从树的上段起进行对齐的操作来生成合成 EKB。再有，在同一段中，进行以左侧为开头的数据排列。

其结果，合成 EKB 作为具有下述的部分的 EKB 来生成：标识符部分为 100，010，010，000，000，111，000，111，111，001，111，111、密钥部分为 Enc(K010,Kroot),Enc(K110,Kroot),Enc(K111,Kroot),Enc（K0111，Kroot），Enc（K01100，Kroot）。该合成 EKB 是属于类别树 A，5100 的除了排除装置（01101）5150 的装置和属于类别树 B，5200 的树的装置能取得根密钥的 EKB。

（5）EKB 的利用

将密钥发行中心(KDC)利用上述那样的处理生成的 EKB 发送给 EKB 请求者。

例如在 EKB 请求者是〔a〕CD、DVD 等的提供内容存储媒体的内容提供者（CP）、〔b〕提供电子信息分配（ECD）服务的内容提供者的情况下，利用由 EKB 能取得的根密钥对内容密钥进行加密、用内容密钥对提供给用户装置的内容进行加密以使内容流通。利用该结构，只有属于 EKB 能处理的特定的类别树的装置才能利用内容。

此外，在 EKB 请求者是〔c1〕例如在制造时在记录媒体中存储 EKB 那样的格式中对记录媒体供给已取得的 EKB 的格式持有者的情况下，对记录媒体制造业者提供用根密钥加密了的内容密钥，记录媒体制造业者或 EKB 请求者制造存储了用 EKB 和根密钥进行了加密的内容密钥的记录媒体并使其流通。利用该结构，只有属于 EKB 能处理的特定的

类别树的装置才能进行利用了记录媒体的 EKB 的内容记录播放时的加密处理、解密处理。

再者，在 EKB 请求者是〔c2〕例如在制造时在记录装置中存储 EKB 那样的格式中对记录装置供给已取得的 EKB 的格式持有者的情况下，对记录装置制造业者提供用根密钥加密了的内容密钥，记录装置制造业者或 EKB 请求者制造存储了用 EKB 和根密钥进行了加密的内容密钥的记录装置并使其流通。利用该结构，只有属于 EKB 能处理的特定的类别树的装置才能进行利用了 EKB 的内容记录播放时的加密处理、解密处理。

利用以上那样的处理来发行 EKB。再有，在 EKB 发行处理过程中的各实体、EKB 请求者、密钥发行中心（KDC）、TLCE 间的通信中，根据需要进行相互认证处理、发送数据的加密处理。此外，也可作成进行其它的消息加密处理、数字署名的生成、验证处理的结构。再有，在进行基于公开密钥密码方式的认证或密码通信的情况下，在各实体间预先进行互相保有公开密钥的手续。

（将子 EKB 的单纯集合定为合成 EKB 的结构例）

在从上述的子 EKB 生成合成 EKB 的处理中，对各个子 EKB 中包含的加密密钥数据的排列以从整个树的上段至下段的方式进行了重新排列的处理。其次，说明不进行这样的重新排列处理、而是按原样在合成 EKB 中依次存储了各类别树的 TLCE 生成的子 EKB 的结构。

图 60 是示出了以原有的形态存储了多个类别树的 TLCE 生成的多个子 EKB 的合成 EKB6000 的例子。

在 EKB 的发行处理中，密钥发行中心（KDC）对作为与由 EKB 请求者指定的 EKB 类型识别编号对应地在 EKB 类型定义表上记录了的类别树的管理实体的 TLCE 发行子 EKB 的生成要求，将从各 TLCE 提出的子 EKB6110、6120…简单地集中起来存储在合成 EKB 内。但是，附加各子 EKB 部分的大小（ex.数据范围）6111 和表示该子 EKB 是哪个类别用的数据（ex.节点 ID）6112，以便属于各类别的装置能从该合成 EKB 中选择与该装置能处理的自身的装置所属的类别对应的子 EKB。

即，在作为存储对象被选择的子 EKB 的每一个中，表示子 EKB 存储区的数据长度的范围和作为子 EKB 识别数据的各子 EKB 的对应类别树的节点识别符的节点 ID 对应地被存储。此外，附加合成 EKB 中包

含的子 EKB 的数目作为标题信息 6200。根据合成 EKB 的全部数据，生成并附加署名（ex.认证局（CA）的署名）。

如果按照本方式生成与使用上述的图 57 的说明对应的合成 EKB，则生成图 61 中示出的合成 EKB。子 EKB6110 的存储 EKB 是在图 55 中已说明的类别树 A 的 TLCE 生成的子 EKB－（A）本身，标识符部分为 101，010，000，111，111、密钥部分为 Enc（K010，Kroot），Enc（K011，Kroot）。此外，子 EKB6120 的存储 EKB 是在图 56 中已说明的类别树 B 的 TLCE 生成的子 EKB－（B）本身，标识符部分为 110，010，000，111，111、密钥部分为 Enc（K110，Kroot），Enc（K111，Kroot）。

此外，使用上述的图 58、图 59 已说明的有排除装置的情况的合成 EKB 成为图 62 中示出的数据结构。子 EKB6110 的存储 EKB 是在图 58 中已说明的类别树 A 的 TLCE 生成的子 EKB－（A′）本身，标识符部分为 101，010，000，111，000，001，111，111、密钥部分为 Enc（K010，Kroot），Enc（K0111，Kroot），Enc（K01100，Kroot）。此外，未发生排除装置的子 EKB6120 的存储 EKB 是在图 56 中已说明的类别树 B 的 TLCE 生成的子 EKB－（B）本身，标识符部分为 110，010，000，111，111、密钥部分为 Enc（K110，Kroot），Enc（K111，Kroot）。

通过采取这样的结构，属于各类别的装置可选择与自己的装置所属的类别对应的子 EKB 进行处理（解密）。因而，在各个类别（TLCE）中，可使用完全任意的密码算法或密钥长度来生成子 EKB。即，TLCE 可在不被其它的类别左右的情况下决定密码算法或密钥长度。

对于密钥发行中心（KDC）来说，可不对从各 TLCE 集合起来的子 EKB 的标识符和密钥数据部分进行分解、重新组合，可减轻负担。

得到了按照该方式的 EKB 的装置可找到自己所属的类别的子 EKB，通过用管理自身的装置的 TLCE 决定的独自的方法来处理该子 EKB，可得到根密钥。由于不需要知道处理其它的子 EKB 用的其它的类别的 TLCE 决定的方法、此外在子 EKB 中不需要用固定的长度来表示各自的密钥等的办法，故从理论上说，在任何大小的密钥中都能使用。

（排除处理－（1））

以下说明利用了能在多个类别中共同地使用的 EKB 的处理中的发生了排除时进行的处理。首先说明利用网络或媒体从外部接受了加密内容并使用由 EKB 取得的密钥取得内容密钥来进行内容的利用的情况

的排除处理。

一边参照图 63，一边进行说明。设想利用了在类别树 A，7100 和类别树 B，7200 中共同地被使用的 EKB7000 的状况。此外，关于在类别树 A，7100 和类别树 B，7200 中共同地被使用的 EKB7000，在 EKB 类型定义表中 EKB 类型识别编号被定义为＃1。

在这样的状况下，内容提供者利用网络或媒体提供了用内容密钥进行了加密的内容，属于类别树 A，7100 和类别树 B，7200 的装置使用 EKB7000 进行根密钥的取得、由根密钥的解密处理进行的内容密钥的取得、由内容密钥进行的加密内容的取得而利用了内容。

在该状况下，假定发觉了属于类别树 A，7100 的装置 A1，7120 的密钥数据的泄漏等的能进行不正当处理的状况，进行装置 A1，7120 的排除。

此时，类别树 A，7100 的 TLCE 对密钥发行中心（KDC）进行树变更通知（参照图 53），密钥发行中心（KDC）根据已接受的树变更通知，对管理下的各 TLCE、EKB 请求者进行通知。此时的通知只是告知接受了树变更通知，不进行 EKB 类型定义表的更新处理。

再有，也可作成只对作为利用了在发生了排除的类别树中能处理的 EKB 的实体的 EKB 请求者或只对管理应用了与发生了排除的类别树共有的 EKB 的其它的类别树的类别实体来进行基于排除发生的树变更通知的结构。为了进行该处理，密钥发行中心（KDC）保有使 EKB 类型识别编号与利用了该 EKB 类型的 EKB 请求者相对应的表作为发行完的 EKB 的利用者表。

以进行了排除处理的类别树的装置作为对象并进行了内容的分配的作为 EKB 请求者的内容提供者对密钥发行中心（KDC）进行 EKB 发行要求，使其生成只在排除处理对象以外的装置中能处理的更新了的 EKB。此时，作为 EKB 请求者的内容提供者指定作为在类别树 A，7100 和类别树 B，7200 中共同地使用的 EKB 的类型而被定义了的 EKB 类型识别编号＃1。此外，或是 EKB 请求者自身生成新的根密钥并发送给 KDC，或是要求 KDC 生成新的根密钥。

密钥发行中心（KDC）根据已被指定的 EKB 类型识别编号＃1，参照 EKB 类型定义表，根据对应的类别树的节点，对类别树 A，7100 和类别树 B，7200 的 TLCE 要求生成在正当的装置中能取得新的根密钥

的子 EKB。

类别树 A，7100 和类别树 B，7200 的 TLCE 根据要求分别生成子 EKB。此时，在类别树 A，7100 中生成只在排除了被排除的装置 A1，7120 的其它的装置中才能取得新的根密钥的子 EKB－（A）。如果在类别树 B，7200 中不存在被排除的装置，则生成在属于类别的全部的装置中能取得新的根密钥的子 EKB－（B）并发送给密钥发行中心（KDC）。

密钥发行中心（KDC）根据从各 TLCE 接受了的子 EKB，按照上述的方法生成合成 EKB，将已生成的 EKB 发送给 EKB 请求者（ex. 内容提供者）。

EKB 请求者（ex. 内容提供者）应用从密钥发行中心（KDC）接受了的新的 EKB，进行内容分配。具体地说，提供用内容密钥进行了加密的内容，用由 EKB 的解密得到的根密钥对内容密钥进行加密来提供。属于类别树 A，7100 和类别树 B，7200 的装置使用 EKB 进行根密钥的取得、由根密钥的解密处理进行的内容密钥的取得、由内容密钥进行的加密内容的取得而能利用内容。但是，类别树 A，7100 的排除装置 A1，7120 由于不能处理已被更新的 EKB 而不能利用内容。

再有，在上述的说明中，说明了在密钥发行中心（KDC）接受了来自 TLCE 的树变更通知的情况下、在该时刻不进行 EKB 类型定义表的更新处理的例子，但也可作成在 KDC 接受了树变更通知的时刻密钥发行中心（KDC）根据树变更信息进行 EKB 类型定义表的更新处理、EKB 更新处理、对各 EKB 请求者、TLCE 发送已被更新的 EKB 类型定义表的结构。

（排除处理－（2））

其次，说明例如在记录装置或记录媒体中存储了 EKB 的结构中假定用户对各种各样的内容进行加密而记录在记录媒体上并使用了从在记录装置或记录媒体中存储了在加密处理、解密处理中为必要的密钥的 EKB 取得的根密钥的所谓的自己记录型的形态中的伴随排除处理的处理。

一边参照图 64，一边进行说明。设想利用了在类别树 A，8100 和类别树 B，8200 中共同地被使用的 EKB8000 的状况。即，假定在类别树 A，8100 和类别树 B，8200 中共同地被使用的记录装置或记录媒体中存储共同的 EKB，用户进行了由利用了 EKB 的内容加密、解密处理

进行的内容记录播放。再有，关于在类别树 A，8100 和类别树 B，8200 中共同地被使用的 EKB8000，假定在 EKB 类型定义表中 EKB 类型识别编号被定义为＃1。

在该状况下，假定发觉了属于类别树 A，8100 的装置 A1，8120 的密钥数据的泄漏等的能进行不正当处理的状况，进行装置 A1，8120 的排除。

此时，类别树 A，8100 的 TLCE 对密钥发行中心（KDC）进行树变更通知（参照图 53），密钥发行中心（KDC）根据已接受的树变更通知，对管理下的各 TLCE、关联 EKB 请求者进行通知。此时的通知只是告知接受了树变更通知，不进行 EKB 类型定义表的更新处理。

由于进行了排除处理的类别树的 TLCE 使利用了排除装置 A1，8120 中的将来的 EKB 的新的内容处理停止，故作为自身的 EKB 请求者，对密钥发行中心（KDC）进行 EKB 发行要求，使其生成只在排除处理对象以外的装置中能处理的更新了的 EKB。此时，作为 EKB 请求者的 TLCE 指定作为在类别树 A，8100 和类别树 B，8200 中共同地使用的 EKB 的类型而被定义了的 EKB 类型识别编号＃1。此外，或是 EKB 请求者自身生成新的根密钥并发送给 KDC，或是要求 KDC 生成新的根密钥。

密钥发行中心（KDC）根据已被指定的 EKB 类型识别编号＃1，参照 EKB 类型定义表，根据对应的类别树的节点，对类别树 A，8100 和类别树 B，8200 的 TLCE 要求生成在正当的装置中能取得新的根密钥的子 EKB。

类别树 A，8100 和类别树 B，8200 的 TLCE 根据要求分别生成子 EKB。此时，在类别树 A，8100 中生成只在排除了被排除的装置 A1，8120 的其它的装置中才能取得新的根密钥的子 EKB－（A）。如果在类别树 B，8200 中不存在被排除的装置，则生成在属于类别的全部的装置中能取得新的根密钥的子 EKB－（B）并发送给密钥发行中心（KDC）。

密钥发行中心（KDC）根据从各 TLCE 接受了的子 EKB，按照上述的方法生成合成 EKB，将已生成的 EKB 发送给 TLCE（ex.格式持有者）。

各 TLCE（ex.格式持有者）将从密钥发行中心（KDC）接受的新的 EKB 分配给各装置，进行 EKB 的更新。属于类别树 A，8100 和类别树 B，8200 的装置可在加密/解密过程中使用从更新了的 EKB 抽出的根密钥在装置中记录新的内容。由于使用新的 EKB 进行了加密并已被记录

的内容只在应用了对应的 EKB 的情况下才能解密，故在已被排除的装置中不能利用。

以上一边参照特定的实施例一边详细地解释了本发明。但是，很明显的是，在不脱离本发明的要旨的范围内，业内人士可进行该实施例的修正或替代。即，用例示的形态公开了本发明，不应解释为对本发明作了限定。为了判断本发明的要旨，应参照后附的权利要求书。

产业上利用的可能性

如以上所说明的那样，按照本发明的信息管理系统和方法，在构成具有根据类别区分的、由类别实体管理的多个子树的密钥树、选择构成密钥树的通路并生成由选择通路上的低位密钥进行的高位密钥的加密处理数据构成的 EKB 和将其提供给装置的的结构中，由于以根据使 EKB 类型识别符与能处理 EKB 的 1 个以上的类别树的识别数据相对应的 EKB 类型定义表来进行 EKB 的发行管理的方式来构成，故作为 EKB 生成要求者的 EKB 请求者能任意地选择成为适用对象的类别。

此外，按照本发明的信息管理系统和方法，由于作成对 EKB 的利用实体进行关于能处理被 EKB 类型定义表定义的 EKB 的类别树中的因排除等引起的状态变化发生的通知处理的结构，故 EKB 请求者等的实体能常时地进行基于最新的 EKB 类型定义信息的处理。

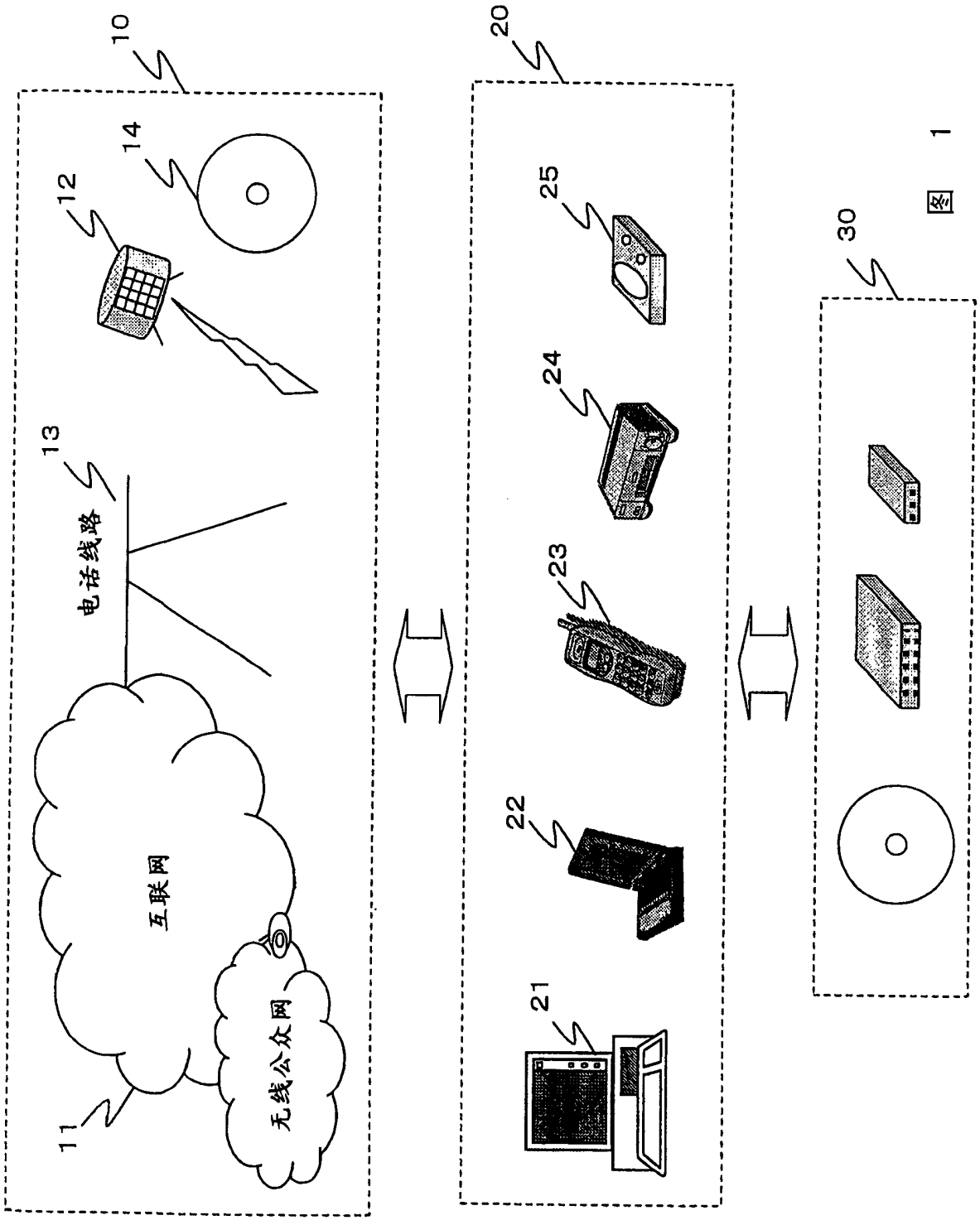


图 1

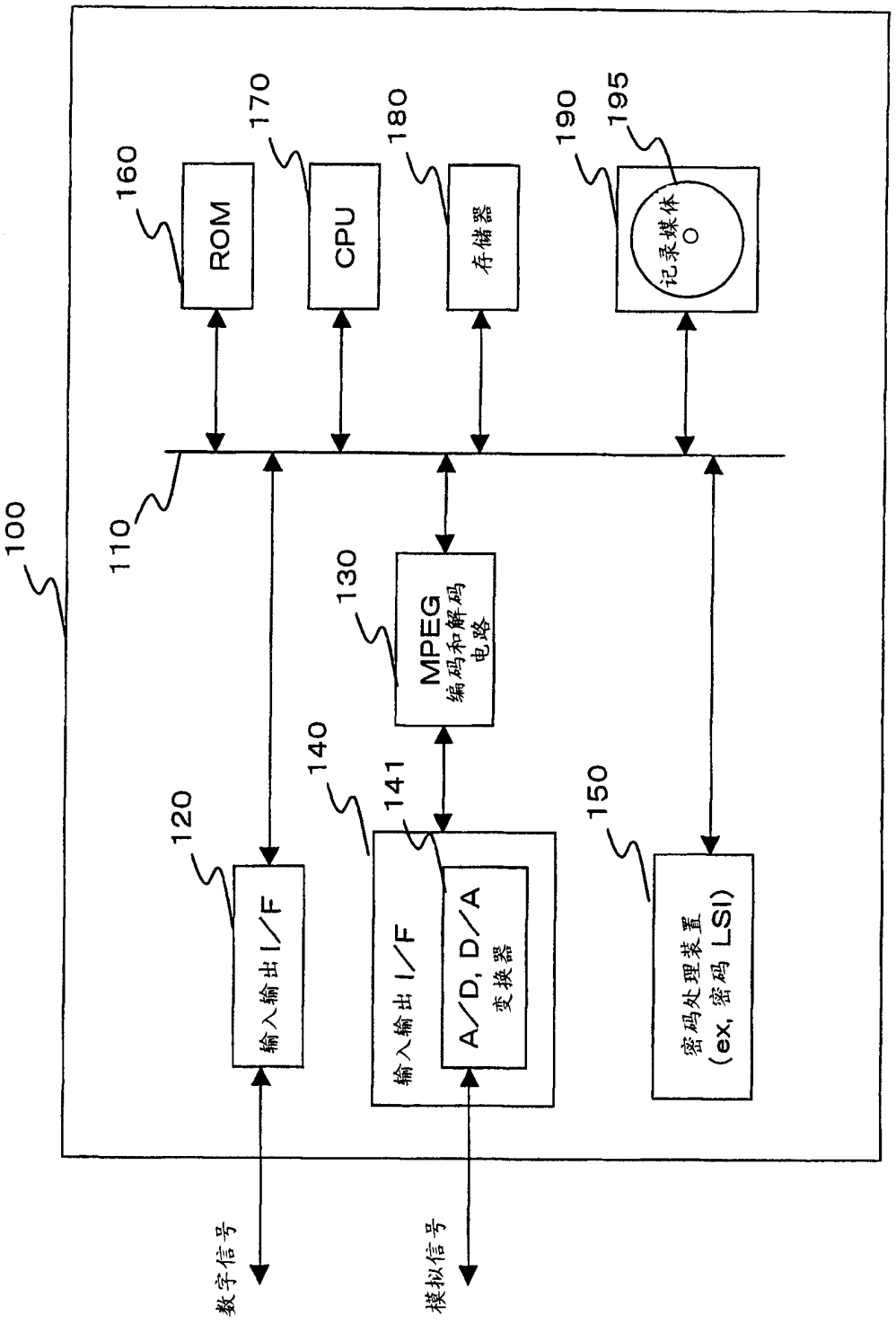

100
110
160
ROM
170
CPU
180
存储器
190
195
记录媒体
130
MPEG
编码和解码
电路
140
141
120
150
输入输出 I/F
A/D, D/A
变换器
输入输出 I/F
密码处理装置
(ex, 密码 LSI)
数字信号
模拟信号

图 2

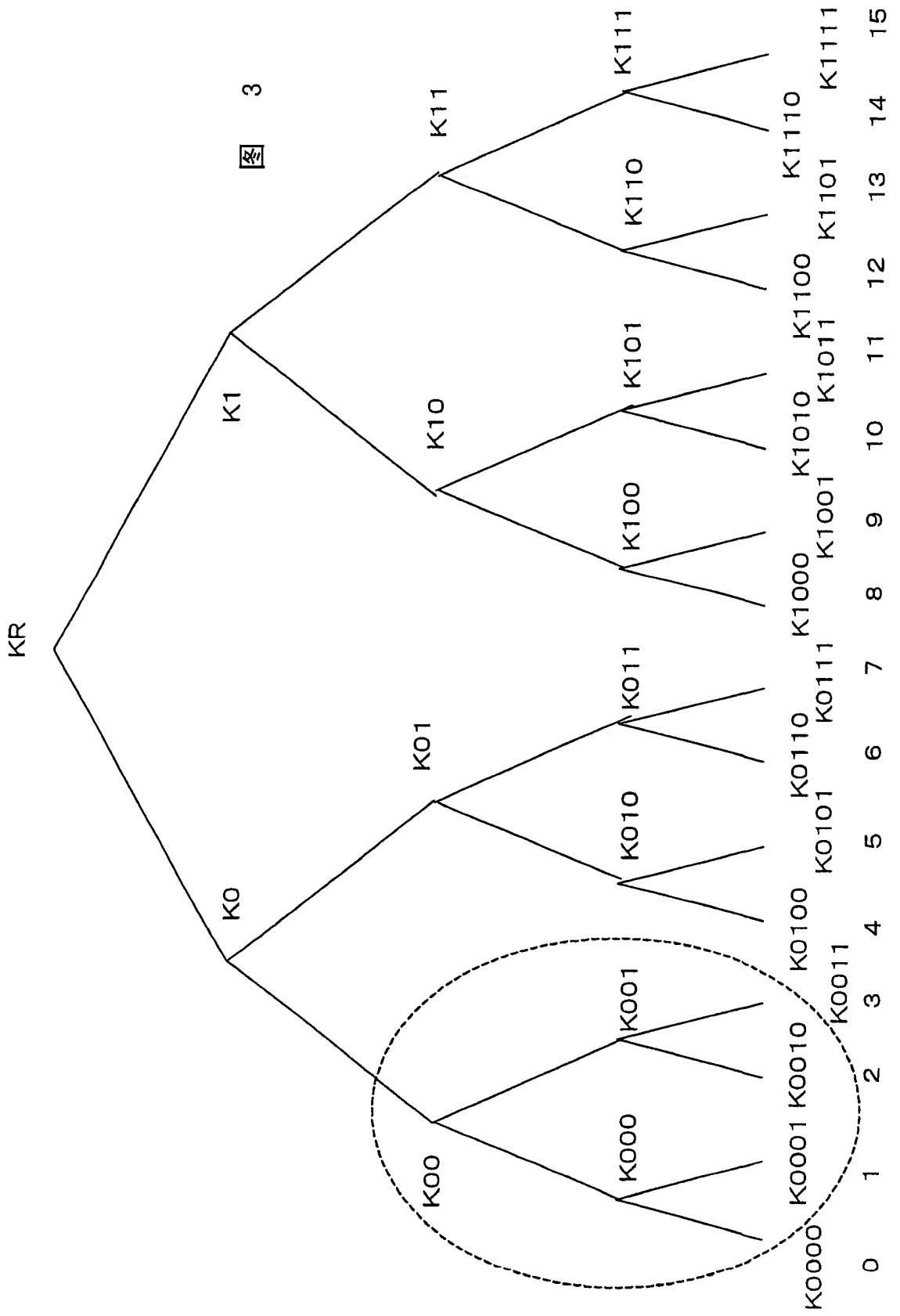

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
装置

图 3

(A) 有效化密钥块(EKB)例1

对装置0、1、2发送版本t的节点密钥

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)

(B) 有效化密钥块(EKB)例2

对装置0、1、2发送版本t的节点密钥

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 4

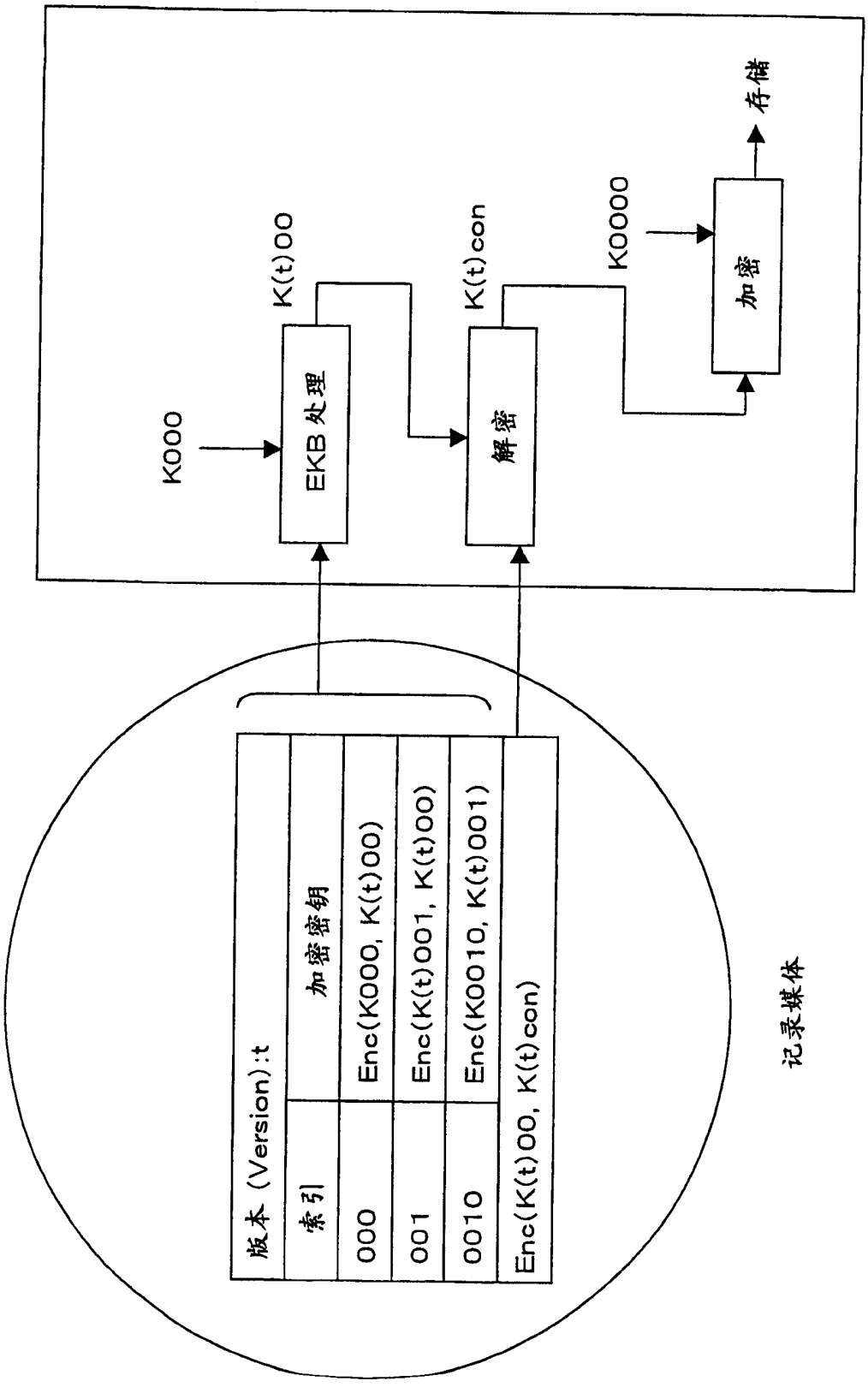

K000
EKB 处理
K(t)00
解密
K(t)con
K0000
加密
存储
装置 0
记录媒体
版本 (Version):t
索引
加密密钥
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)

图 5

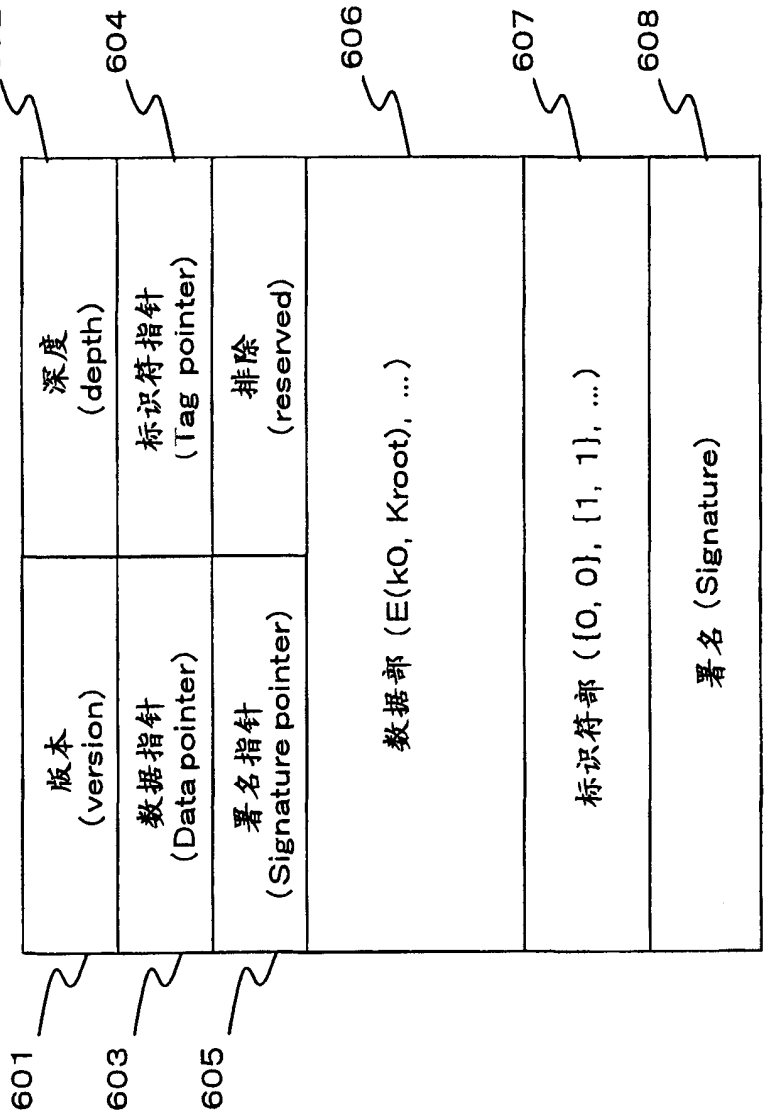

602
604
606
607
608
深度 (depth)
标识符指针 (Tag pointer)
排除 (reserved)
版本 (version)
数据指针 (Data pointer)
署名指针 (Signature pointer)
数据部（E(k0, Kroot), ...）
标识符部（{0, 0}, {1, 1}, ...）
署名 (Signature)
601
603
605

图 6

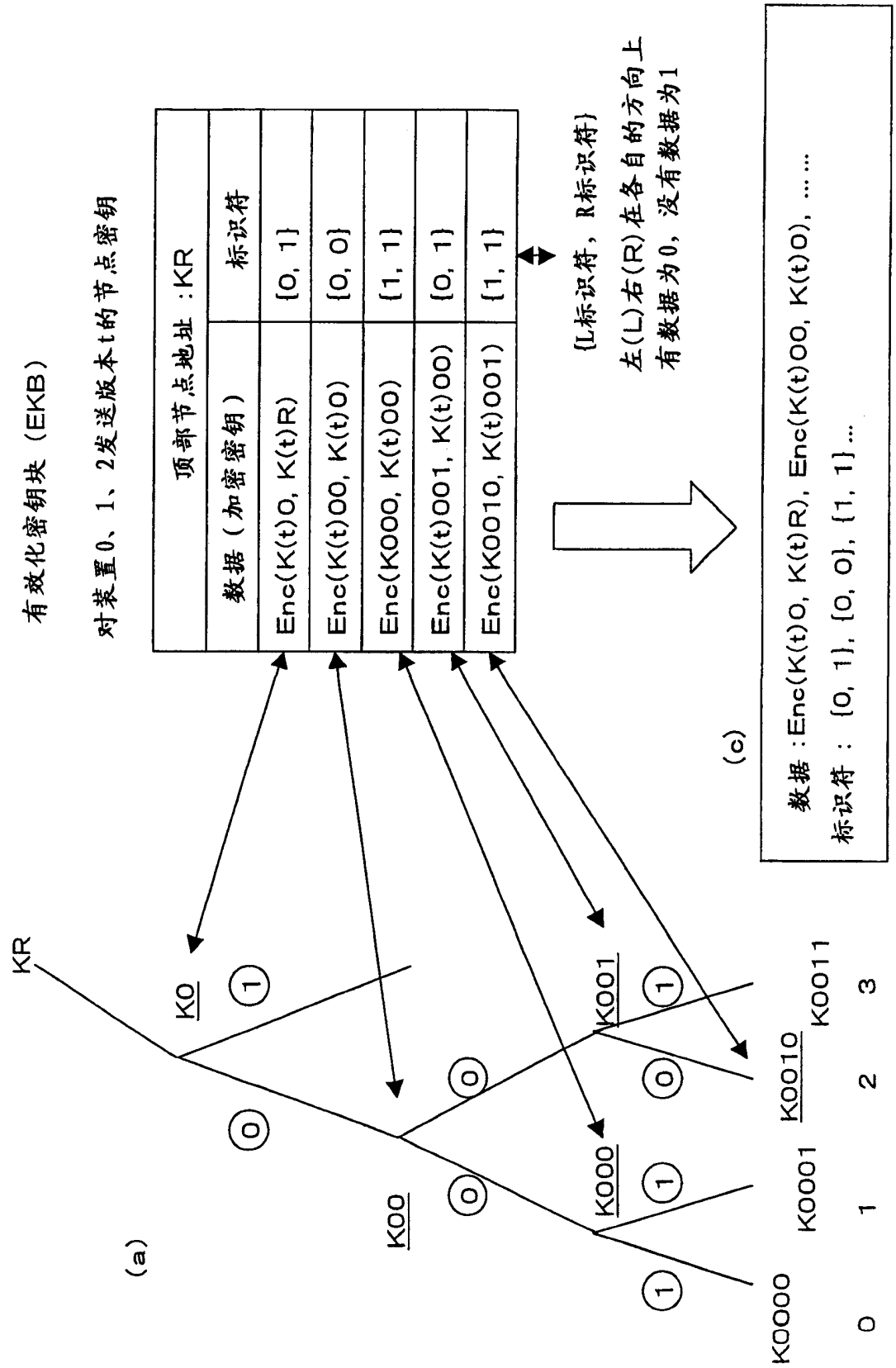

(a)
KR
K0
K00
K000
K0000
K0001
K0010
K0011
K001
0
1
2
3
(b)
有效化密钥块（EKB）
对装置0、1、2发送版本t的节点密钥
顶部节点地址 :KR
数据（加密密钥）
标识符
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{L标识符，R标识符}
左(L)右(R)在各自的方向上
有数据为0，没有数据为1
(c)
数据 :Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
标识符 : {0, 1}, {0, 0}, {1, 1}…

图 7

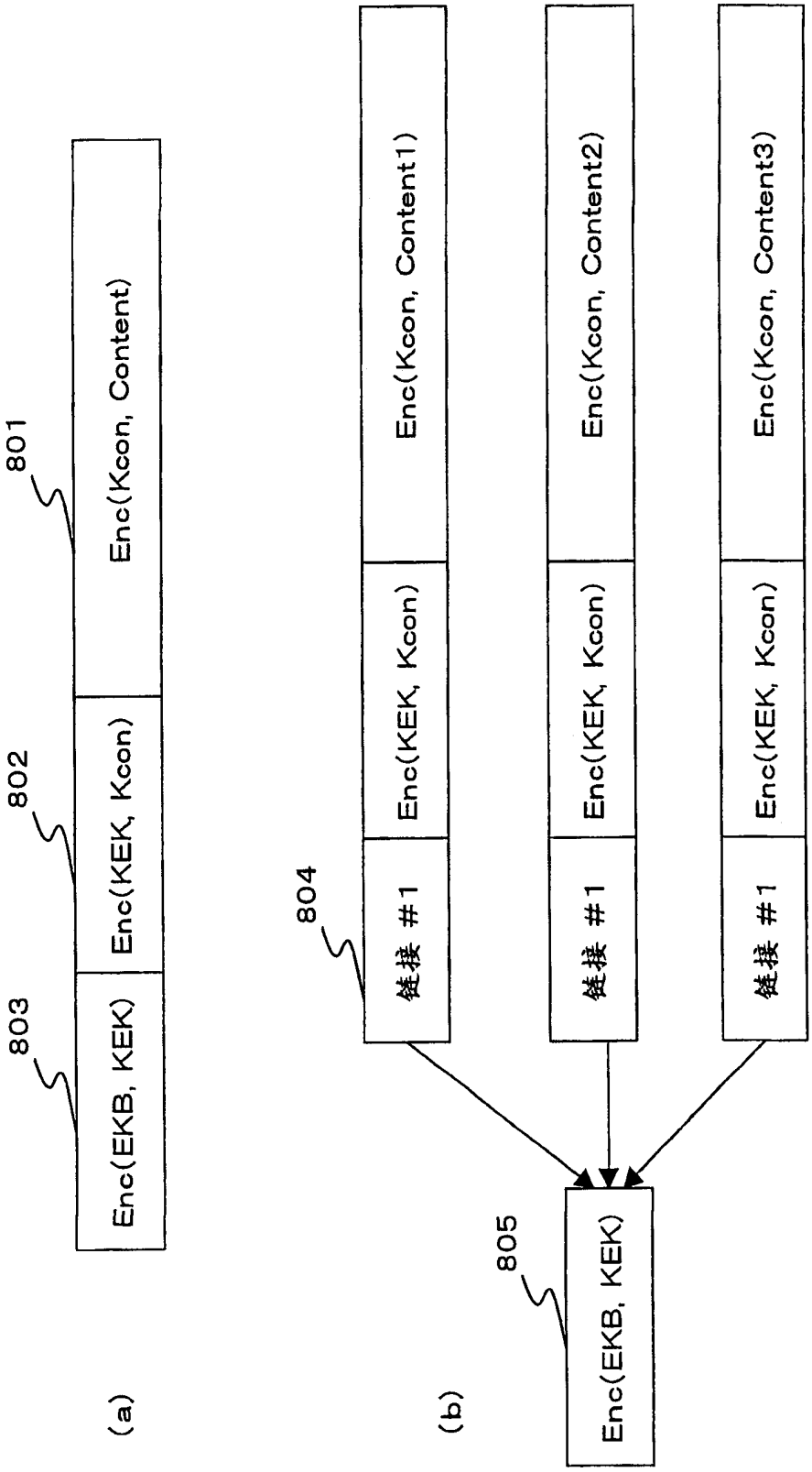

(a)
Enc(EKB, KEK)
Enc(KEK, Kcon)
Enc(Kcon, Content)
801
802
803
(b)
链接 #1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
Enc(Kcon, Content2)
Enc(Kcon, Content3)
804
805
Enc(EKB, KEK)

图 8

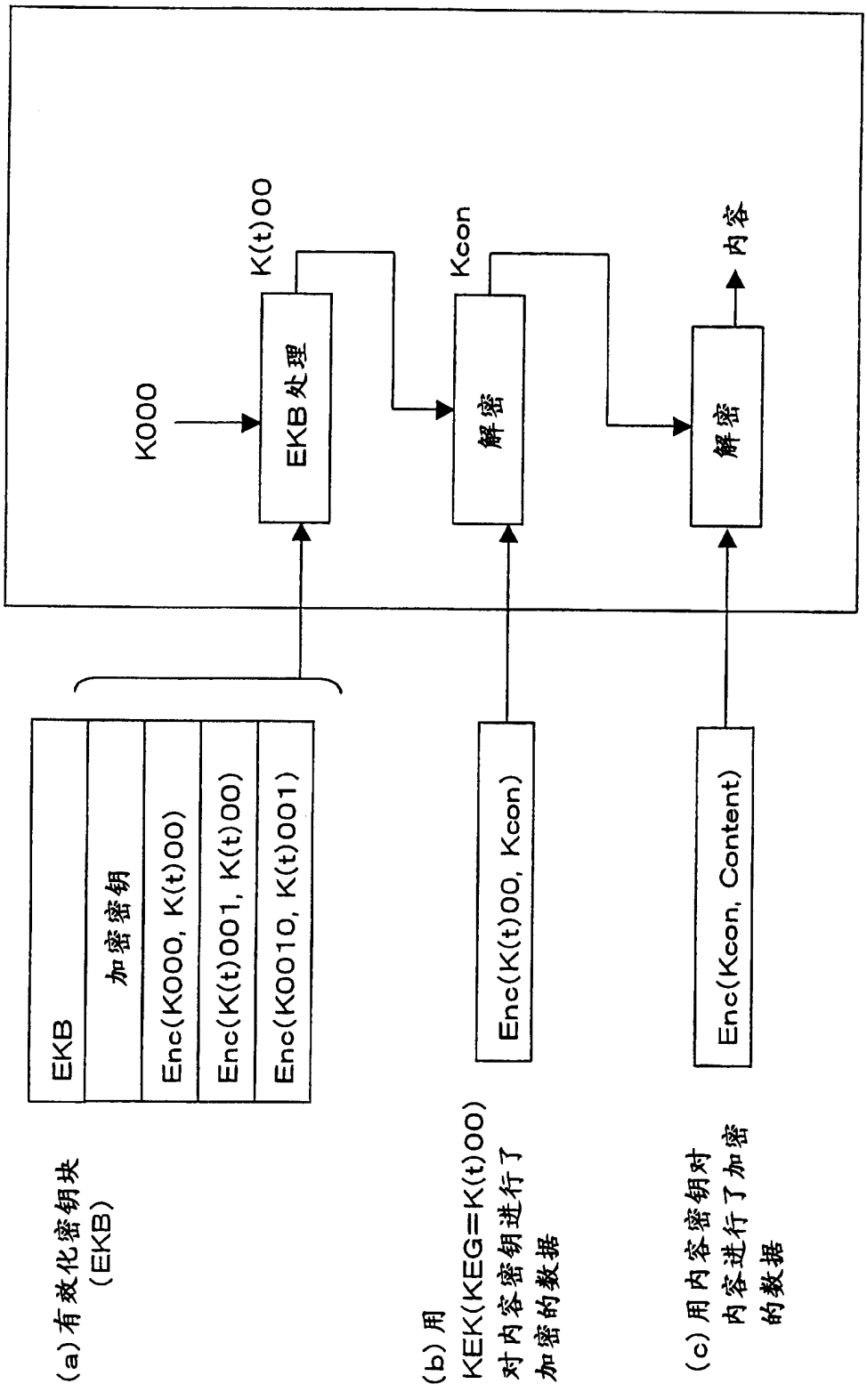

K000
EKB处理
K(t)00
Kcon
解密
解密
内容
装置O
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
Enc(K(t)00, Kcon)
Enc(Kcon, Content)
(a)有效化密钥块
(EKB)
(b)用
KEK(KEG=K(t)00)
对内容密钥进行了
加密的数据
(c)用内容密钥对
内容进行了加密
的数据

图 9

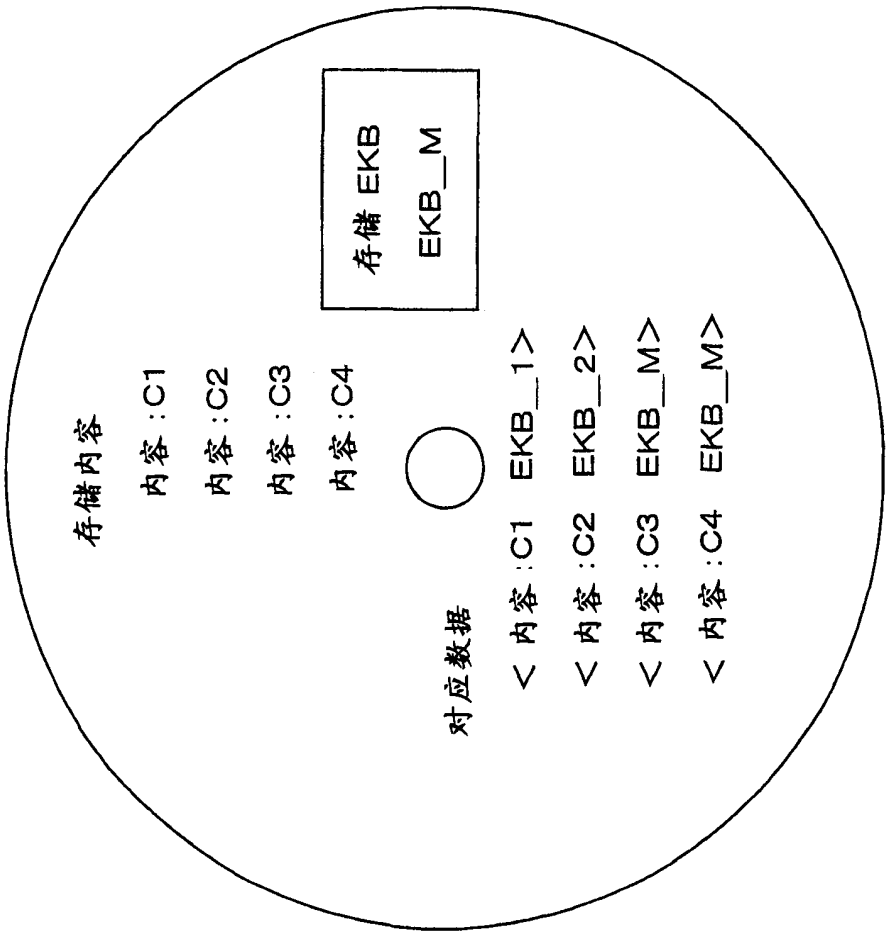

存储内容
内容:C1
内容:C2
内容:C3
内容:C4
存储 EKB
EKB_M
对应数据
< 内容:C1 EKB_1>
< 内容:C2 EKB_2>
< 内容:C3 EKB_M>
< 内容:C4 EKB_M>
记录媒体

图 10

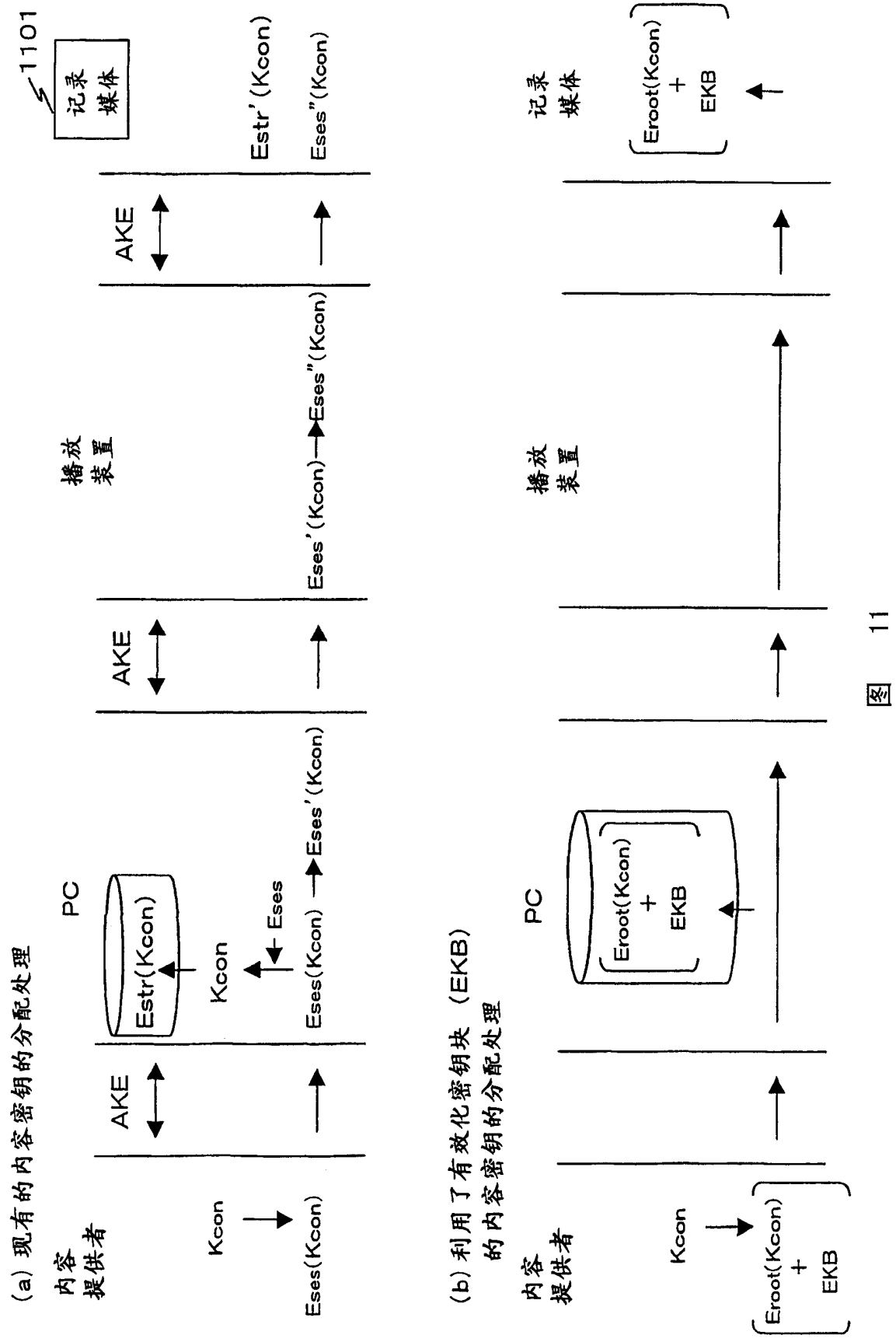

(a) 现有的内容密钥的分配处理
内容提供者
PC
播放装置
记录媒体
1101
AKE
Kcon
Estr(Kcon)
Eses(Kcon)
Ses(Kcon)
Eses'(Kcon)
Estr'(Kcon)
Eses"(Kcon)
(b) 利用了有效化密钥块（EKB）的内容密钥的分配处理
Eroot(Kcon)
+
EKB

图 11

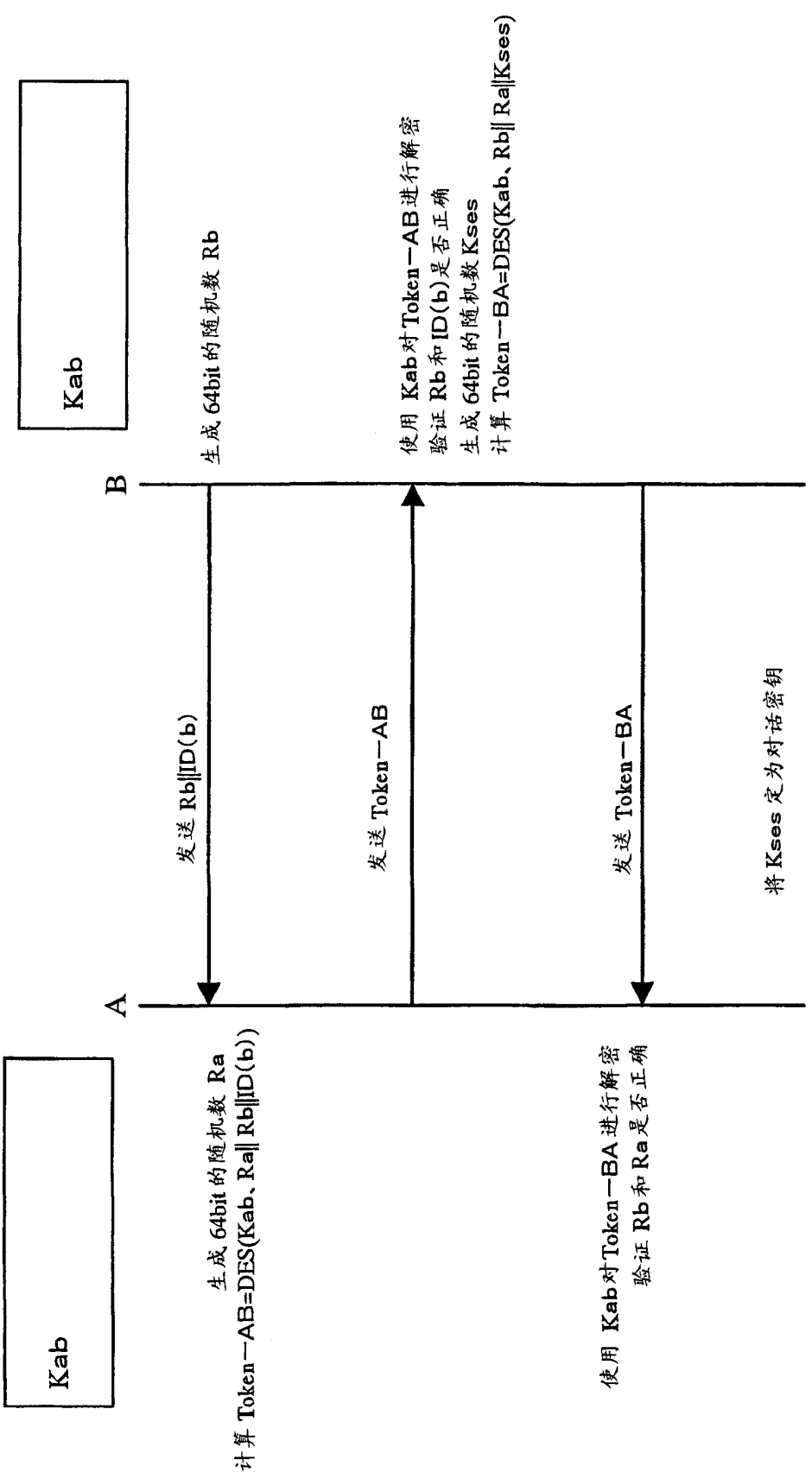

Kab
B
生成 64bit 的随机数 Rb
使用 Kab 对 Token－AB 进行解密
验证 Rb 和 ID(b)是否正确
生成 64bit 的随机数 Kses
计算 Token－BA=DES(Kab、Rb‖Ra‖Kses)
发送 Rb‖ID(b)
发送 Token－AB
发送 Token－BA
将 Kses 定为对话密钥
A
Kab
生成 64bit 的随机数 Ra
计算 Token－AB=DES(Kab、Ra‖Rb‖ID(b))
使用 Kab 对 Token－BA 进行解密
验证 Rb 和 Ra 是否正确

图 12

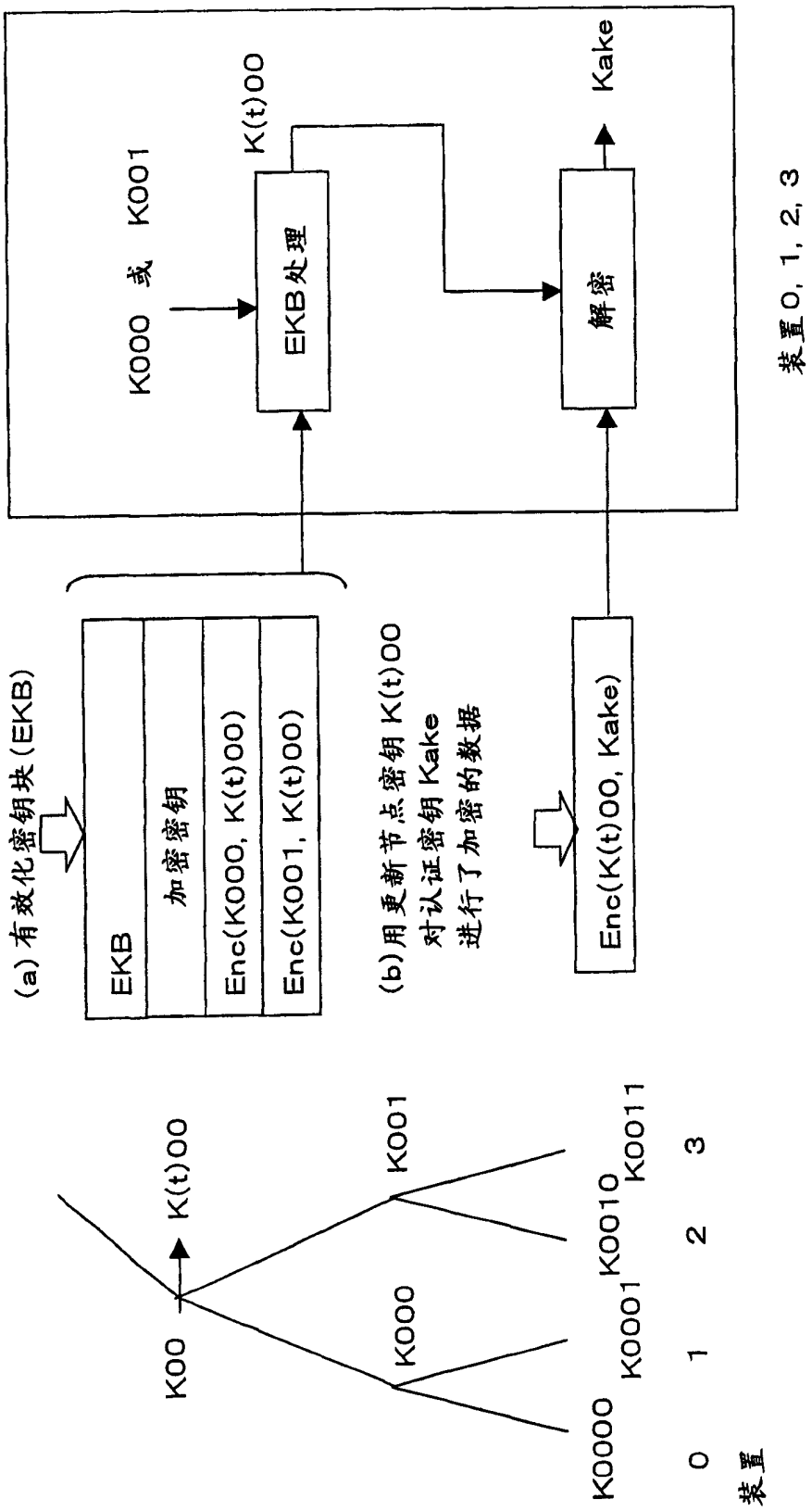

装置0, 1, 2, 3
K000 或 K001
K(t)00
EKB处理
解密
Kake
(a) 有效化密钥块(EKB)
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K001, K(t)00)
(b)用更新节点密钥 K(t)00
对认证密钥 Kake
进行了加密的数据
Enc(K(t)00, Kake)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
装置

图 13

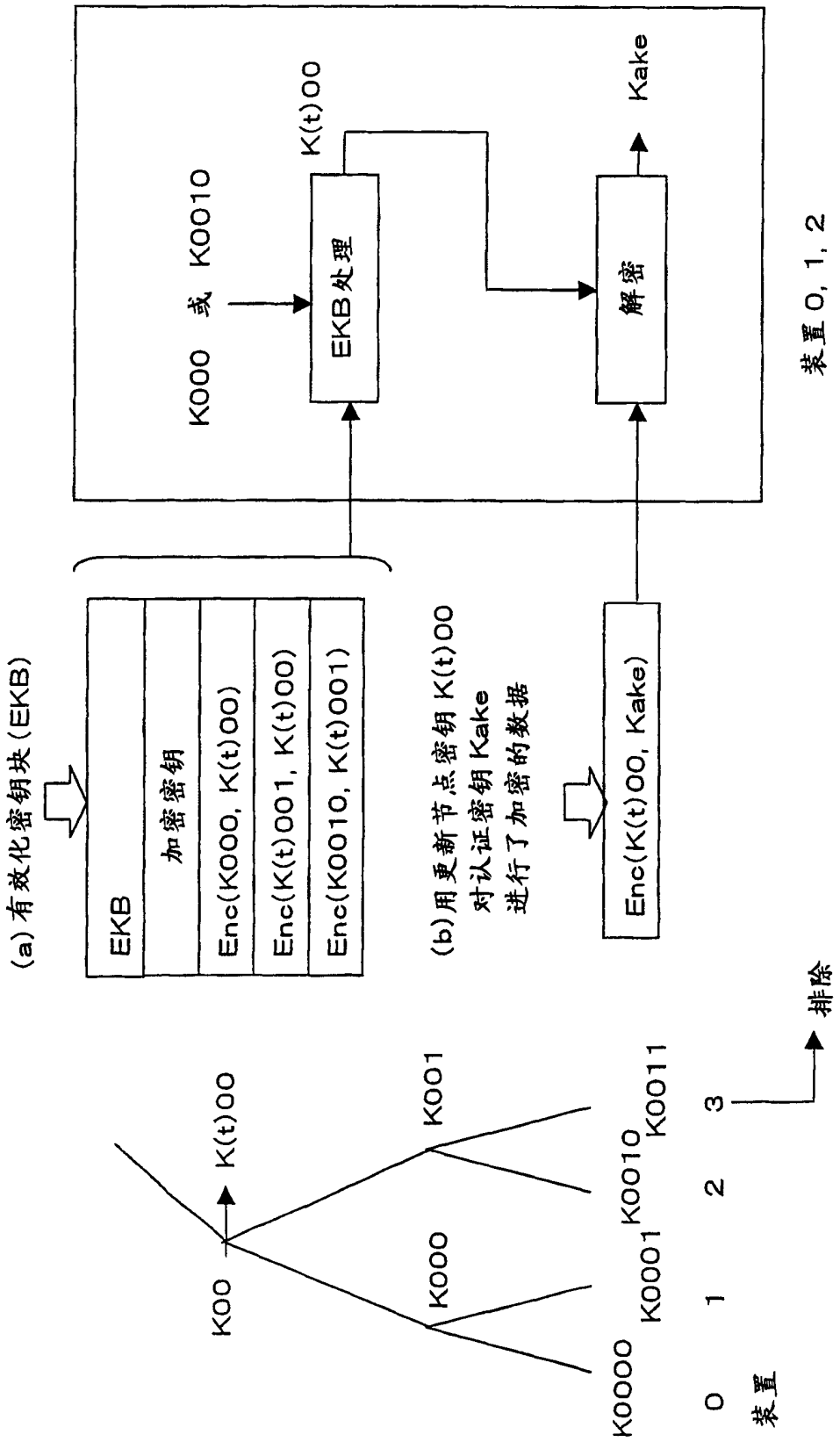

(a) 有效化密钥块 (EKB)
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
(b) 用更新节点密钥 K(t)00
对认证密钥 Kake
进行了加密的数据
Enc(K(t)00, Kake)
装置 0, 1, 2
K000 或 K0010
EKB处理
K(t)00
解密
Kake
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
装置
排除

图 14

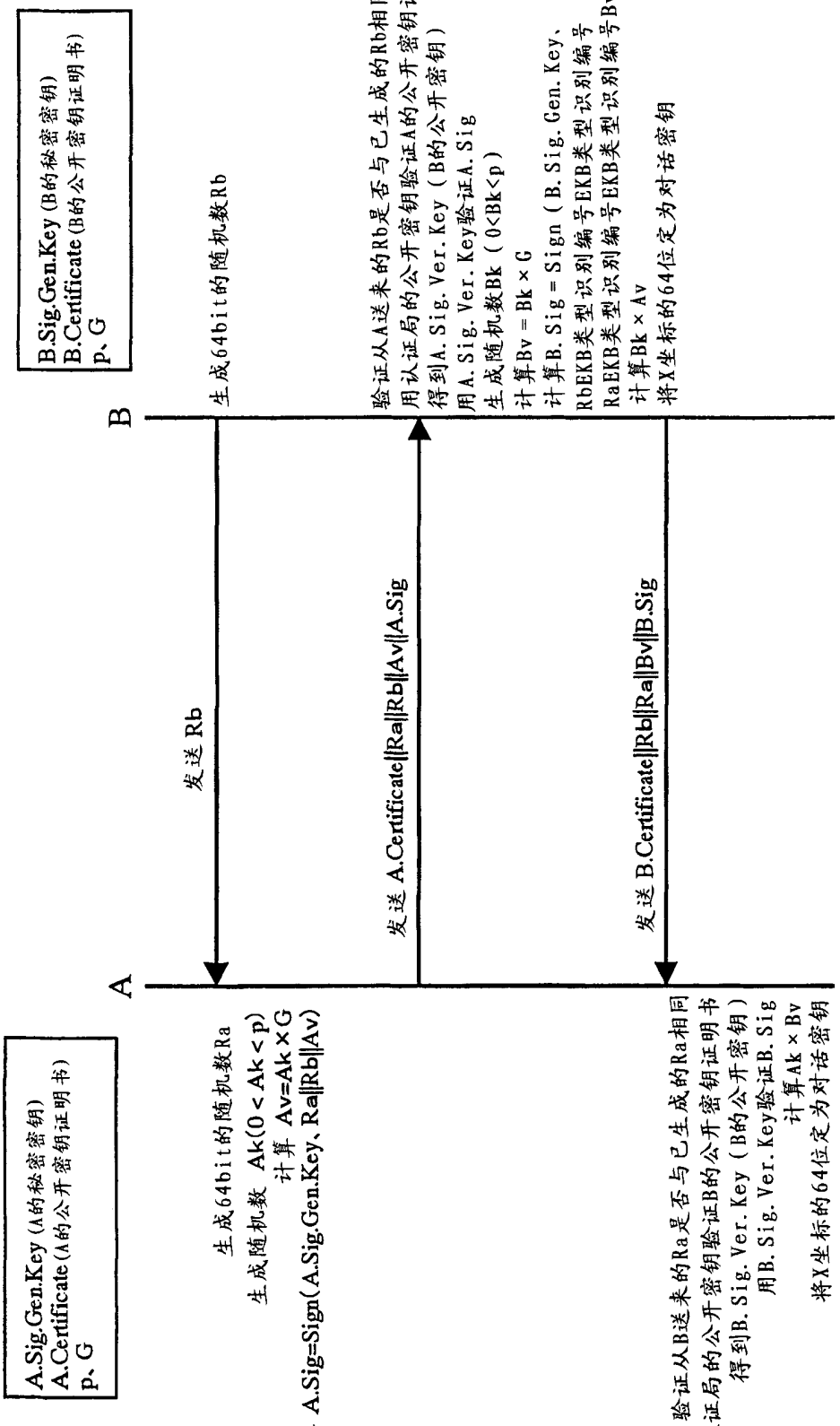

A.Sig.Gen.Key (A的秘密密钥)
A.Certificate (A的公开密钥证明书)
p、G
A
B
B.Sig.Gen.Key (B的秘密密钥)
B.Certificate (B的公开密钥证明书)
p、G
生成64bit的随机数Ra
生成随机数 Ak(0 < Ak < p)
计算 Av=Ak×G
计算 A.Sig=Sign(A.Sig.Gen.Key、Ra||Rb||Av)
发送 Rb
生成64bit的随机数Rb
发送 A.Certificate||Ra||Rb||Av||A.Sig
验证从A送来的Rb是否与已生成的Rb相同
用认证局的公开密钥验证A的公开密钥证明书
得到A.Sig.Ver.Key (B的公开密钥)
用A.Sig.Ver.Key验证A.Sig
生成随机数Bk (0<Bk<p)
计算Bv = Bk × G
计算B.Sig = Sign (B.Sig.Gen.Key、
RbEKB类型识别编号EKB类型识别编号
RaEKB类型识别编号EKB类型识别编号Bv)
计算Bk × Av
将X坐标的64位定为对话密钥
发送 B.Certificate||Rb||Ra||Bv||B.Sig
验证从B送来的Ra是否与已生成的Ra相同
用认证局的公开密钥验证B的公开密钥证明书
得到B.Sig.Ver.Key (B的公开密钥)
用B.Sig.Ver.Key验证B.Sig
计算Ak × Bv
将X坐标的64位定为对话密钥

图 15

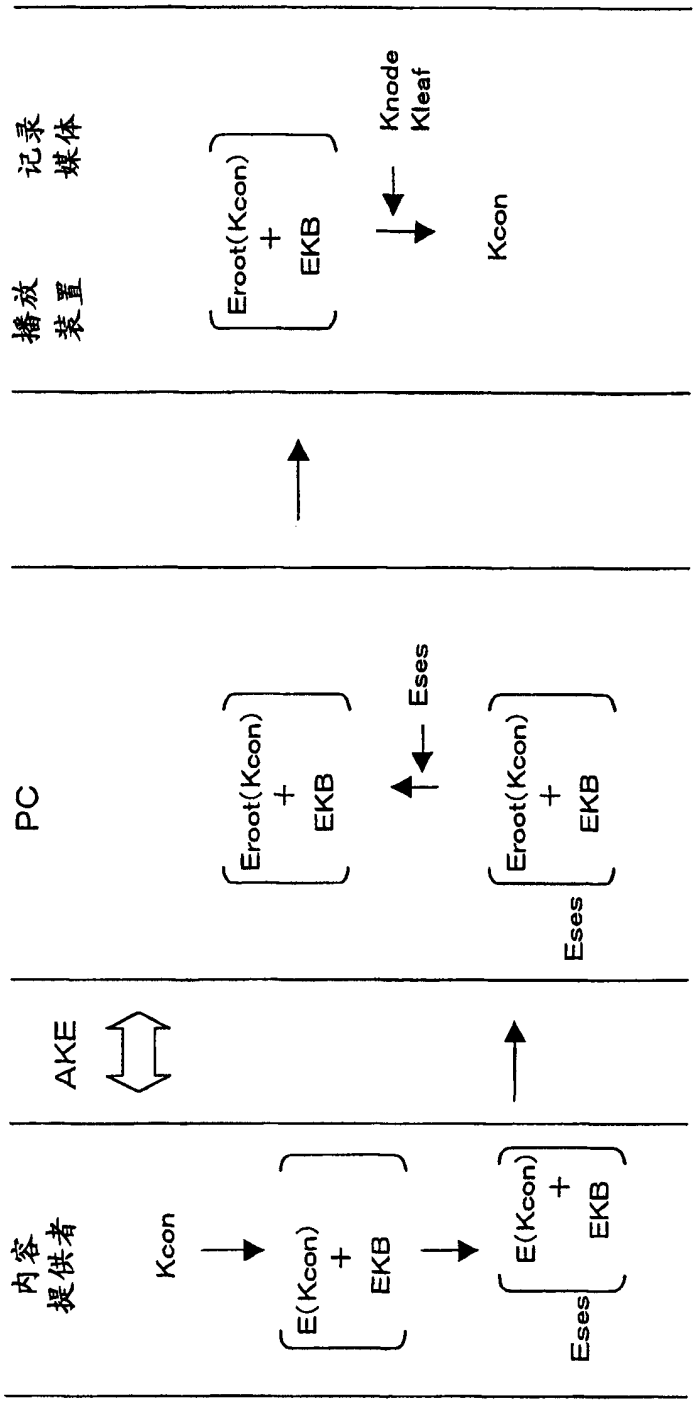

内容
提供者
Kcon
E(Kcon)
+
EKB
AKE
PC
播放
装置
记录
媒体
Eroot(Kcon)
+
EKB
Ekb
Eses
Knode
Kleaf
Kcon

图 16

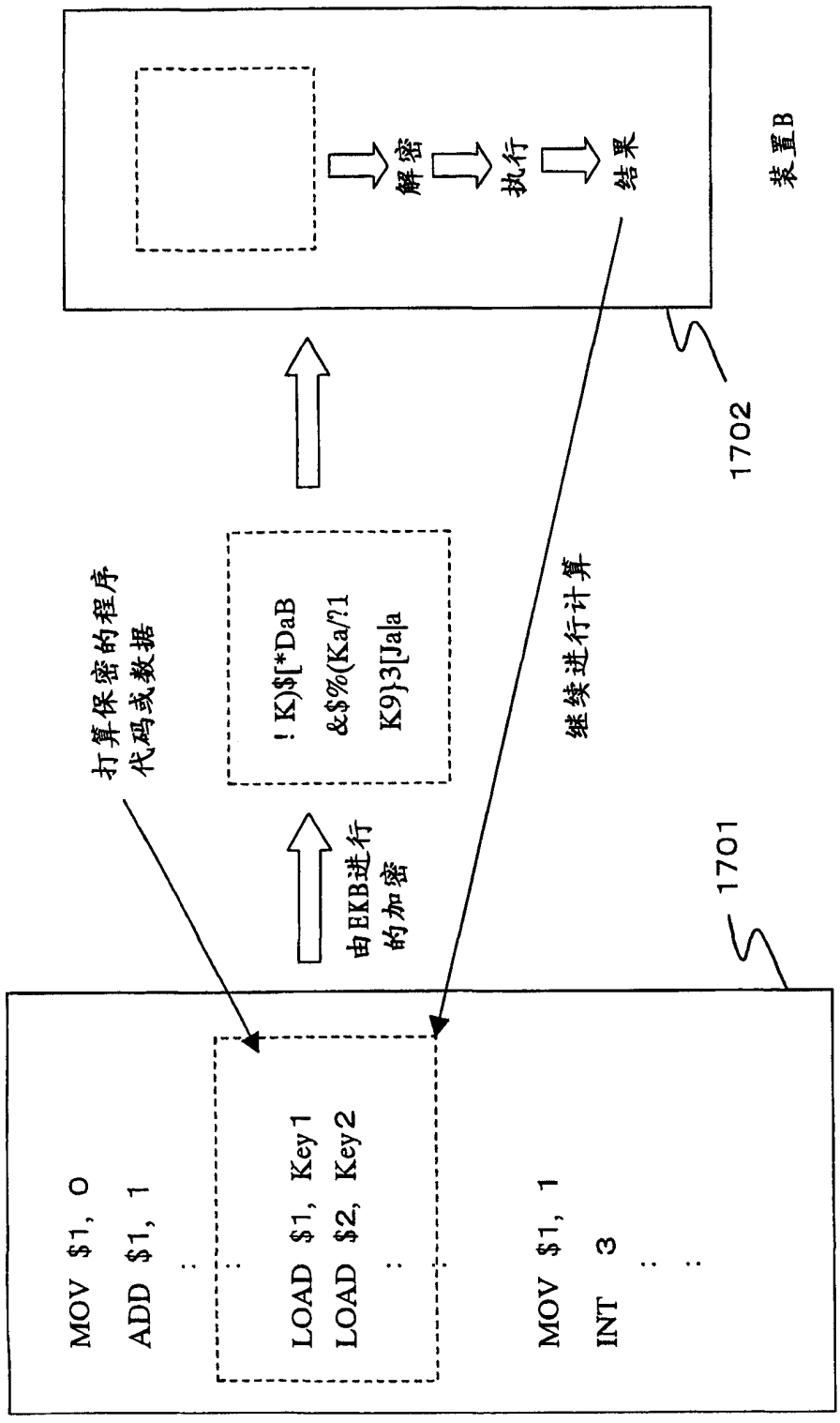

装置B
解密
执行
结果
1702
! K)$['*DaB
&$%(Ka/?1
K9}3[Ja|a
打算保密的程序
代码或数据
由EKB进行
的加密
继续进行计算
1701
MOV $1, 0
ADD $1, 1
LOAD $1, Key1
LOAD $2, Key2
MOV $1, 1
INT 3
装置A

图 17

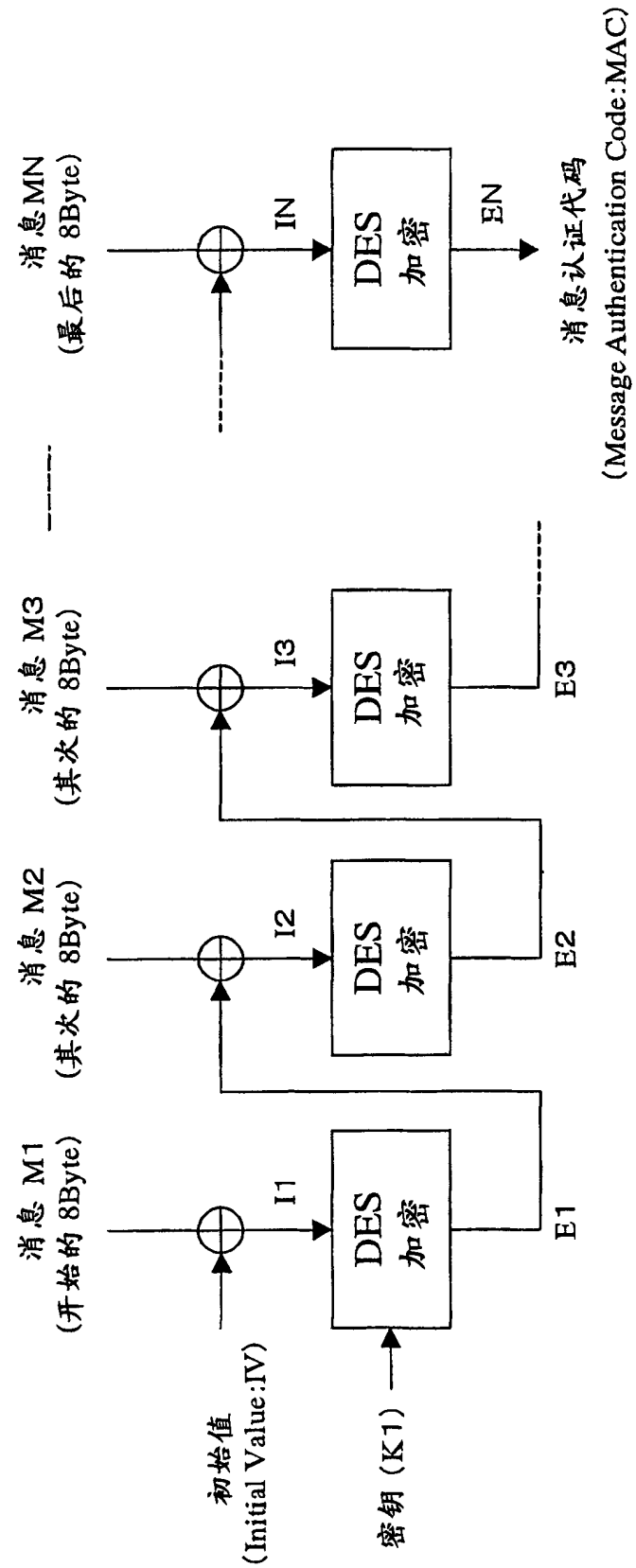

消息 M1
(开始的 8Byte)
消息 M2
(其次的 8Byte)
消息 M3
(其次的 8Byte)
消息MN
(最后的 8Byte)
初始值
(Initial Value:IV)
密钥（K1）
I1
I2
I3
IN
DES
加密
E1
E2
E3
EN
消息认证代码
(Message Authentication Code:MAC)
⊕ ：异或运算处理(8字节单位)

图 18

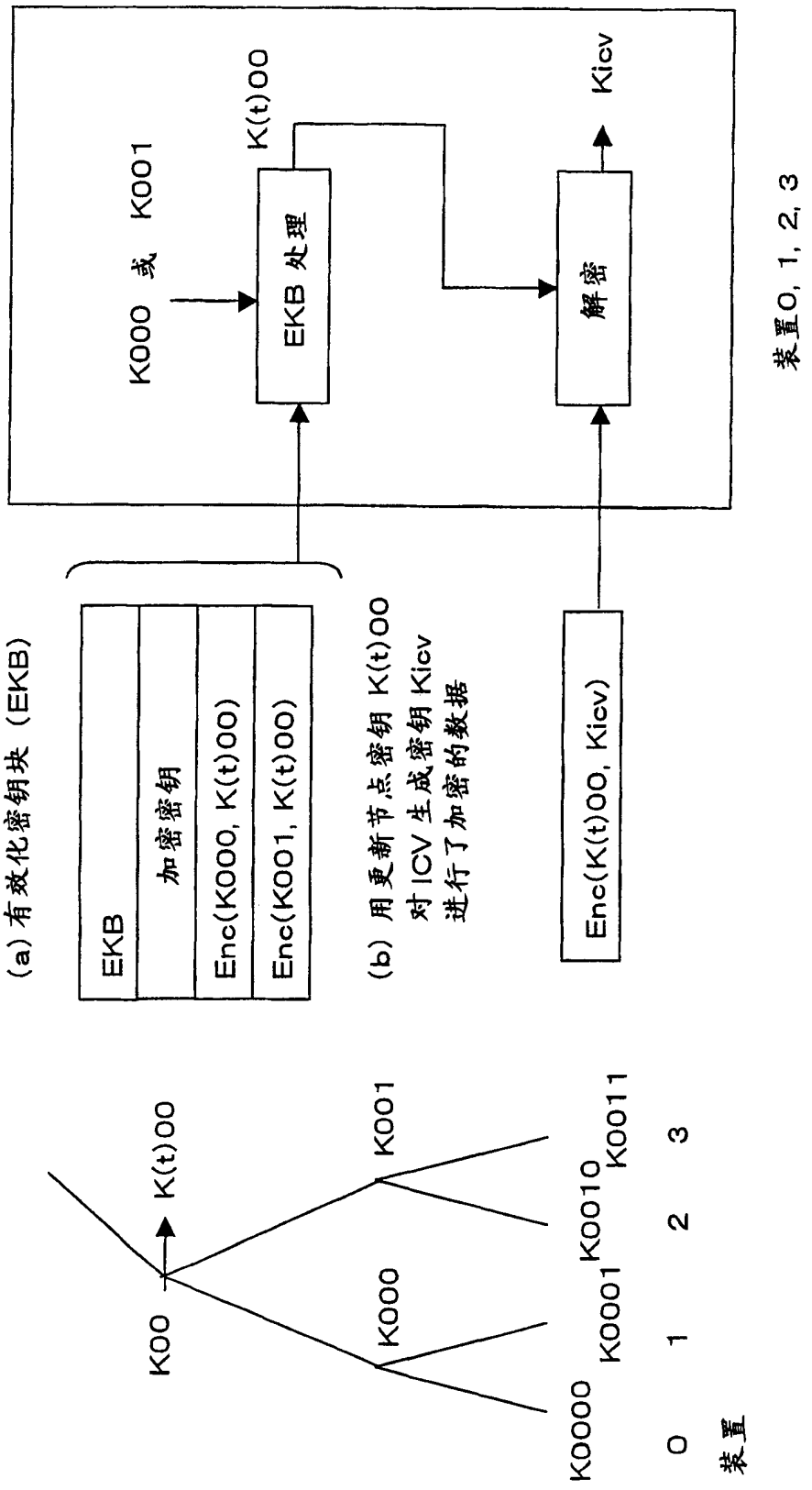

装置 0
K0000
K0001
K0010
K0011
K000
K001
K00
K(t)00
0
1
2
3
装置0, 1, 2, 3
K000 或 K001
K(t)00
EKB 处理
解密
Kicv
(a) 有效化密钥块 (EKB)
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K001, K(t)00)
(b) 用更新节点密钥 K(t)00
对 ICV 生成密钥 Kicv
进行了加密的数据
Enc(K(t)00, Kicv)

图 19

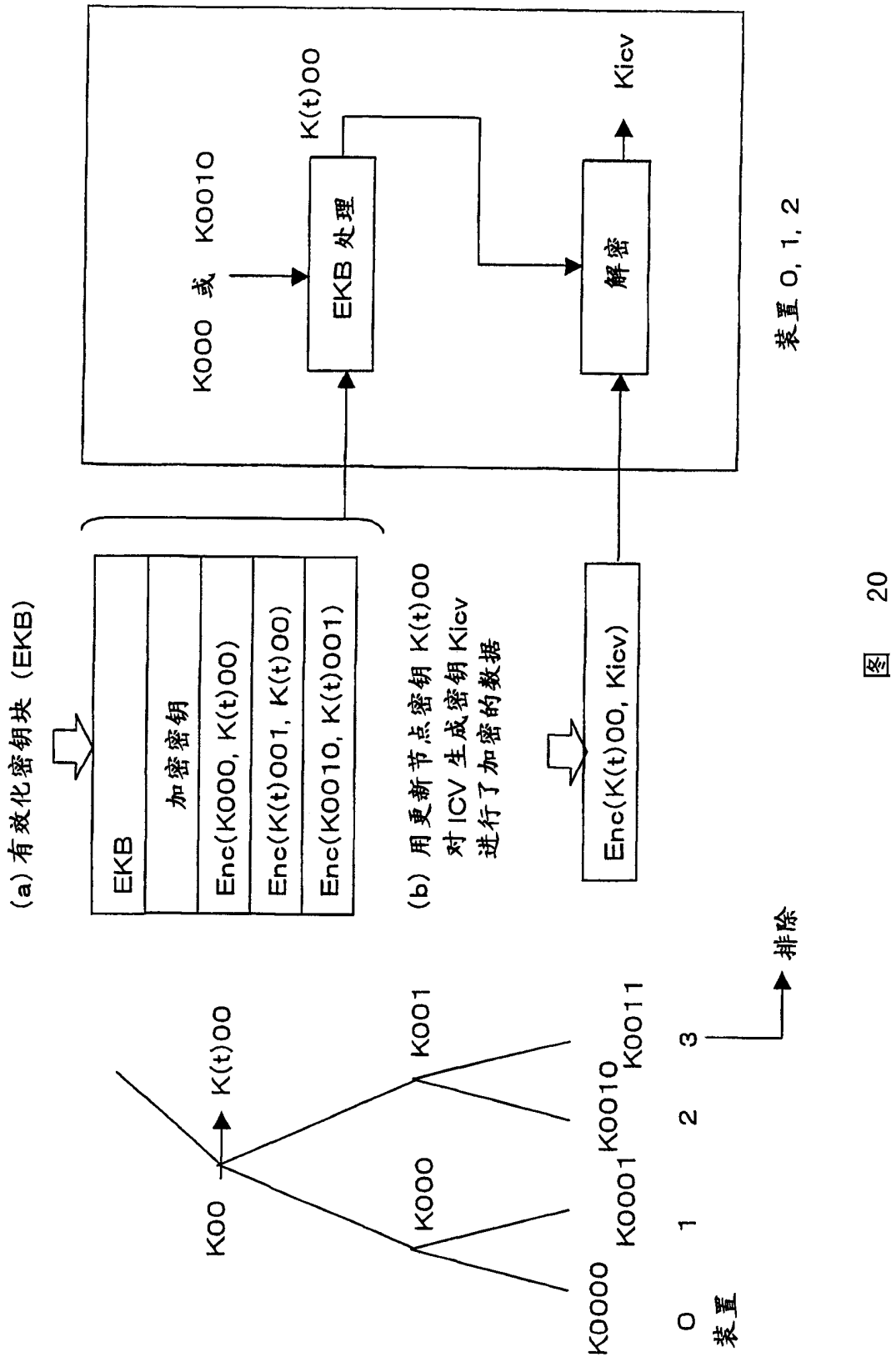

(a) 有效化密钥块（EKB）
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
(b) 用更新节点密钥 K(t)00
对 ICV 生成密钥 Kicv
进行了加密的数据
Enc(K(t)00, Kicv)
K000 或 K0010
EKB 处理
K(t)00
解密
Kicv
装置 0, 1, 2
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
装置
1
2
3
排除

图 20

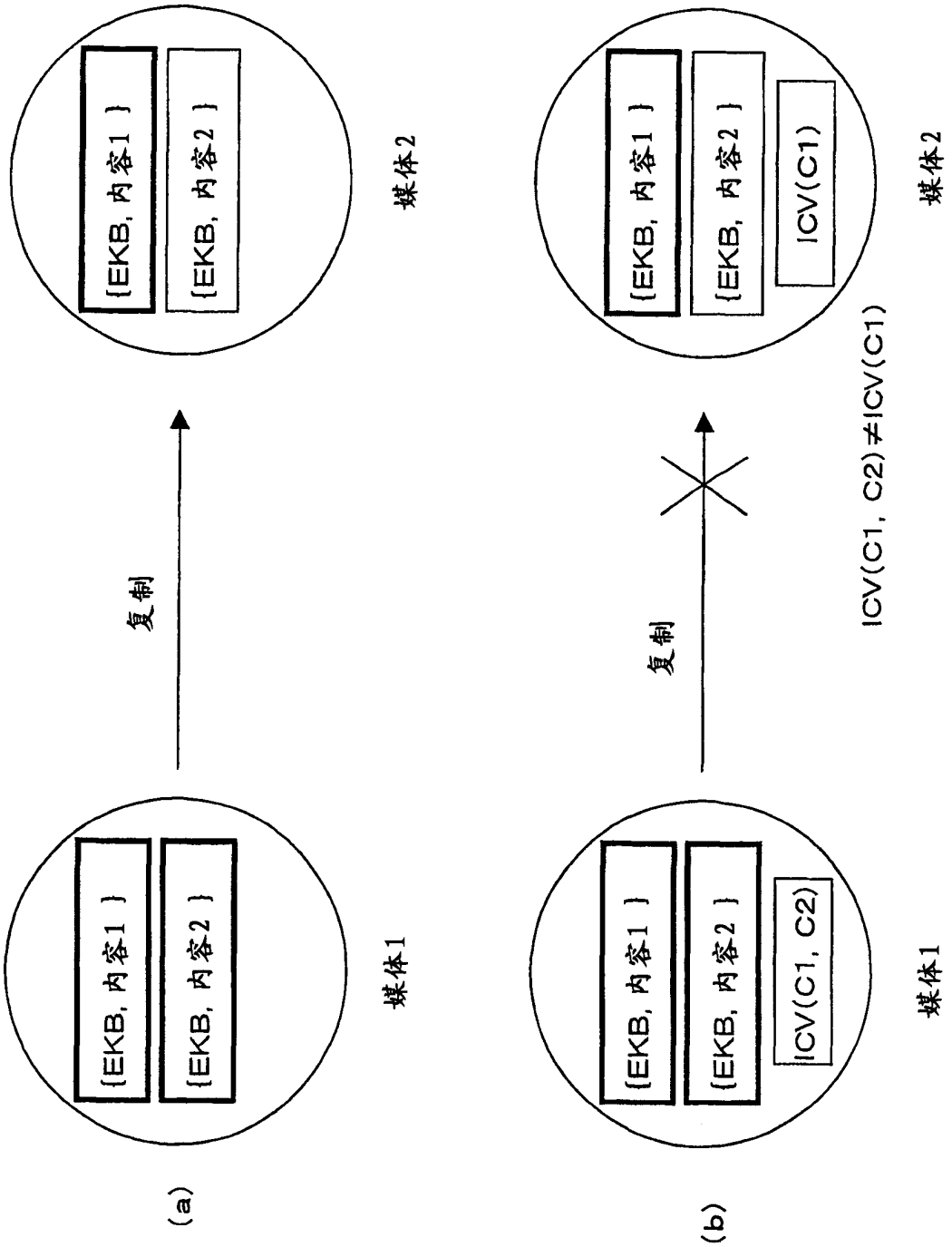

(a)
{EKB, 内容1 }
{EKB, 内容2 }
媒体1
复制
{EKB, 内容1 }
{EKB, 内容2 }
媒体2
(b)
{EKB, 内容1 }
{EKB, 内容2 }
ICV(C1, C2)
媒体1
复制
ICV(C1, C2)≠ICV(C1)
{EKB, 内容1 }
{EKB, 内容2 }
ICV(C1)
媒体2

图 21

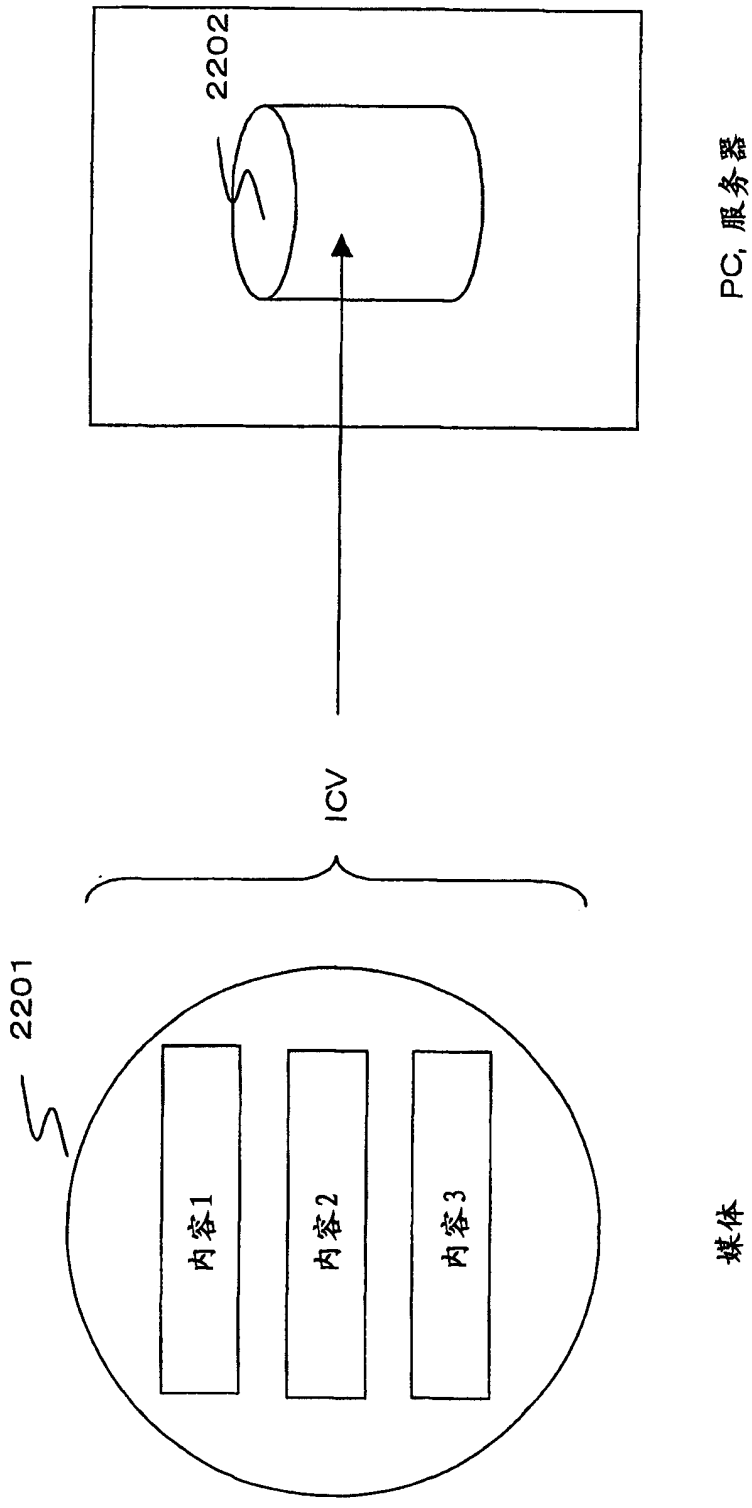


图 22

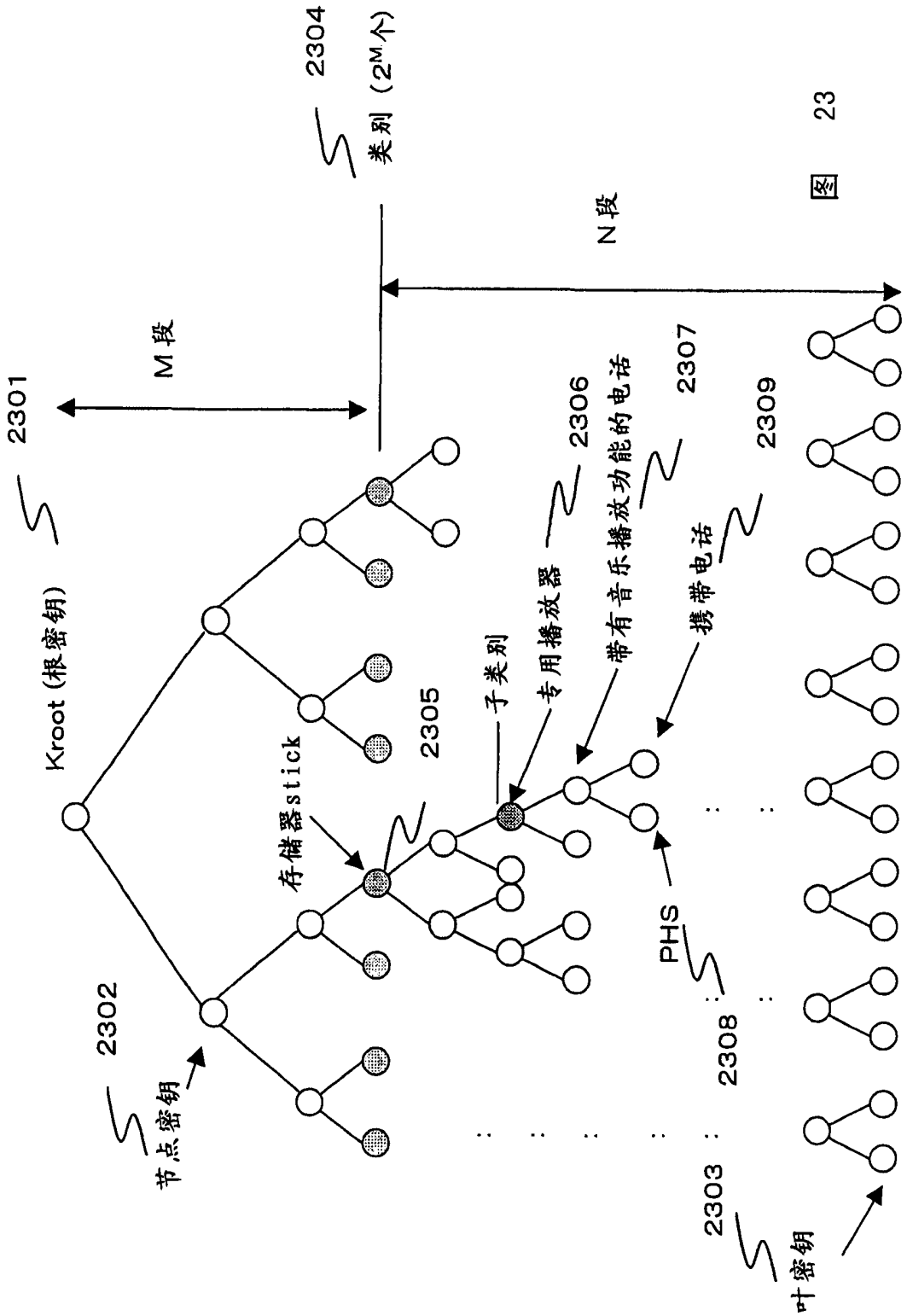
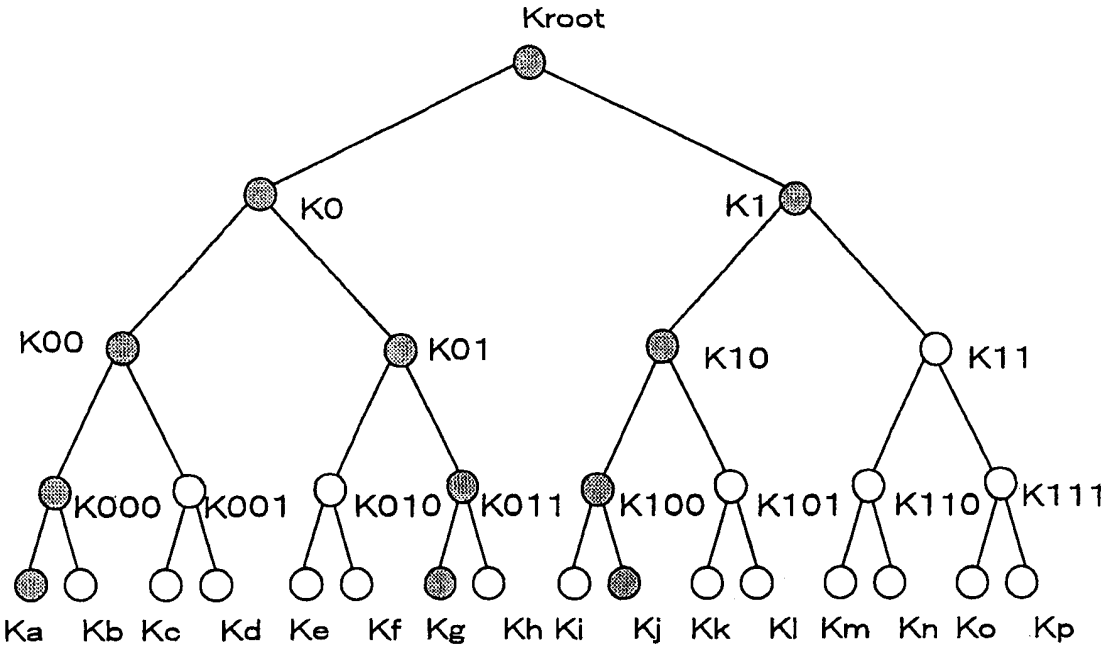

2301
Kroot (根密钥)
M 段
2304
类别 (2^M个)
N 段
2302
节点密钥
存储器stick
2305
子类别
专用播放器
2306
带有音乐播放功能的电话
2307
PHS
2308
携带电话
2309
2303
叶密钥

图 23


Kroot
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
Ka
Kb
Kc
Kd
Ke
Kf
Kg
Kh
Ki
Kj
Kk
Kl
Km
Kn
Ko
Kp

(a)

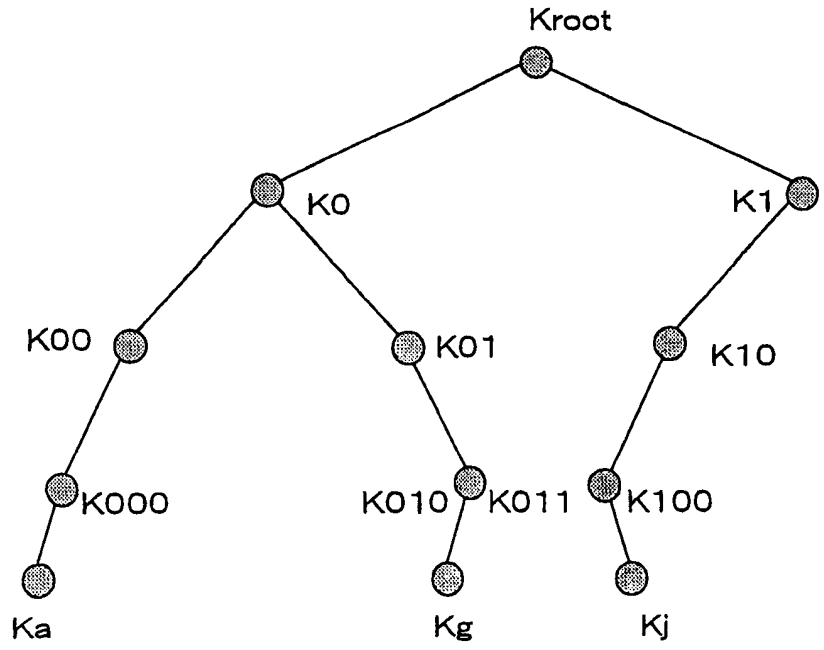
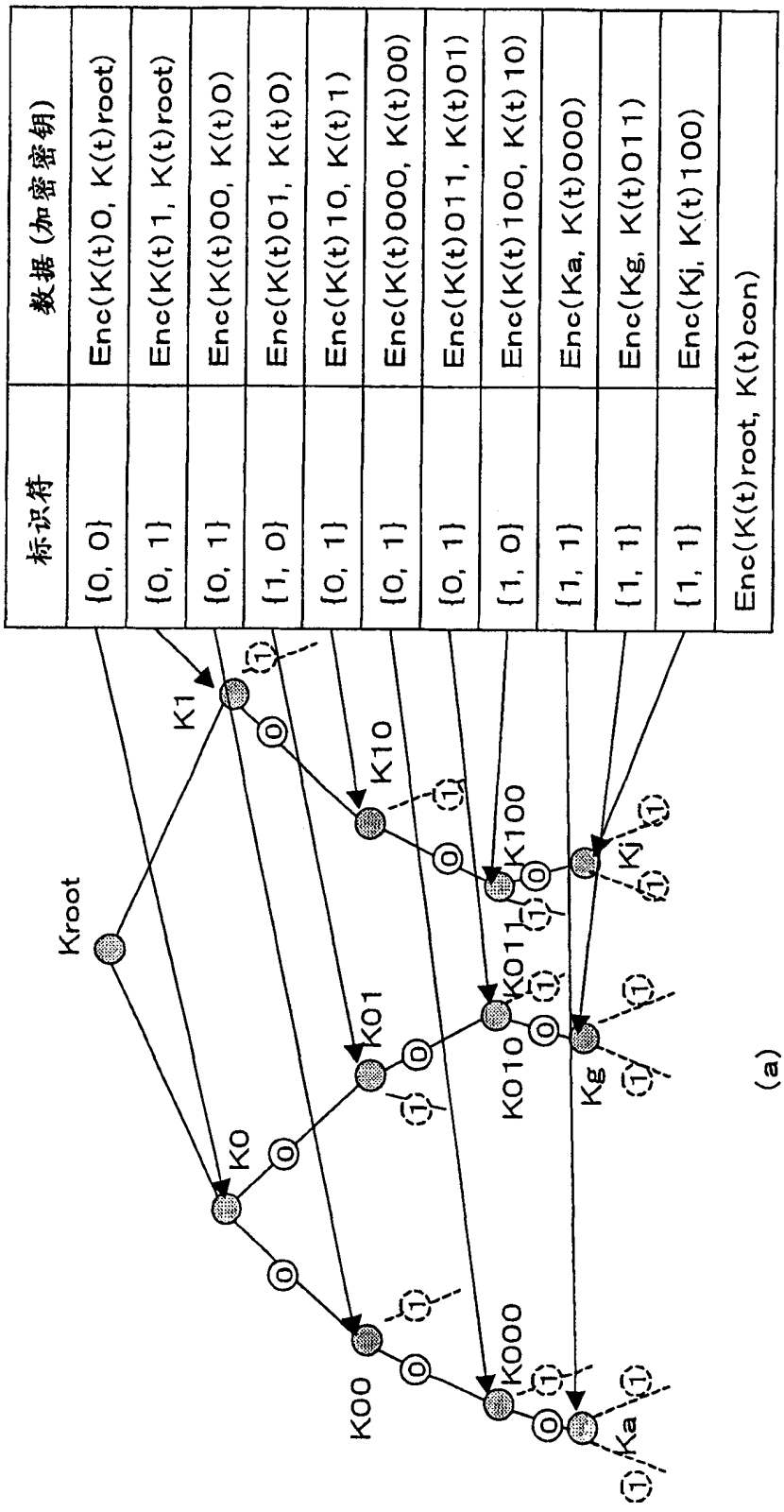

Kroot
K0
K1
K00
K01
K10
K000
K010
K011
K100
Ka
Kg
Kj

图 24

(b)

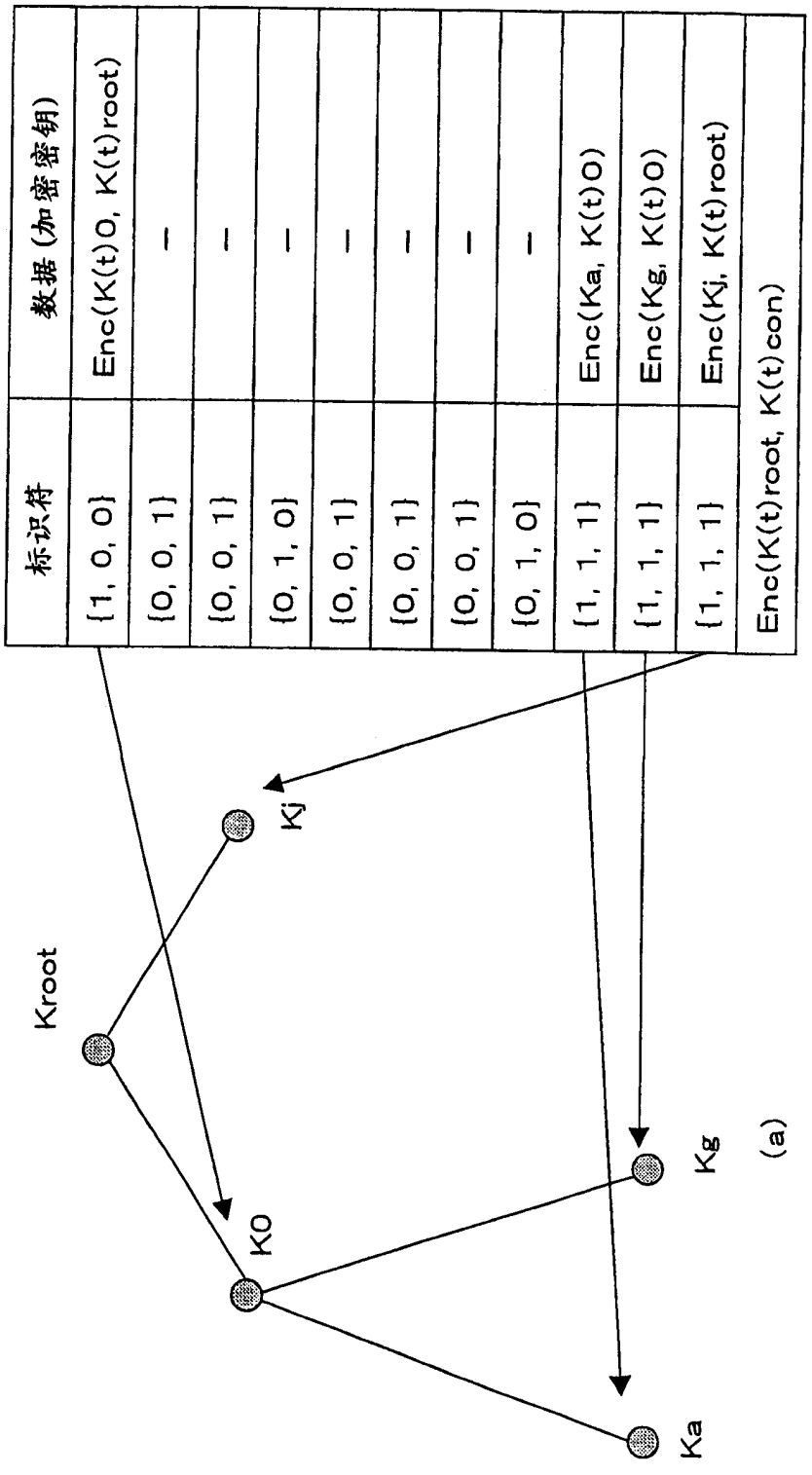


(a)

标识符	数据 (加密密钥)
{0, 0}	Enc(K(t)0, K(t)root)
{0, 1}	Enc(K(t)1, K(t)root)
{0, 1}	Enc(K(t)00, K(t)0)
{1, 0}	Enc(K(t)01, K(t)0)
{0, 1}	Enc(K(t)10, K(t)1)
{0, 1}	Enc(K(t)000, K(t)00)
{0, 1}	Enc(K(t)011, K(t)01)
{1, 0}	Enc(K(t)100, K(t)10)
{1, 1}	Enc(Ka, K(t)000)
{1, 1}	Enc(Kg, K(t)011)
{1, 1}	Enc(Kj, K(t)100)
Enc((K(t)root, K(t)con)	

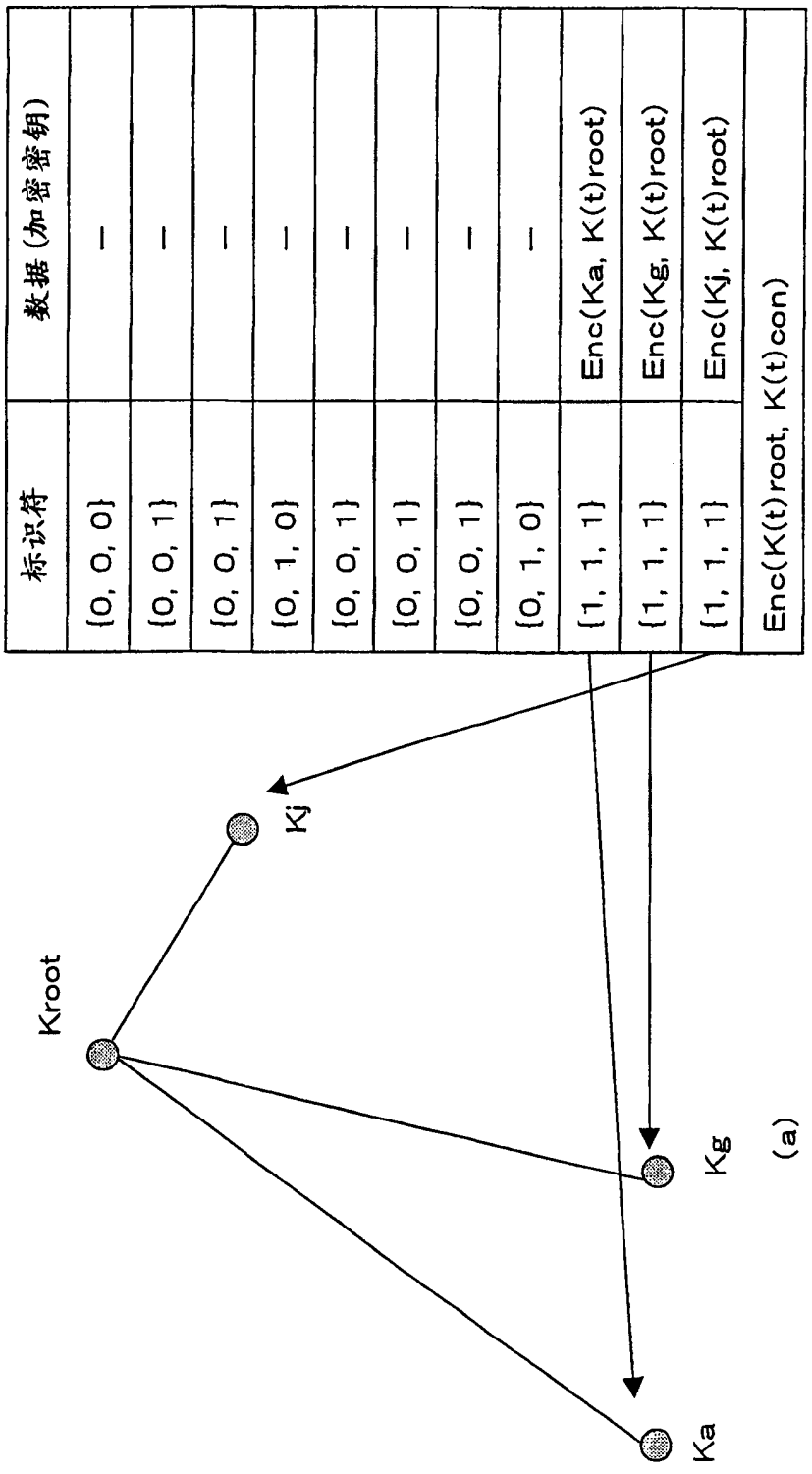
(b)

图 25



标识符	数据(加密密钥)
{1, 0, 0}	Enc(K(t)0, K(t)root)
{0, 0, 1}	—
{0, 0, 1}	—
{0, 1, 0}	—
{0, 0, 1}	—
{0, 0, 1}	—
{0, 0, 1}	—
{0, 1, 0}	—
{1, 1, 1}	Enc(Ka, K(t)0)
{1, 1, 1}	Enc(Kg, K(t)0)
{1, 1, 1}	Enc(Kj, K(t)root)
Enc(K(t)root, K(t)con)	

图 26



标识符	数据(加密密钥)
{0, 0, 0}	—
{0, 0, 1}	—
{0, 0, 1}	—
{0, 1, 0}	—
{0, 0, 1}	—
{0, 0, 1}	—
{0, 0, 1}	—
{0, 1, 0}	—
{1, 1, 1}	Enc(Ka, K(t)root)
{1, 1, 1}	Enc(Kg, K(t)root)
{1, 1, 1}	Enc(Kj, K(t)root)
Enc(K(t)root, K(t)con)	

图 27

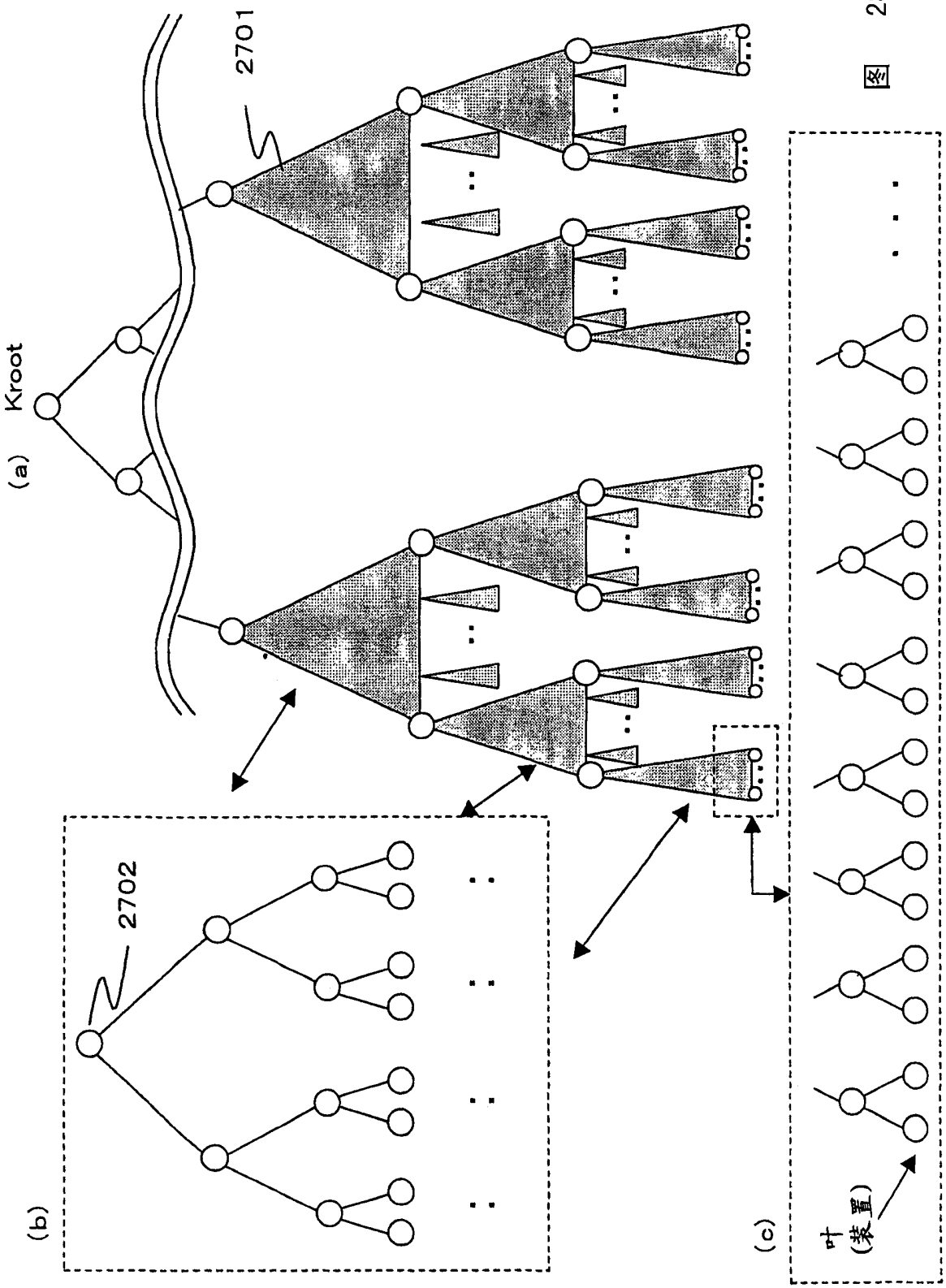


图 28

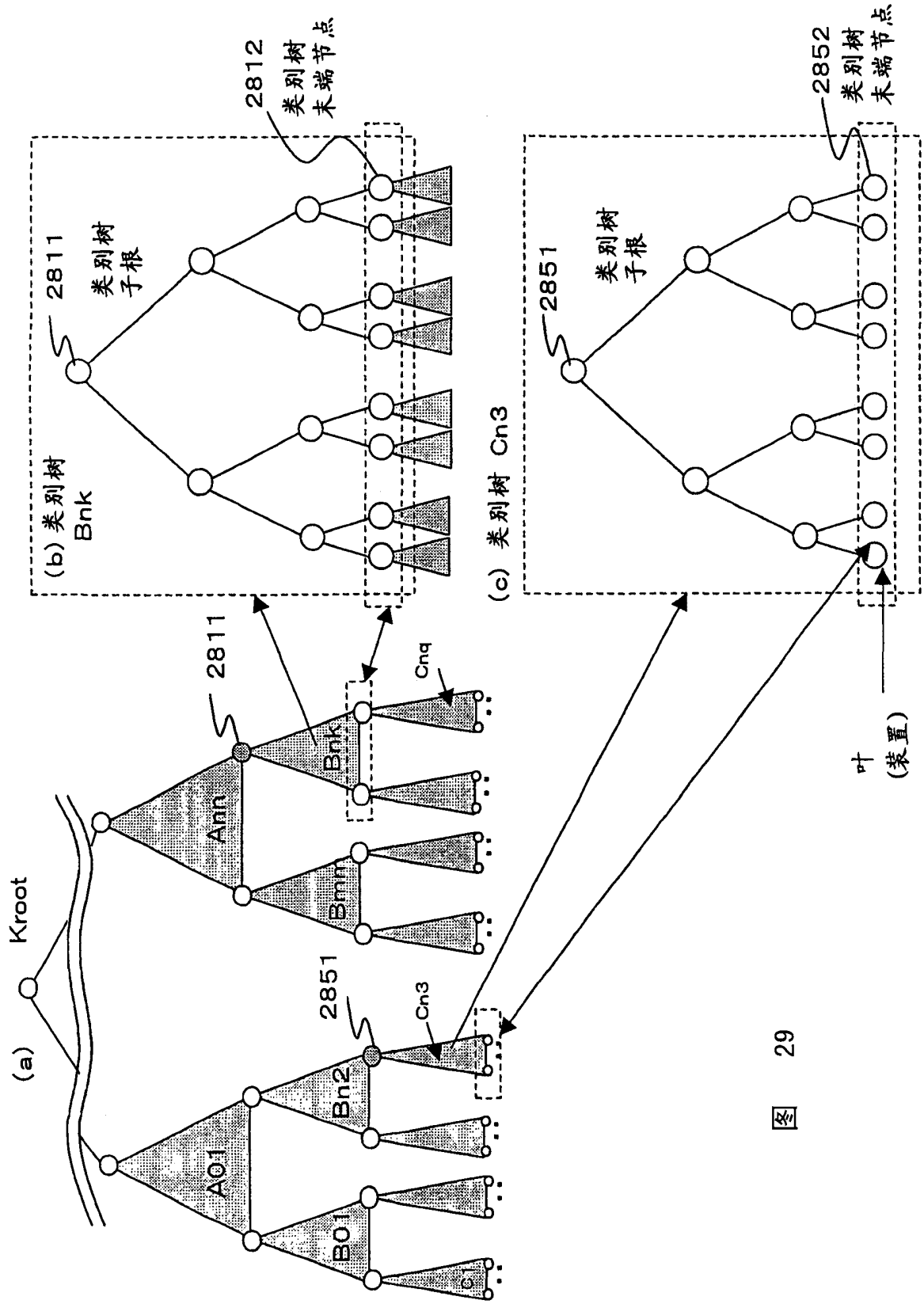

(a)
Kroot
Ann
Bnn
Bnk
Cnq
2811
A01
B01
C1
Bn2
Cn3
2851
(b) 类别树
Bnk
2811
类别树
子根
2812
类别树
末端节点
(c) 类别树 Cn3
2851
类别树
子根
2852
类别树
末端节点
叶
(装置)

图 29

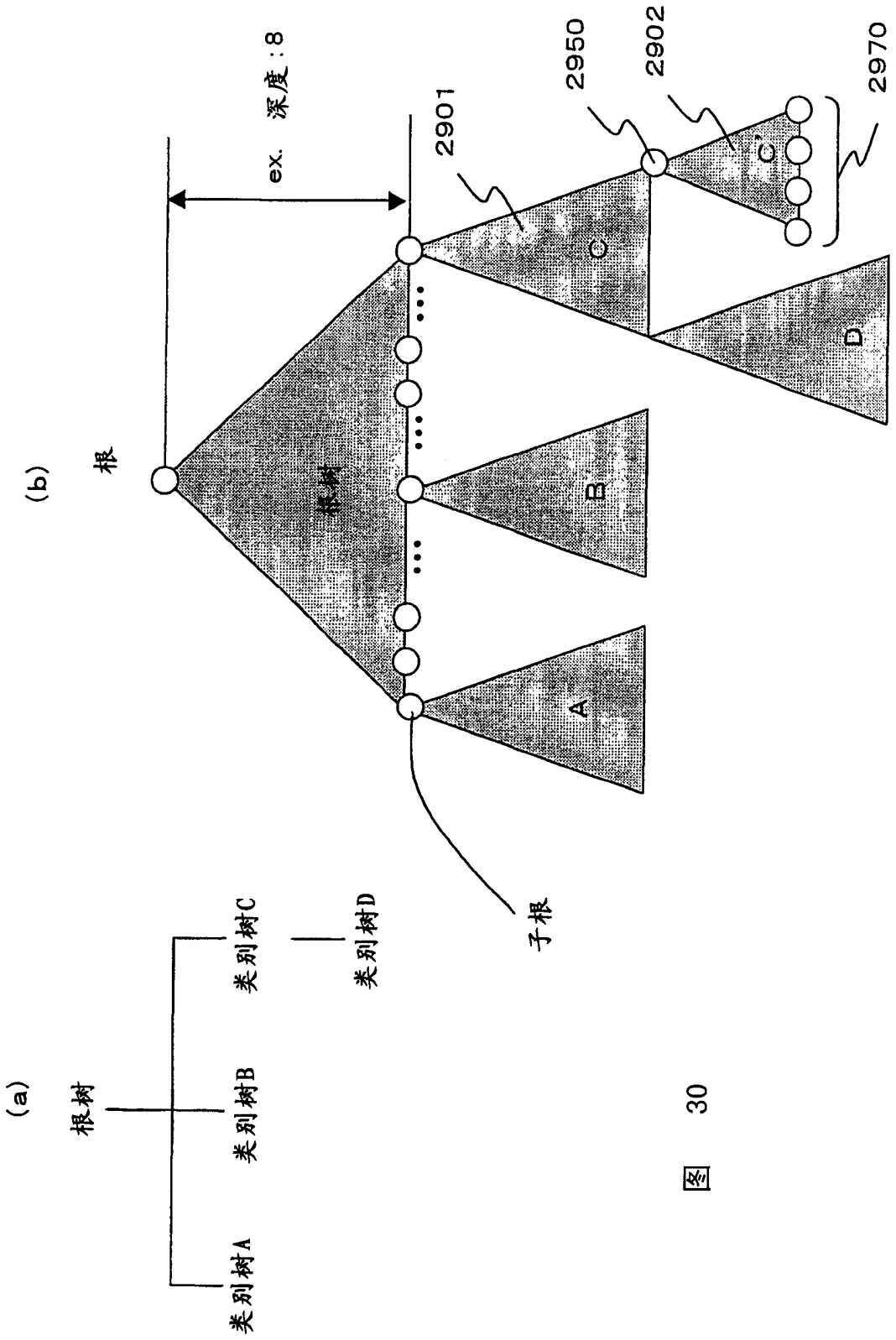

(a)
根树
类别树A
类别树B
类别树C
类别树D
(b)
根
根树
子根
ex. 深度:8
2901
2950
2902
2970
A
B
C
C
D

图 30

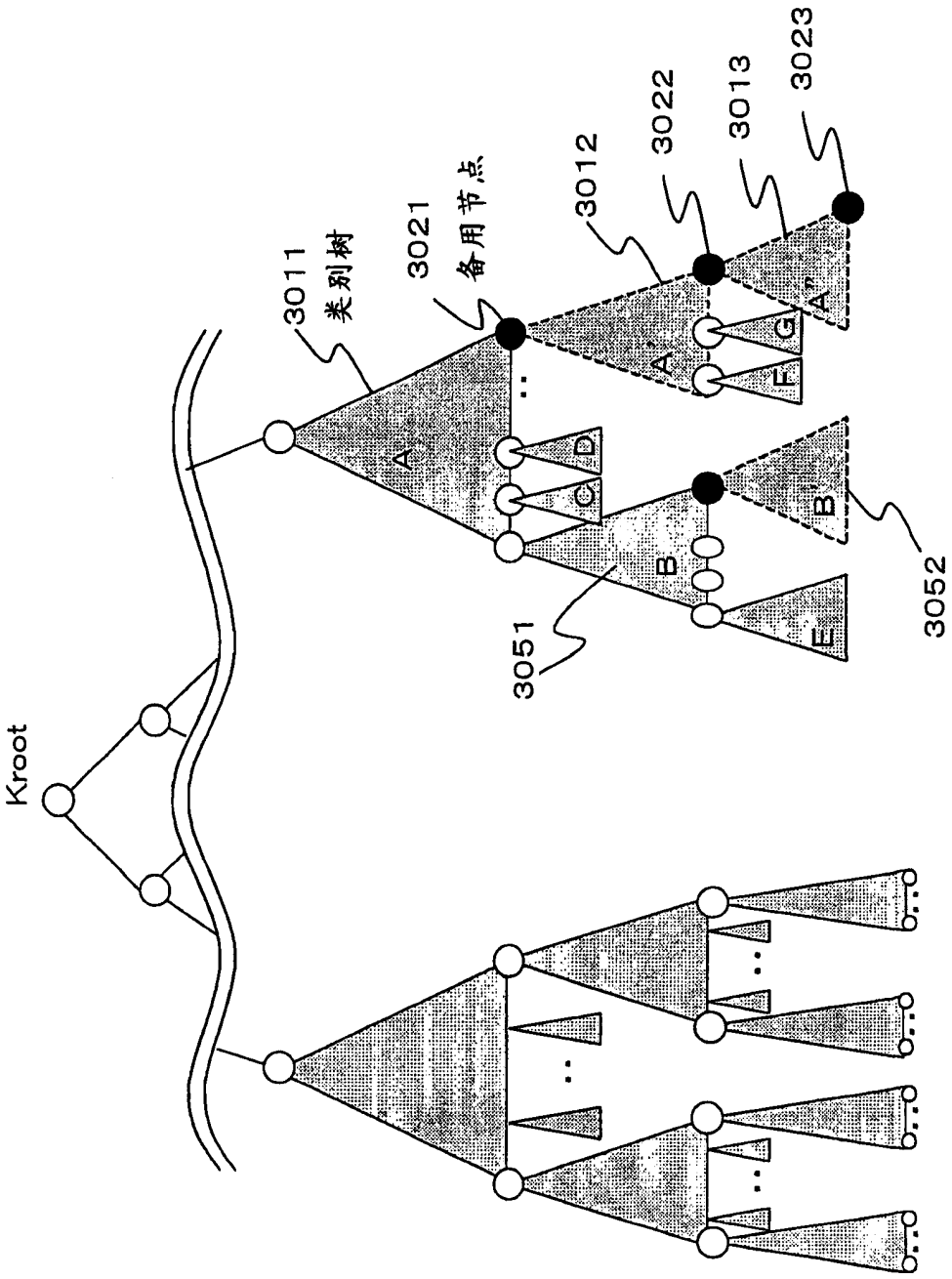

Kroot
3011
类别树
3021
备用节点
3012
3022
3013
3023
3051
3052
A
B
C
D
E
F
G
A'
B'

图 31

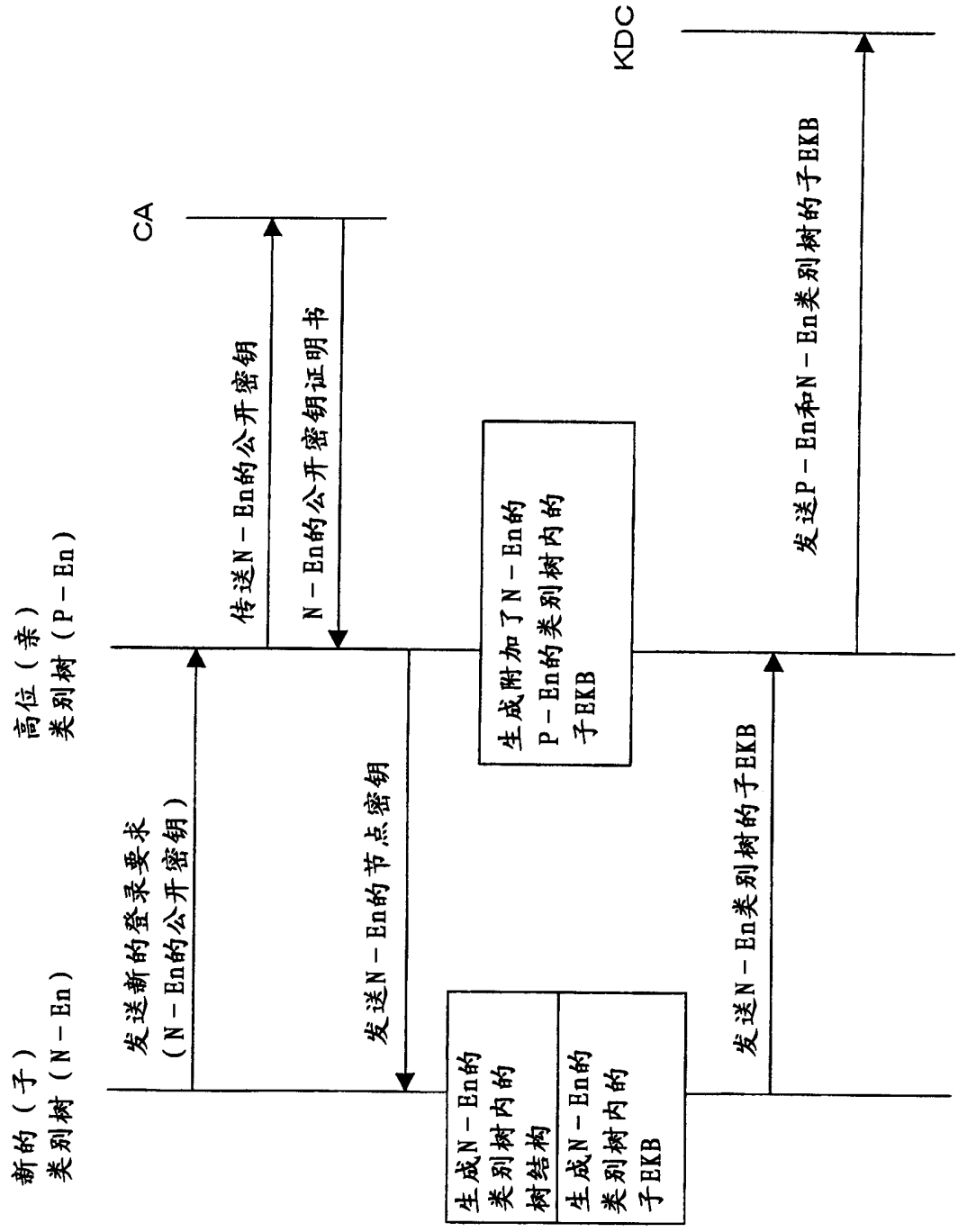

新的（子）
类别树（N－En）
高位（亲）
类别树（P－En）
CA
KDC
发送新的登录要求
（N－En的公开密钥）
传送N－En的公开密钥
N－En的公开密钥证明书
发送N－En的节点密钥
生成附加了N－En的
P－En的类别树内的
子EKB
发送P－En和N－En类别树的子EKB
发送N－En类别树的子EKB
生成N－En的
类别树内的
树结构
生成N－En的
类别树内的
子EKB

图 32

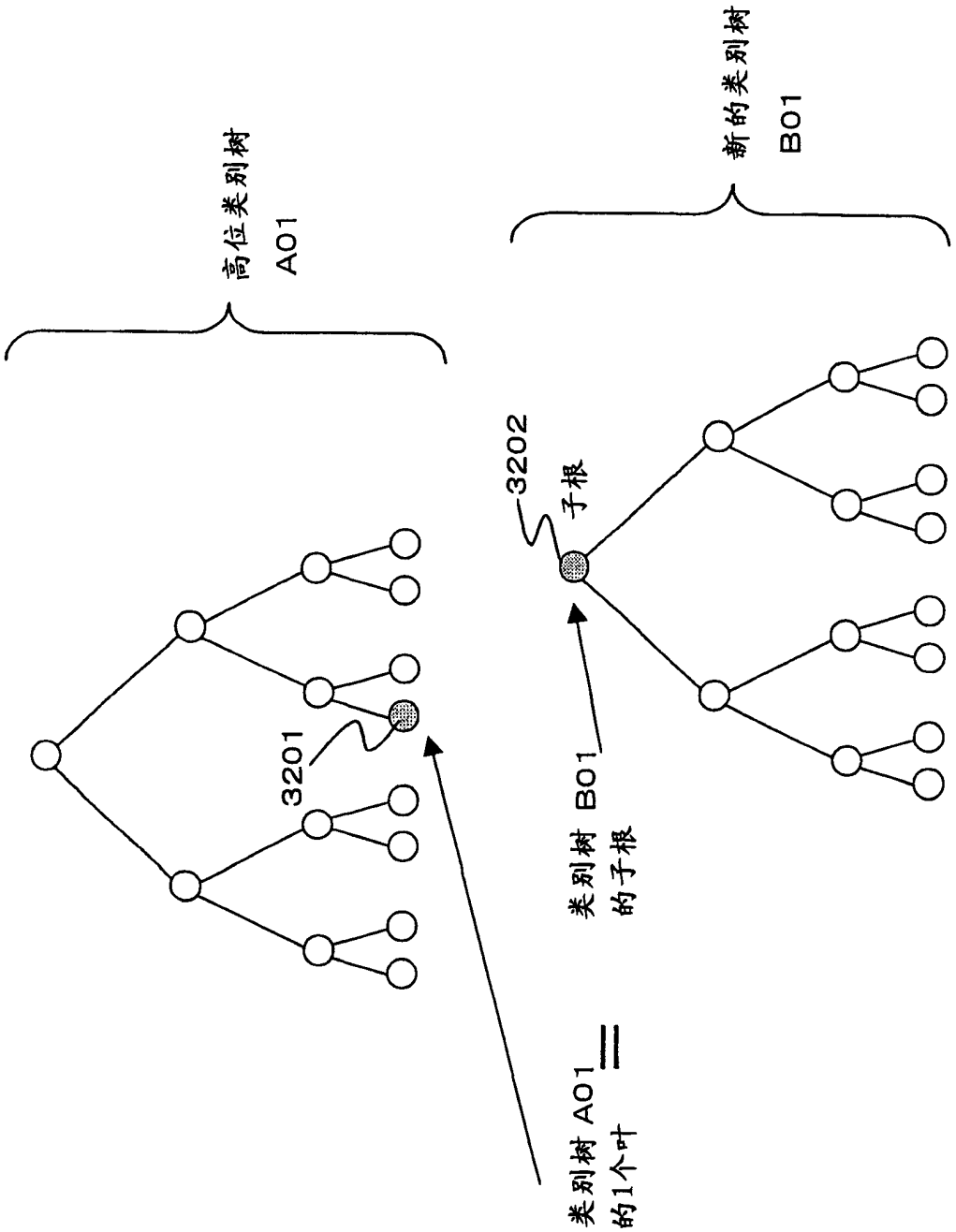


图 33

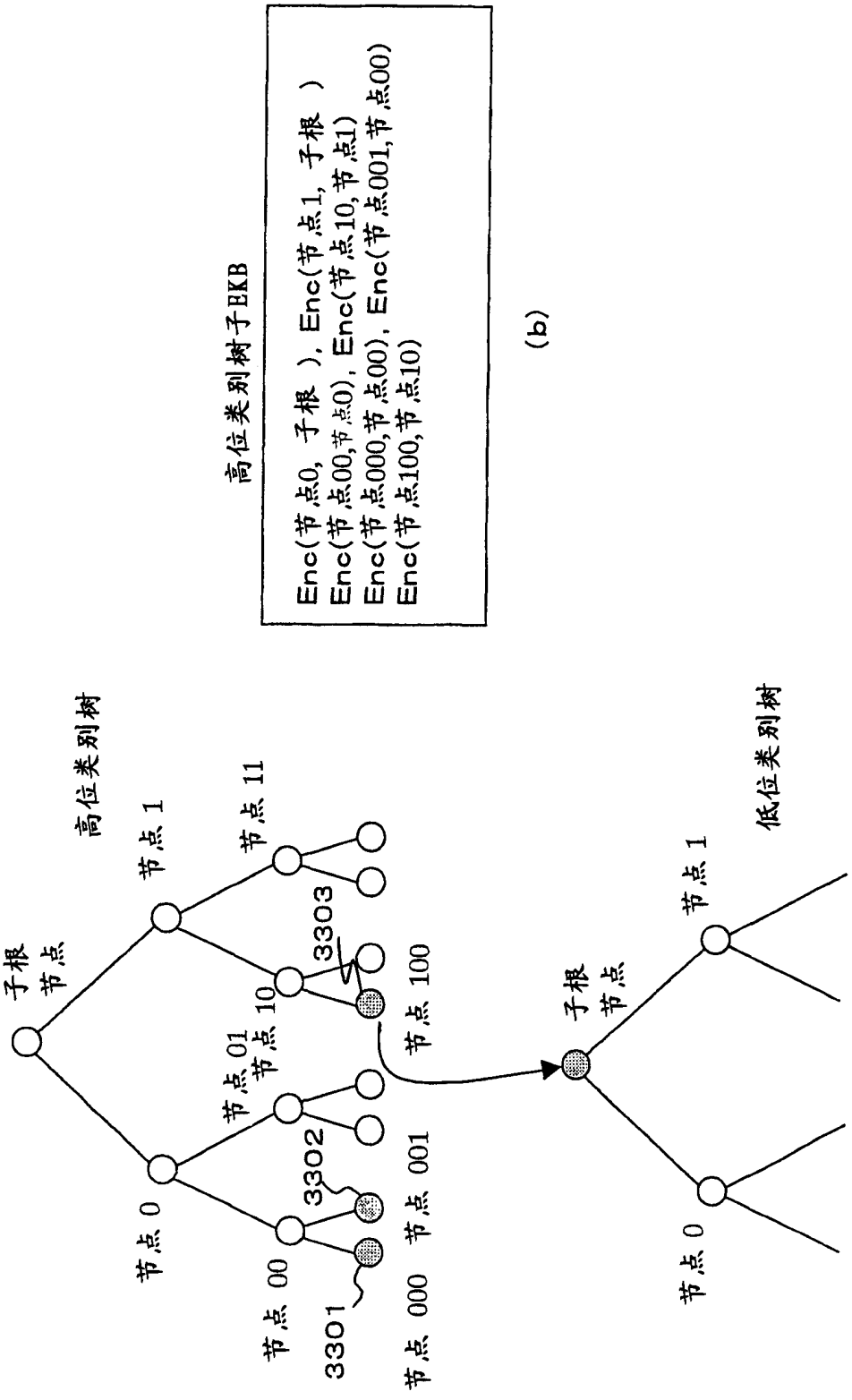

高位类别树子EKB
Enc(节点0, 子根), Enc(节点1, 子根)
Enc(节点00,节点0), Enc(节点10,节点1)
Enc(节点000,节点00), Enc(节点001,节点00)
Enc(节点100,节点10)
(b)
高位类别树
子根节点
节点 0
节点 1
节点 00
节点 01
节点 10
节点 11
节点 000
节点 001
节点 100
3301
3302
3303
子根节点
节点 0
节点 1
低位类别树
(a)

图 34

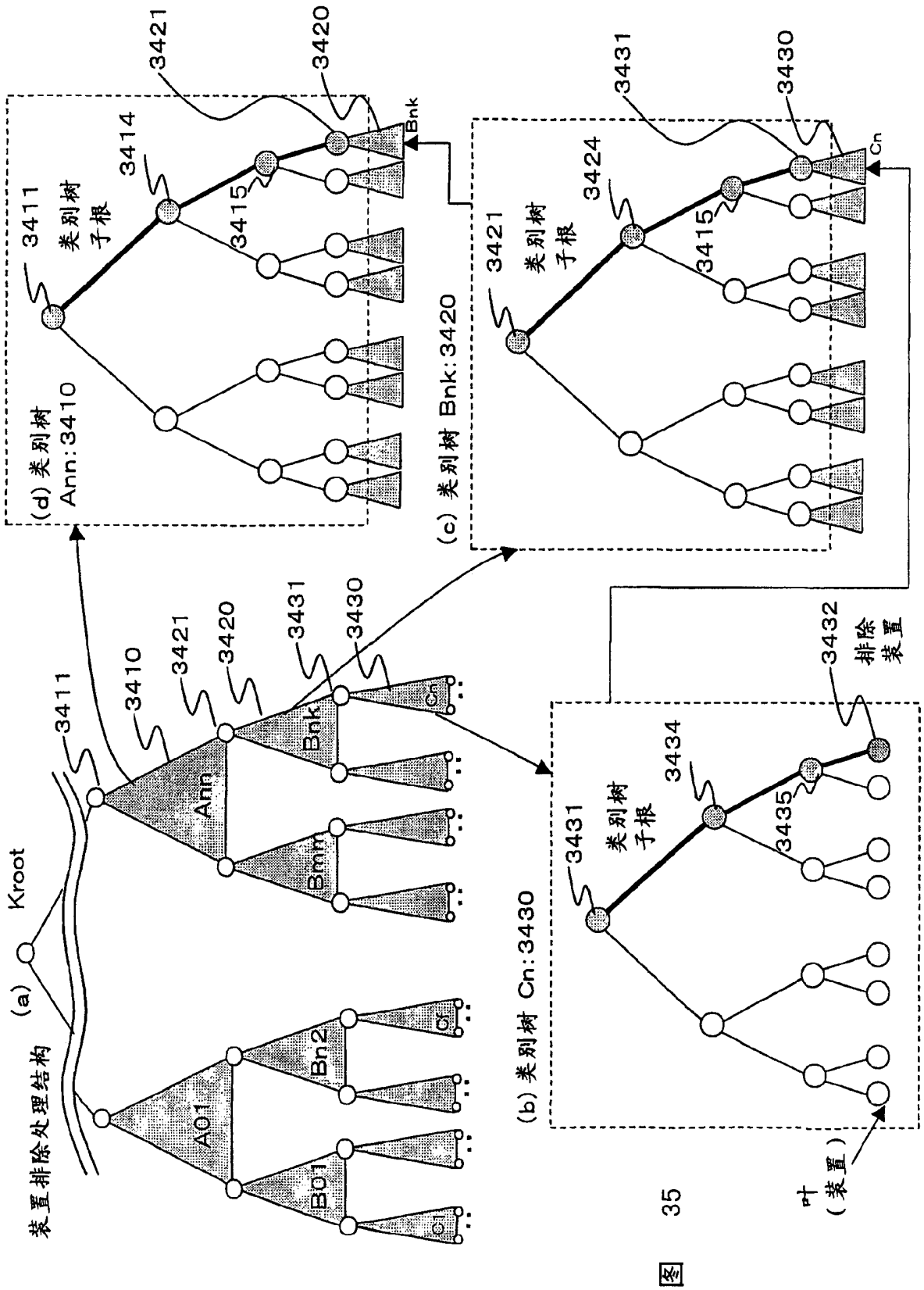

装置排除处理结构
(a)
Kroot
3411
3410
3421
3420
3431
3430
Ann
Bnk
Bmm
A01
B01
C1
Bn2
Cn
(d) 类别树
Ann:3410
3411
类别树
子根
3414
3415
3421
3420
Bnk
(c) 类别树 Bnk:3420
3421
类别树
子根
3424
3415
3431
3430
Cn
(b) 类别树 Cn:3430
3431
类别树
子根
3434
3435
3432
排除
装置
叶
(装置)

图 35

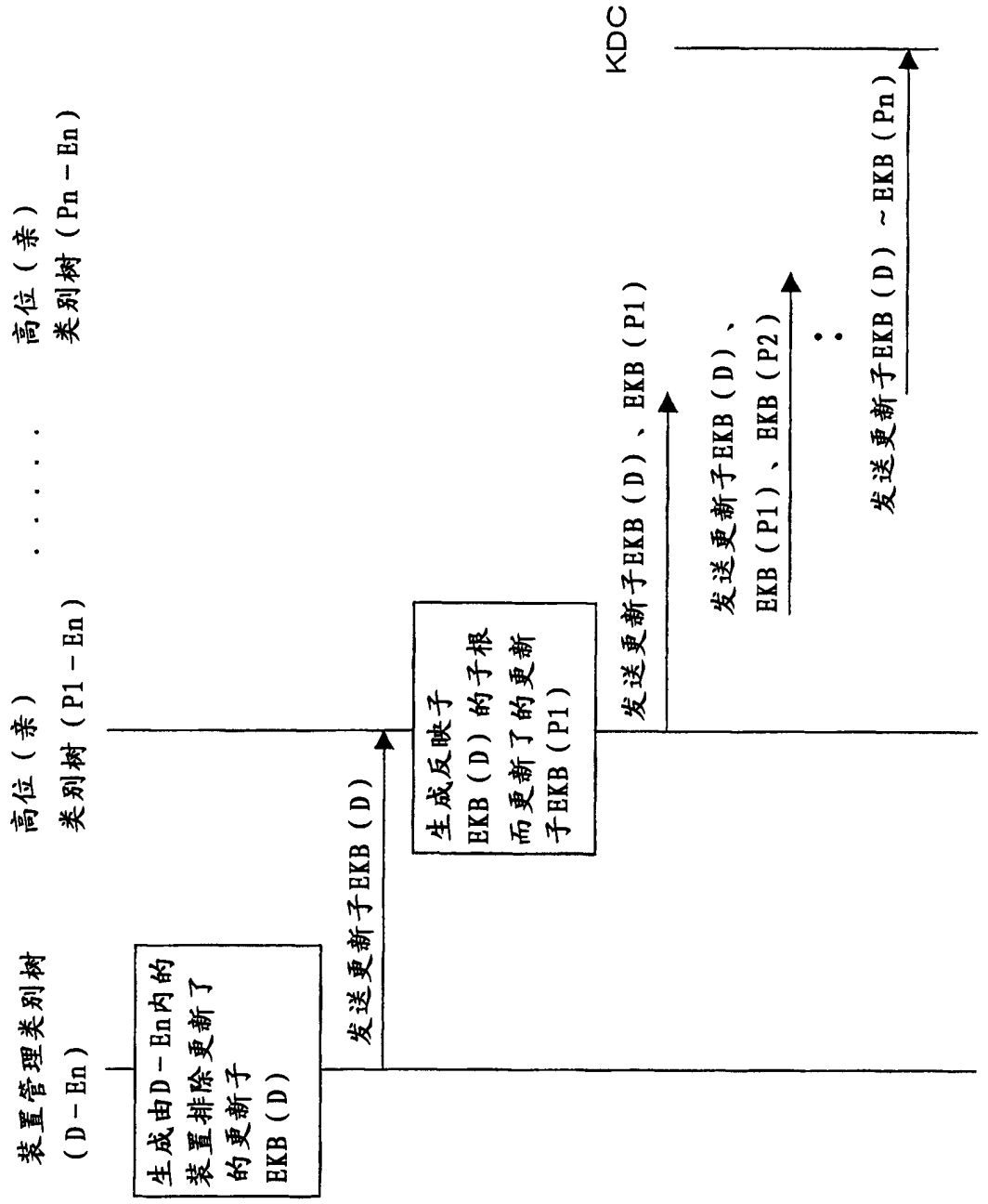
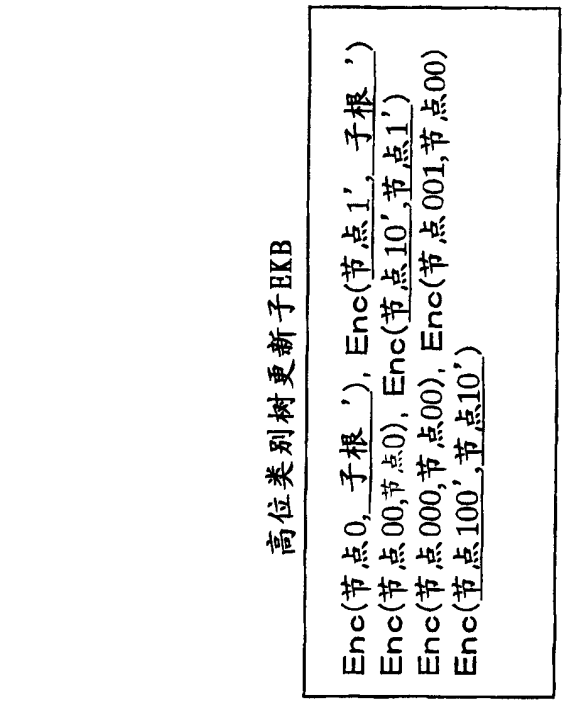
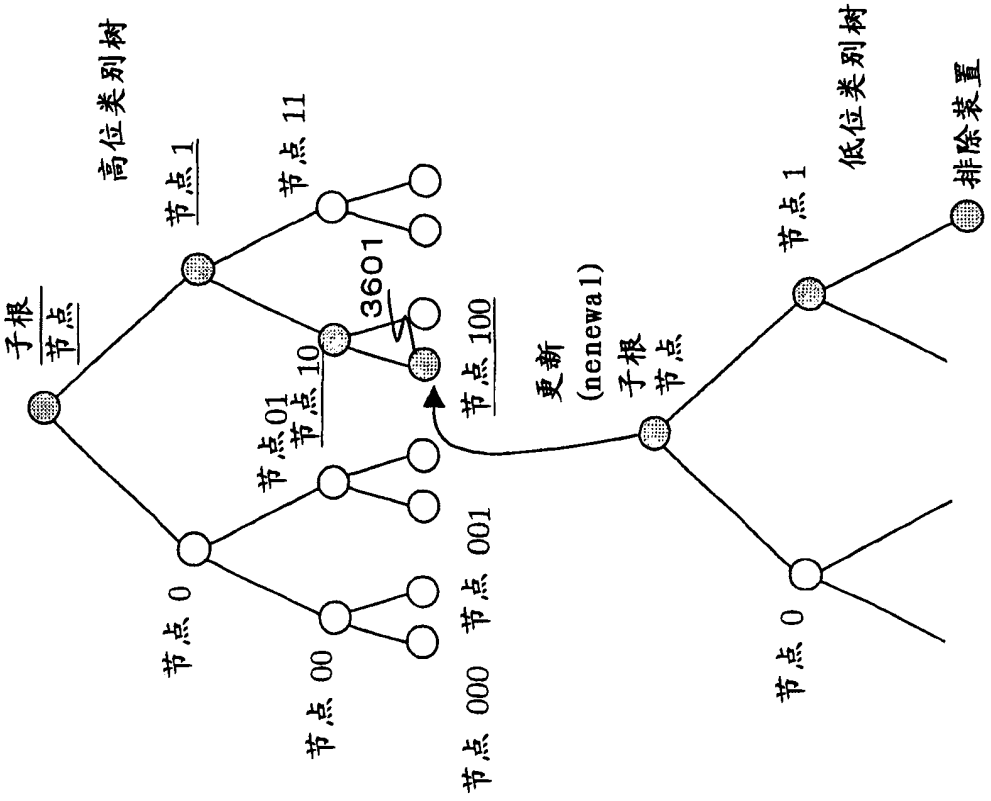

装置管理类别树
(D-En)
高位(亲)
类别树(P1-En)
.....
高位(亲)
类别树(Pn-En)
KDC
生成由D-En内的装置排除更新了的更新子EKB(D)
发送更新子EKB(D)
生成反映子EKB(D)的子根而更新了的更新子EKB(P1)
发送更新子EKB(D)、EKB(P1)
发送更新子EKB(D)、EKB(P1)、EKB(P2)
发送更新子EKB(D)~EKB(Pn)

图 36


高位类别树更新子EKB
Enc(节点0, 子根 '), Enc(节点1', 子根 ')
Enc(节点00,节点0), Enc(节点10',节点1')
Enc(节点000,节点00), Enc(节点001,节点00)
Enc(节点100',节点10')

(b)


高位类别树
子根 节点
节点 0
节点 1
节点 00
节点 01
节点 10
节点 11
节点 000
节点 001
节点 100
3601
更新
(nenewal)
子根
节点
节点 0
节点 1
低位类别树
排除装置

(a)

图 37

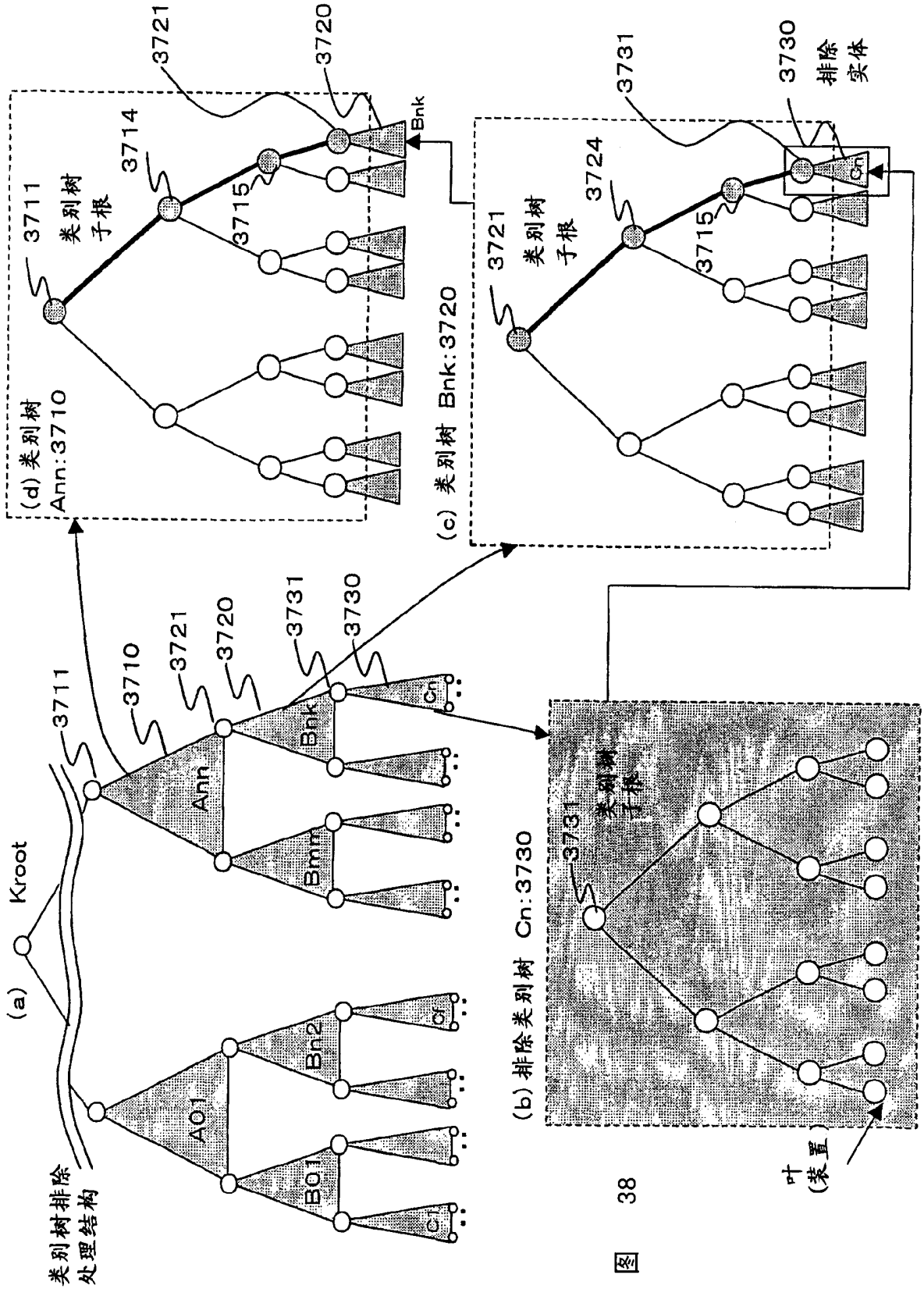

类别树排除
处理结构
(a)
Kroot
3711
3710
3721
3720
3731
3730
Ann
Bnk
Bmn
Cn
A01
B01
C1
Bn2
Cr
(b) 排除类别树 Cn:3730
3731
类别树
子根
叶
(装置)
(c) 类别树 Bnk:3720
3721
类别树
子根
3724
3715
3731
3730
排除
实体
Cn
(d) 类别树
Ann:3710
3711
类别树
子根
3714
3715
3721
3720
Bnk

图 38

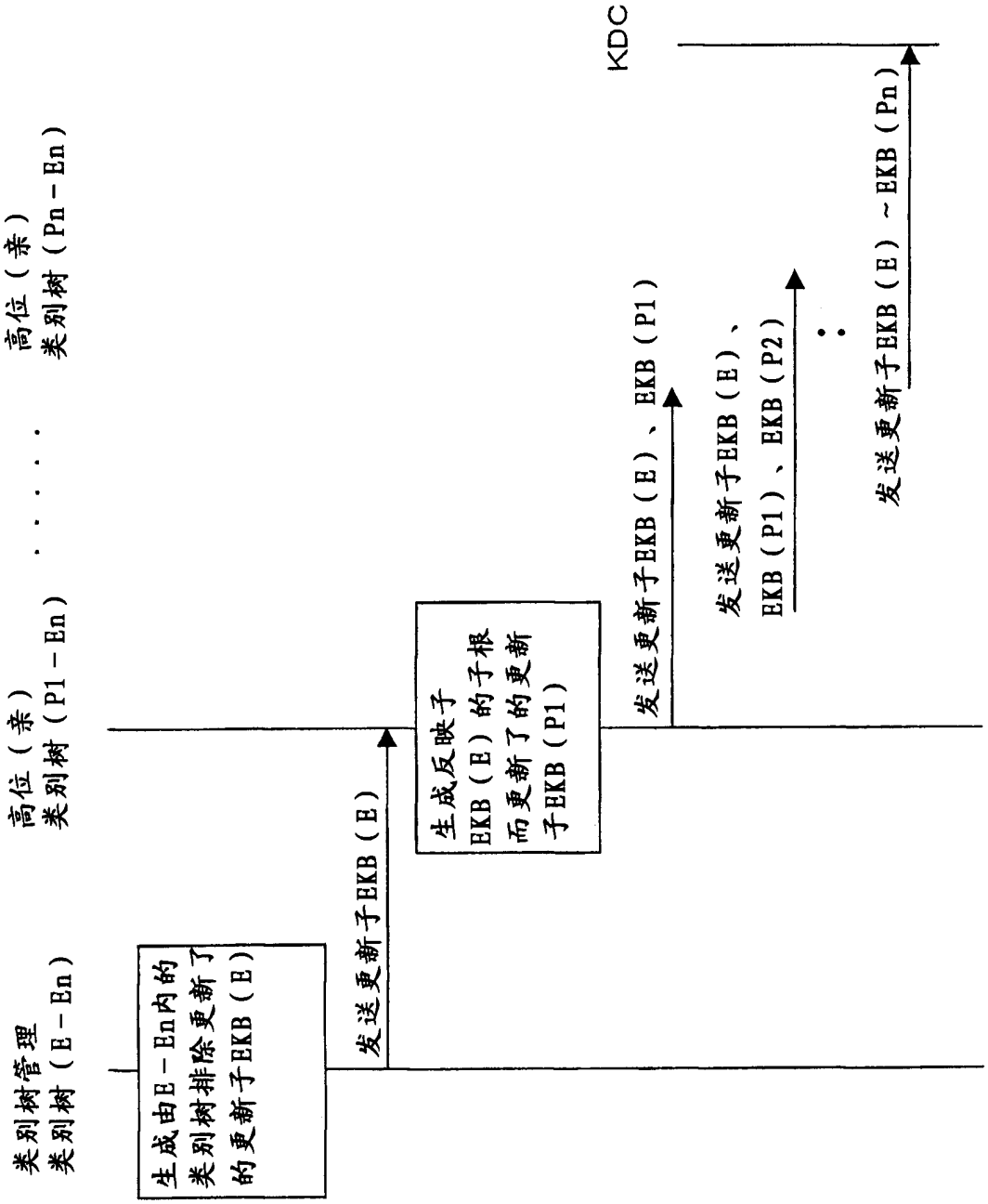

类别树管理
类别树（E－En）
高位（亲）
类别树（P1－En）
高位（亲）
类别树（Pn－En）
KDC
生成由E－En内的类别树排除更新了的更新子EKB（E）
发送更新子EKB（E）
生成反映子EKB（E）的子根而更新了的更新子EKB（P1）
发送更新子EKB（E）、EKB（P1）
发送更新子EKB（E）、EKB（P1）、EKB（P2）
发送更新子EKB（E）～EKB（Pn）

图 39

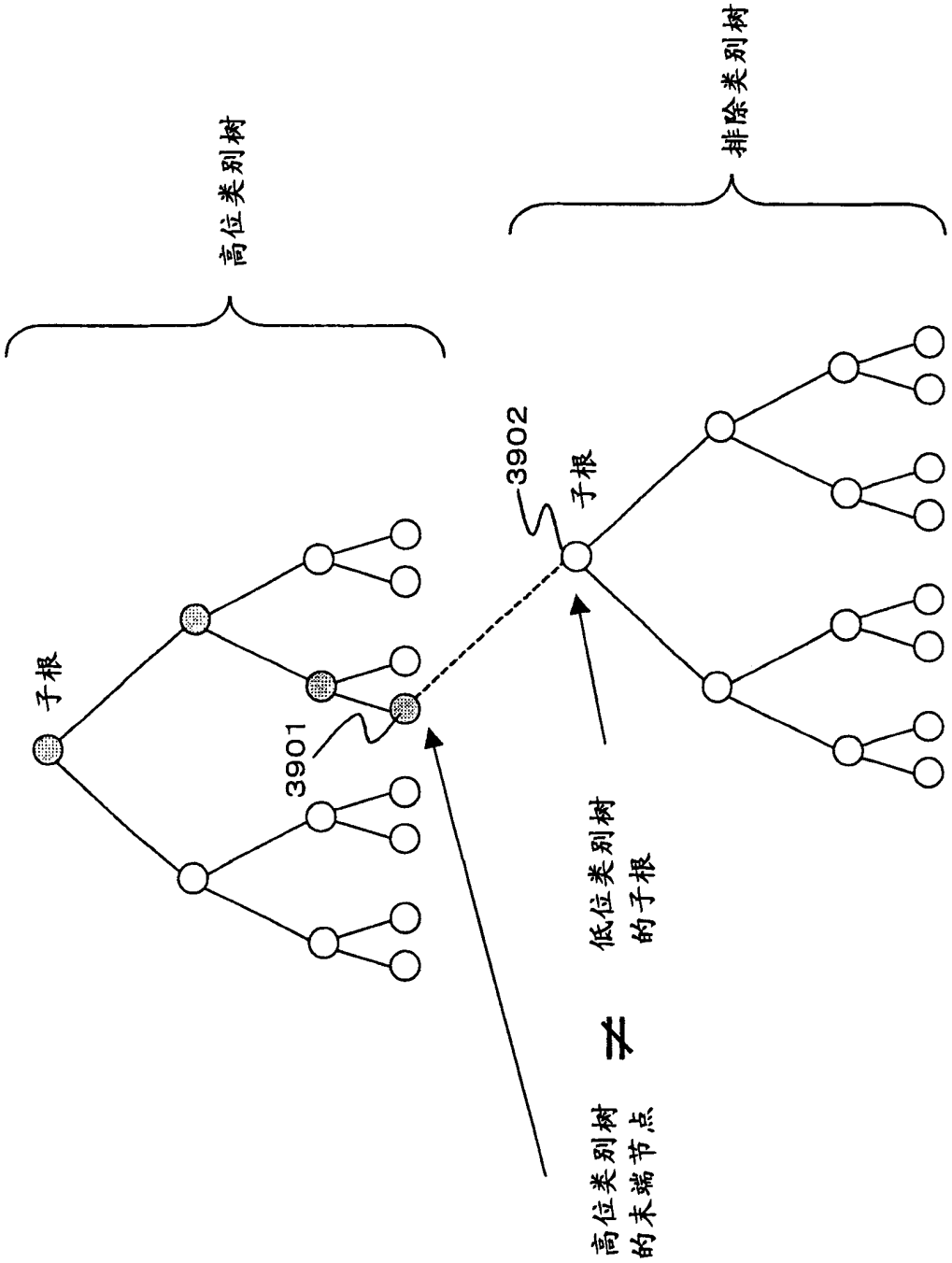


图 40

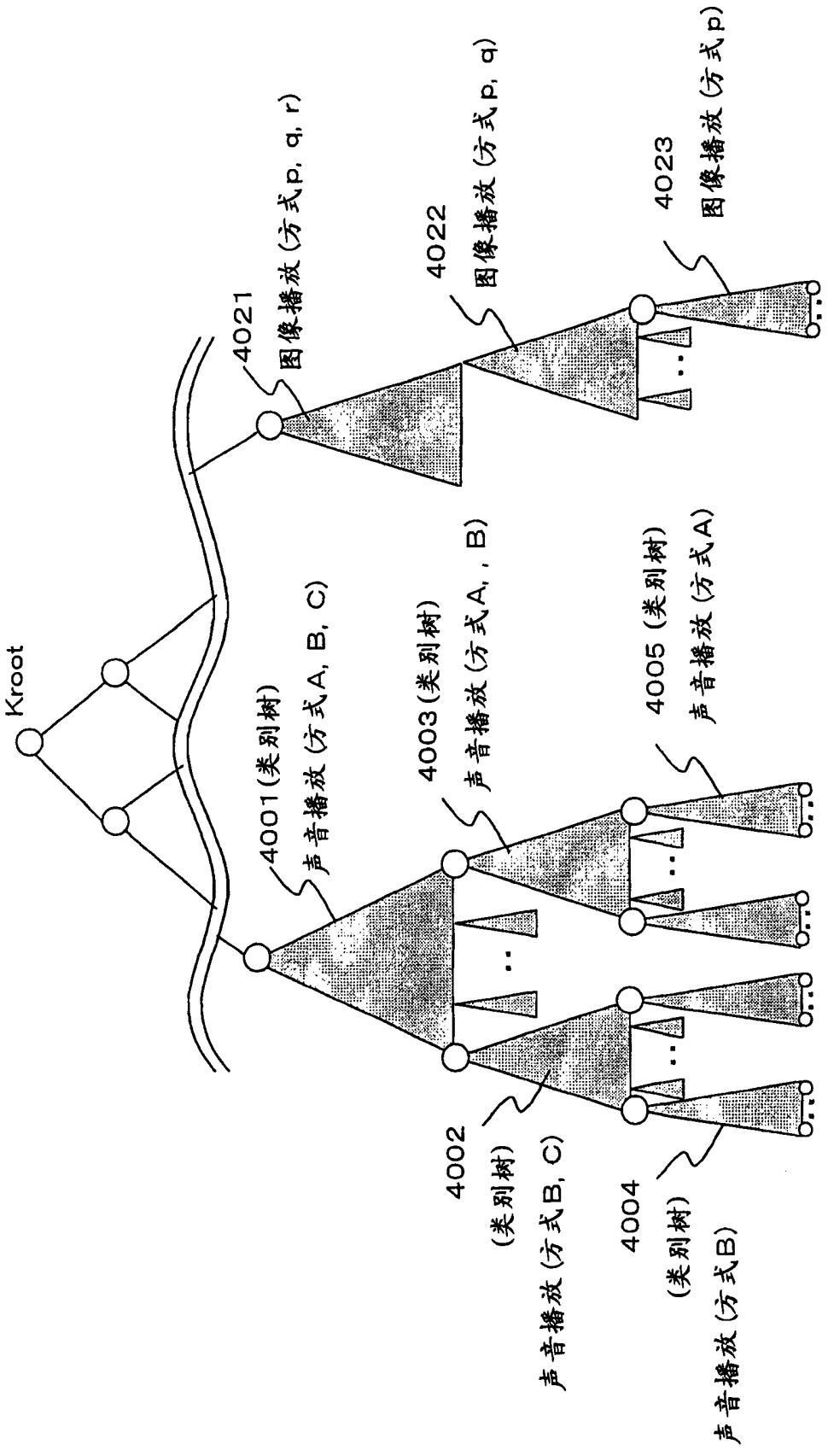

Kroot
4001(类别树)
声音播放(方式A, B, C)
4002
(类别树)
声音播放(方式B, C)
4003(类别树)
声音播放(方式A, , B)
4004
(类别树)
声音播放(方式B)
4005(类别树)
声音播放(方式A)
4021
图像播放(方式p, q, r)
4022
图像播放(方式p, q)
4023
图像播放(方式p)

图 41

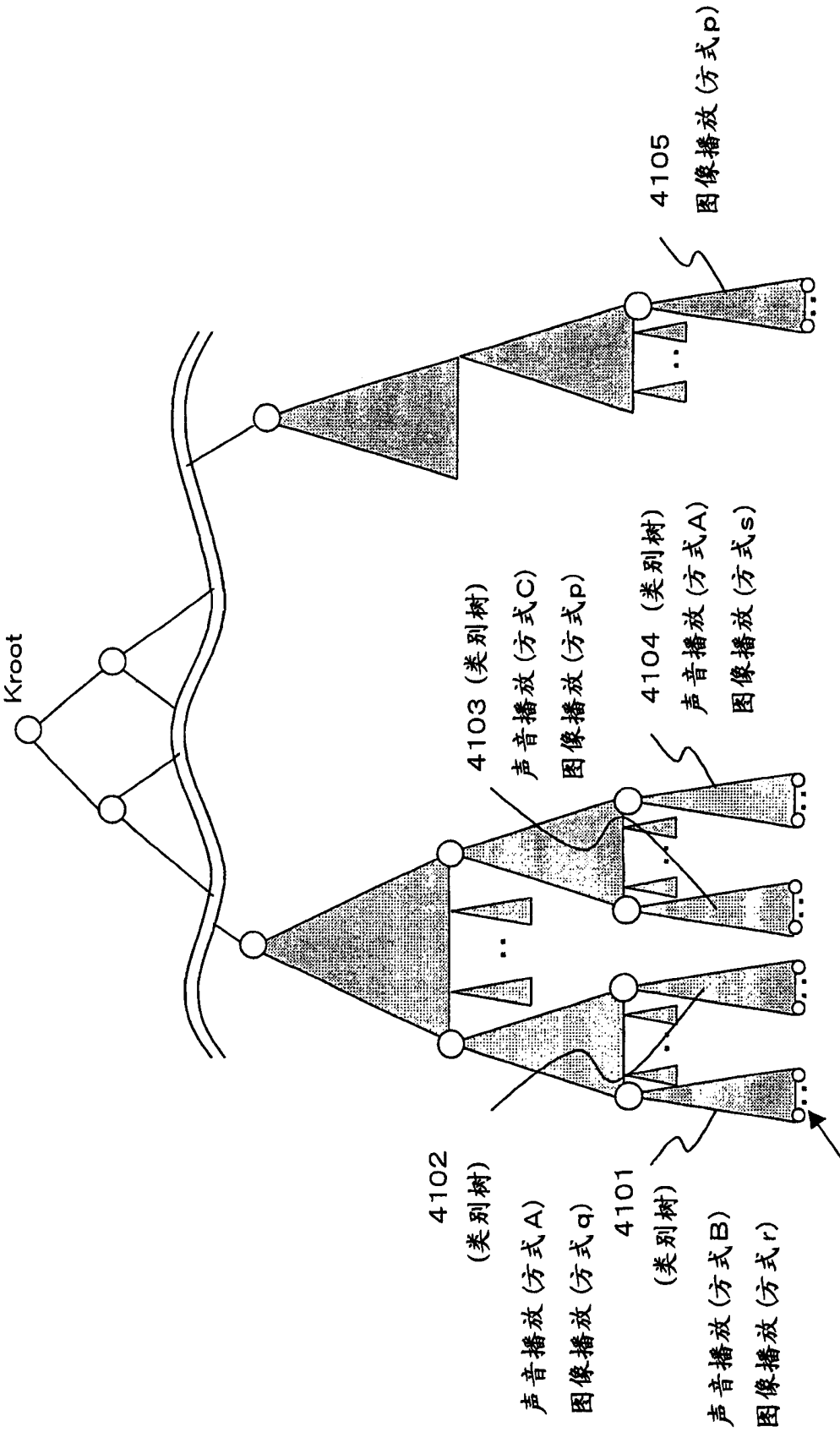

Kroot
4102
(类别树)
声音播放(方式A)
图像播放(方式q)
4101
(类别树)
声音播放(方式B)
图像播放(方式r)
装置
4103 (类别树)
声音播放(方式C)
图像播放(方式p)
4104 (类别树)
声音播放(方式A)
图像播放(方式s)
4105
图像播放(方式p)

图 42

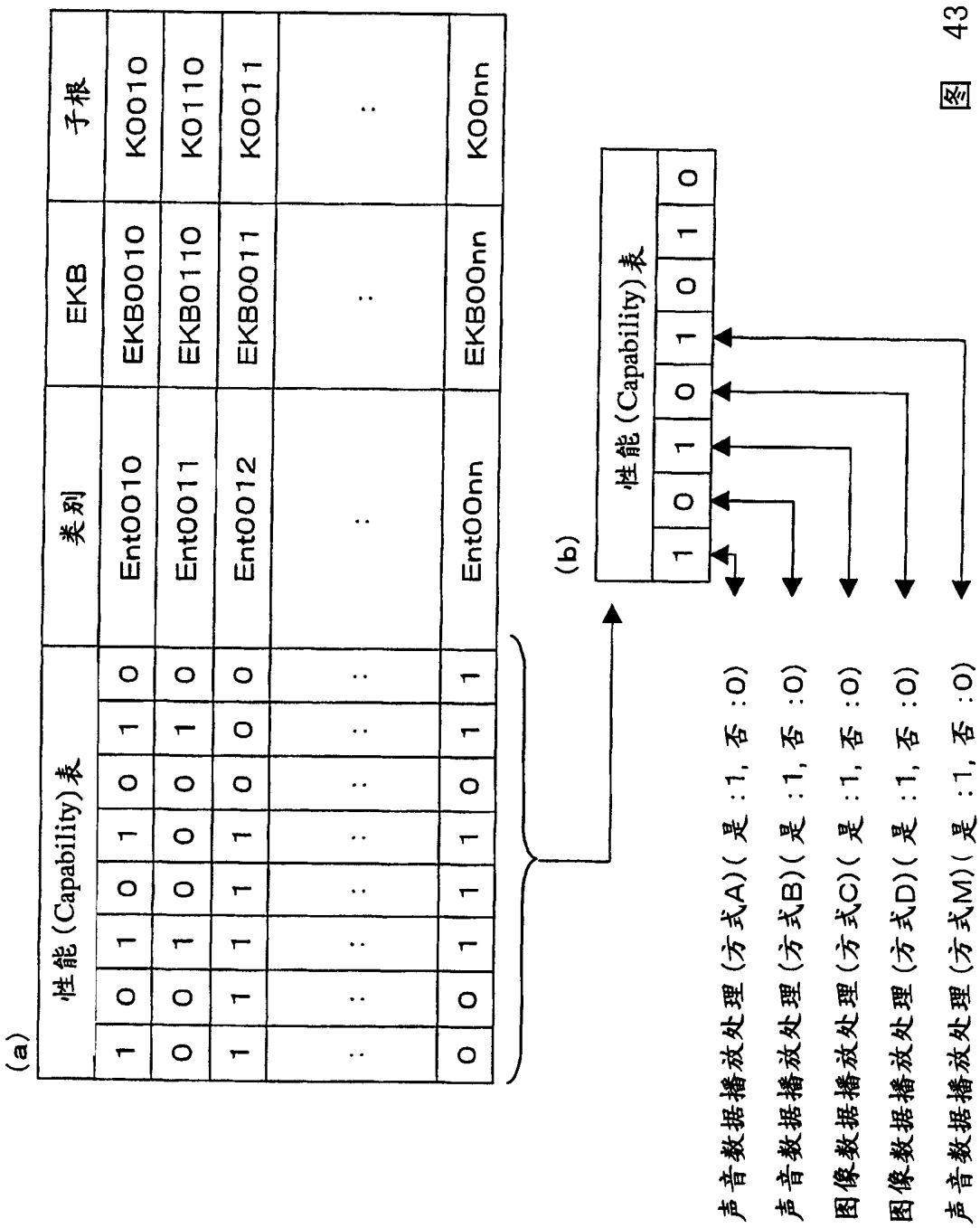

(a)
性能 (Capability)表
类别
EKB
子根
Ent0010
EKB0010
K0010
Ent0011
EKB0110
K0110
Ent0012
EKB0011
K0011
Ent00nn
EKB00nn
K00nn
(b)
性能 (Capability)表
声音数据播放处理 (方式A)(是 :1, 否 :0)
声音数据播放处理 (方式B)(是 :1, 否 :0)
图像数据播放处理 (方式C)(是 :1, 否 :0)
图像数据播放处理 (方式D)(是 :1, 否 :0)
声音数据播放处理 (方式M)(是 :1, 否 :0)

图 43

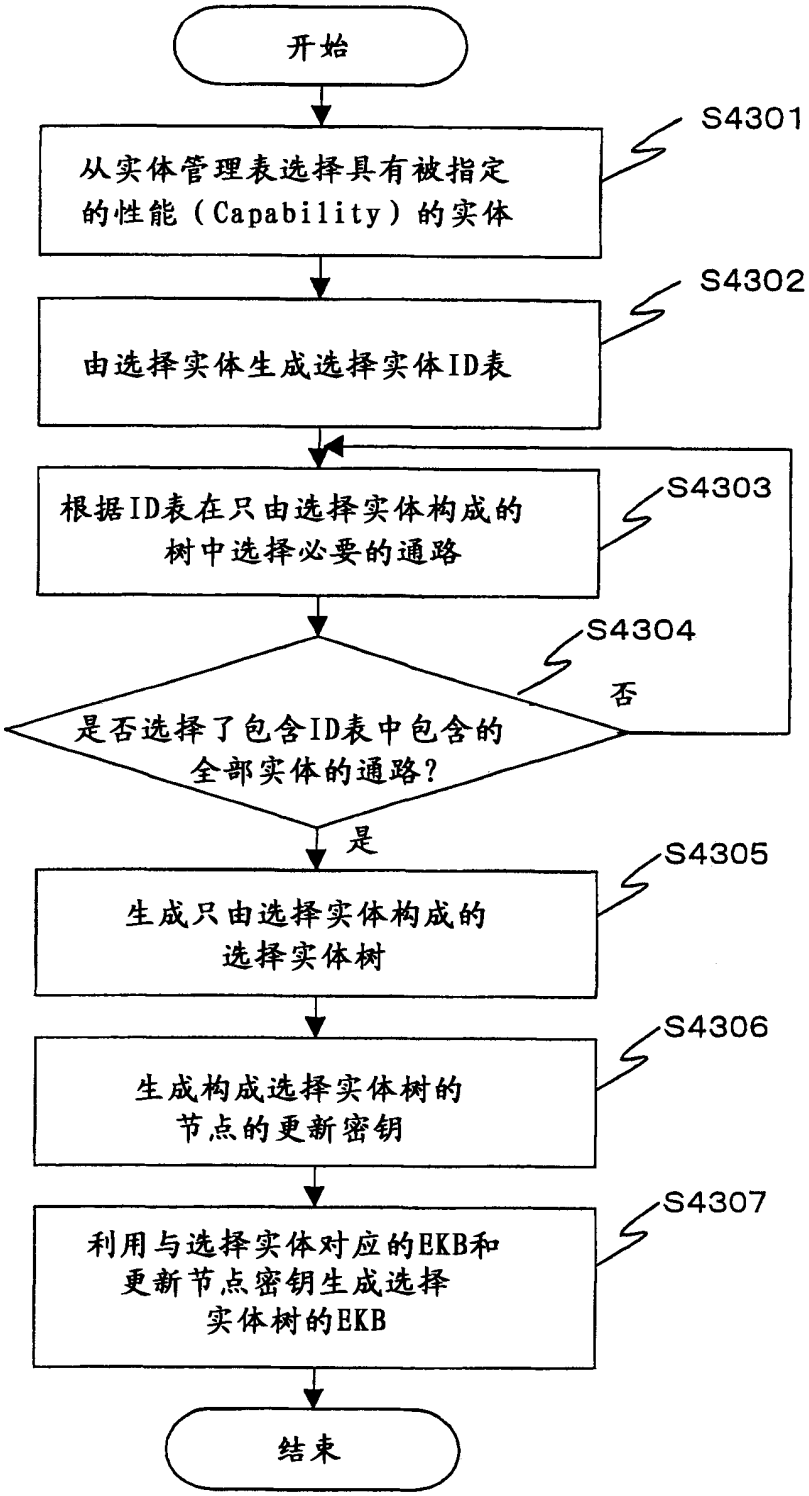

开始
S4301
从实体管理表选择具有被指定的性能（Capability）的实体
S4302
由选择实体生成选择实体ID表
S4303
根据ID表在只由选择实体构成的树中选择必要的通路
S4304
否
是否选择了包含ID表中包含的全部实体的通路？
是
S4305
生成只由选择实体构成的选择实体树
S4306
生成构成选择实体树的节点的更新密钥
S4307
利用与选择实体对应的EKB和更新节点密钥生成选择实体树的EKB
结束

图 44

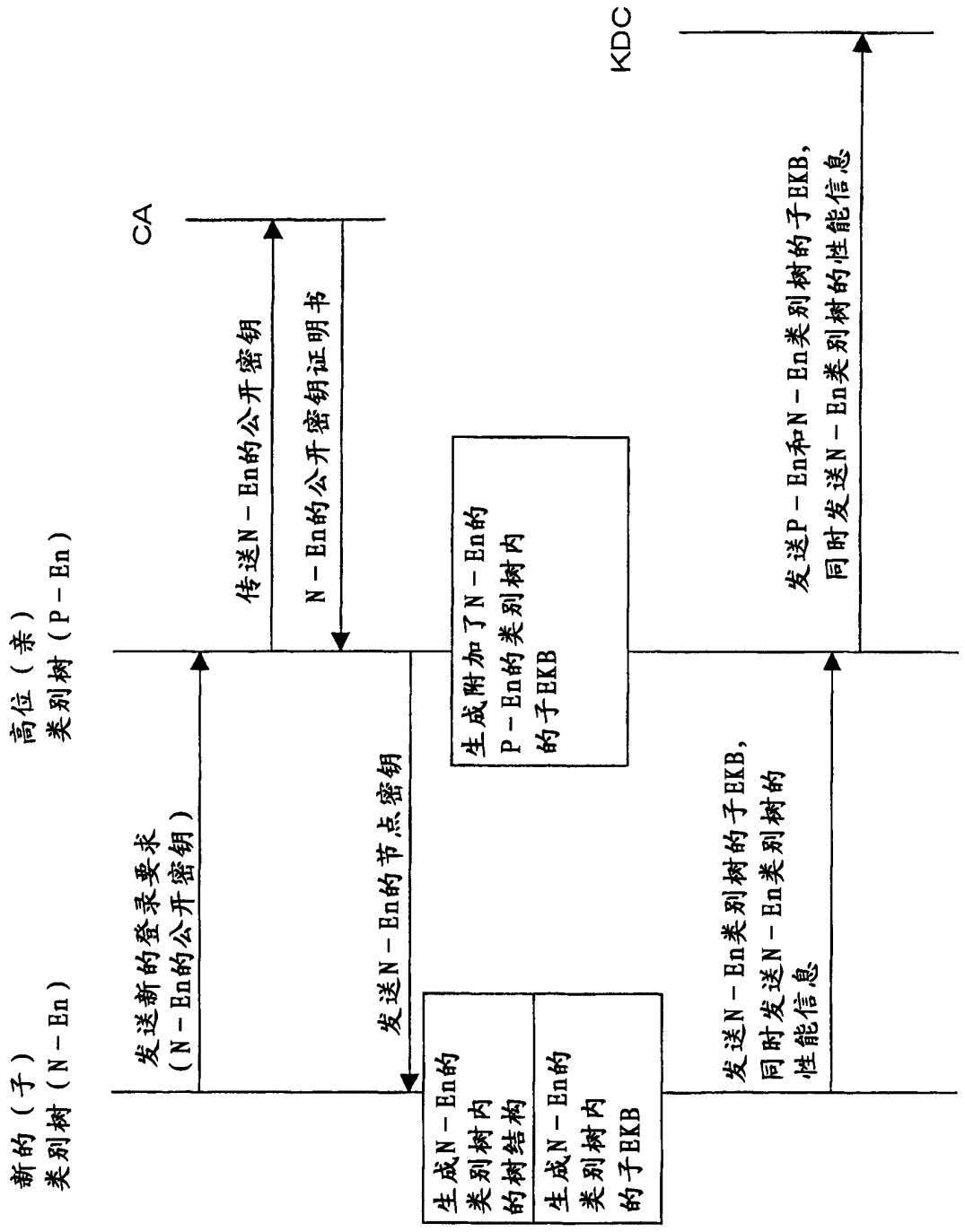

新的（子）
类别树（N－En）
高位（亲）
类别树（P－En）
CA
KDC
发送新的登录要求
（N－En的公开密钥）
传送N－En的公开密钥
N－En的公开密钥证明书
发送N－En的节点密钥
生成附加了N－En的
P－En的类别树内
的子EKB
发送P－En和N－En类别树的子EKB，
同时发送N－En类别树的性能信息
生成N－En的
类别树内
的树结构
生成N－En的
类别树内
的子EKB
发送N－En类别树的子EKB，
同时发送N－En类别树的
性能信息

图 45

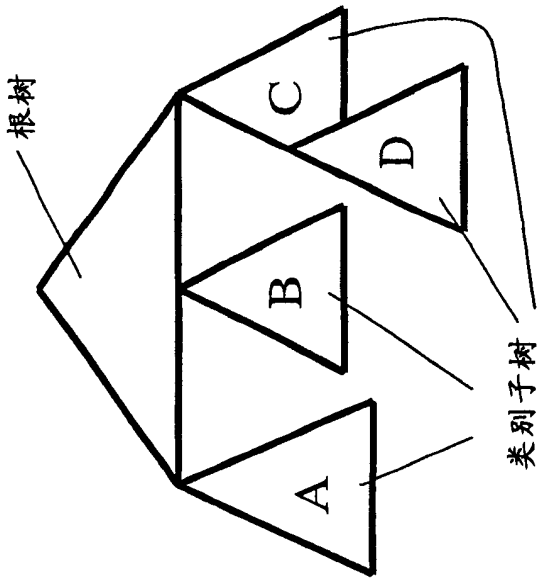


图 46

图 47

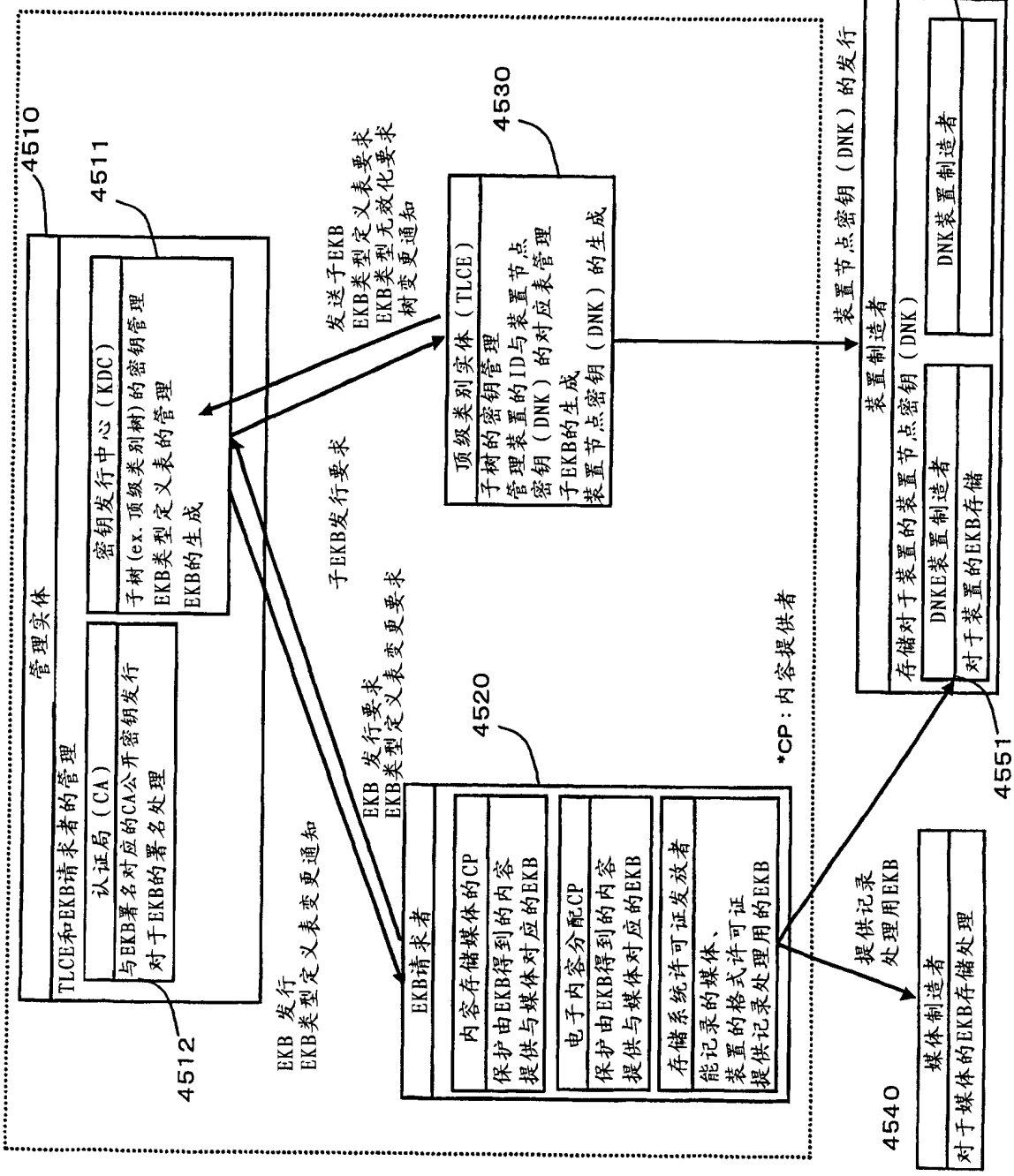
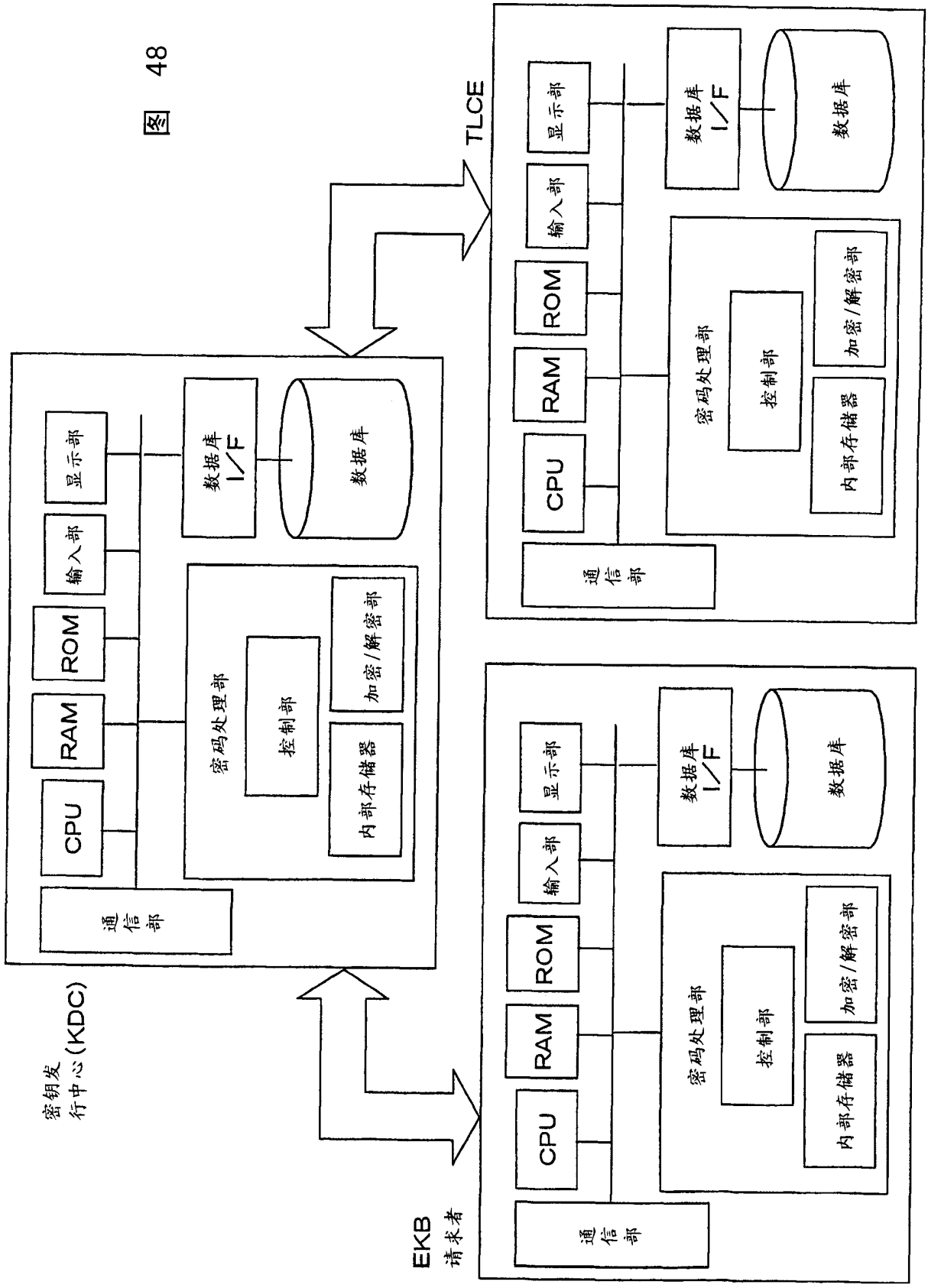

管理实体
TLCE和EKB请求者的管理
认证局（CA）
与EKB署名对应的CA公开密钥发行
对于EKB的署名处理
密钥发行中心（KDC）
子树（ex.顶级类别树）的密钥管理
EKB类型定义表的管理
EKB的生成
4510
4511
4512
EKB 发行
EKB类型定义表变更通知
发送子EKB
EKB类型定义表要求
EKB类型无效化要求
树变更通知
子EKB发行要求
EKB 发行要求
EKB类型定义表变更要求
顶级类别实体（TLCE）
子树的密钥管理
管理装置的ID与装置节点
密钥（DNK）的对应表管理
子EKB的生成
装置节点密钥（DNK）的生成
4530
EKB请求者
内容存储媒体的CP
保护由EKB得到的内容
提供与媒体对应的EKB
电子内容分配CP
保护由EKB得到的内容
提供与媒体对应的EKB
存储系统许可证发放者
能记录的媒体、
装置的格式许可证
提供记录处理用的EKB
4520
*CP：内容提供者
装置制造者
装置节点密钥（DNK）的发行
存储对于装置的装置节点密钥（DNK）
DNKE装置制造者
对于装置的EKB存储
DNK装置制造者
4550
4552
4551
提供记录
处理用EKB
媒体制造者
对于媒体的EKB存储处理
4540

图 48


密钥发行中心(KDC)
通信部
CPU
RAM
ROM
输入部
显示部
数据库I/F
数据库
密码处理部
控制部
加密/解密部
内部存储器
TLCE
EKB请求者

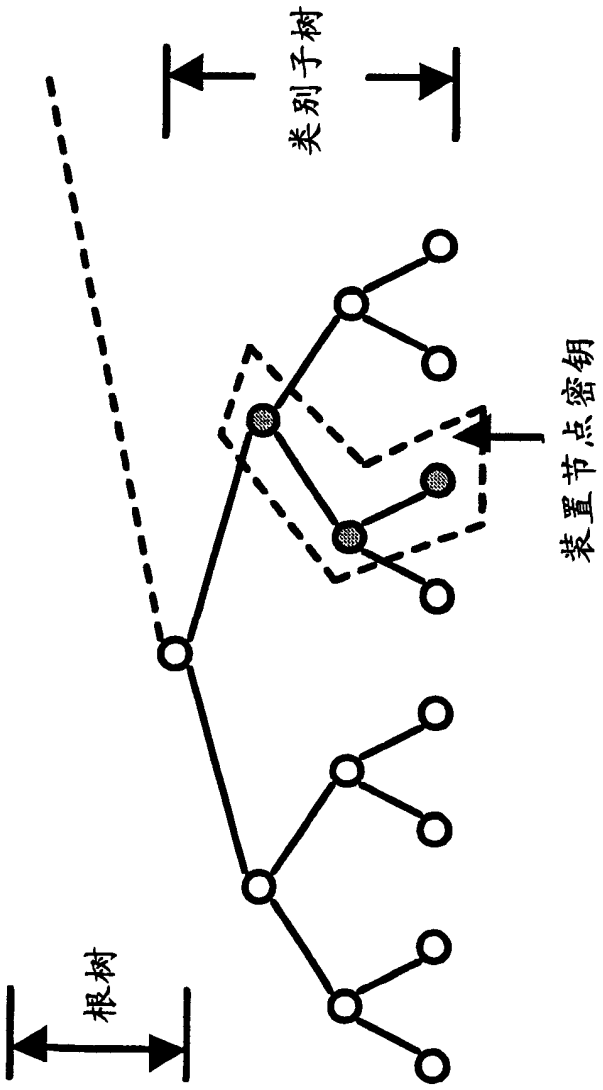


图 49

EKB类型识别编号	节点	说明
1	MS 的节点 ID	它用于MemoryStick
2	PHS 的节点 ID	它用于PHS
3	MS 的节点 ID 和 PHS 的节点 ID	它用于 MemoryStick + PHS
4	MD	它用于MD
5	...	...

图 50

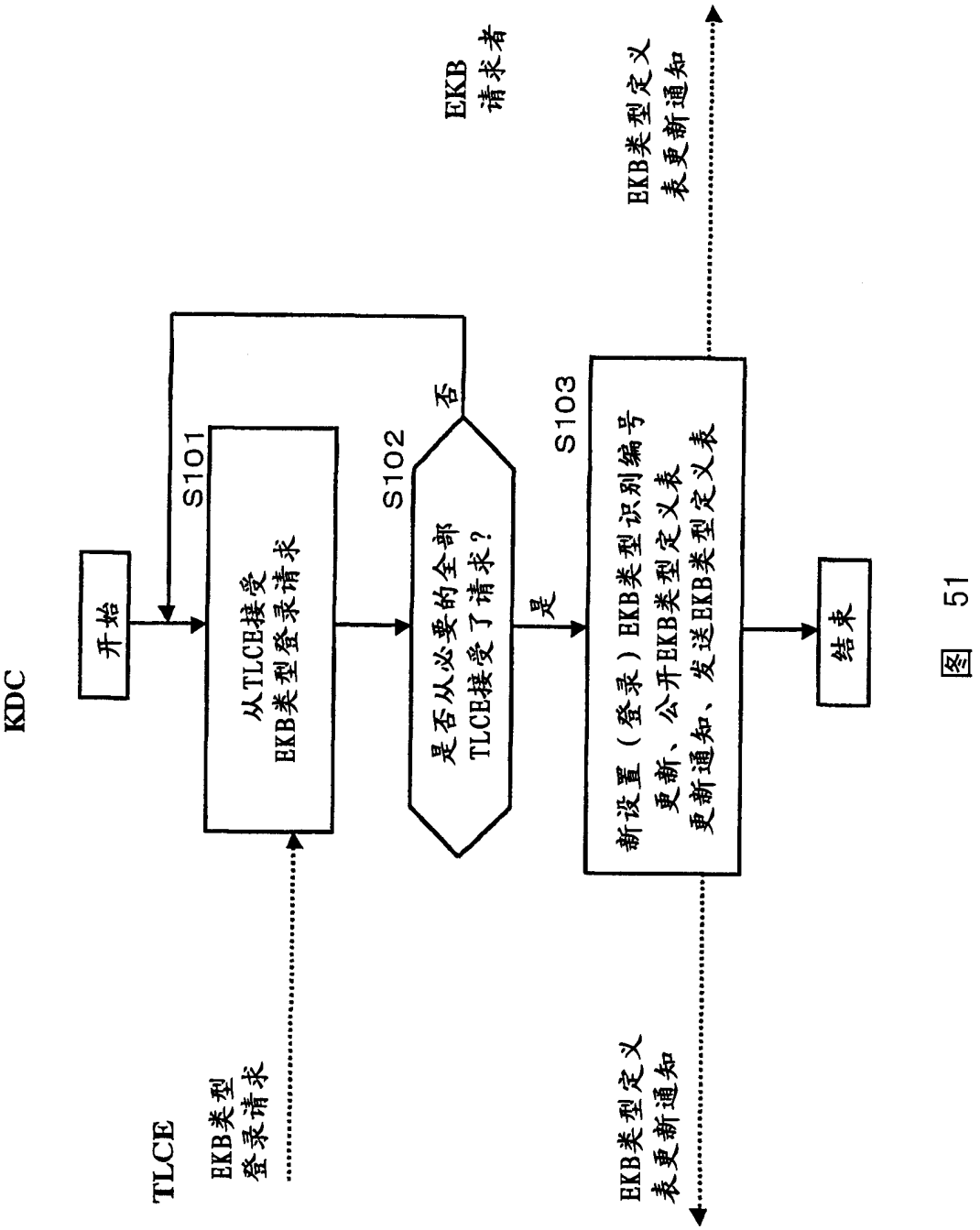

KDC
TLCE
EKB
请求者
开始
S101
从TLCE接受
EKB类型登录请求
S102
是否从必要的全部
TLCE接受了请求？
否
是
S103
新设置（登录）EKB类型识别编号
更新、公开EKB类型定义表
更新通知、发送EKB类型定义表
结束
EKB类型
登录请求
EKB类型定义
表更新通知
EKB类型定义
表更新通知

图 51

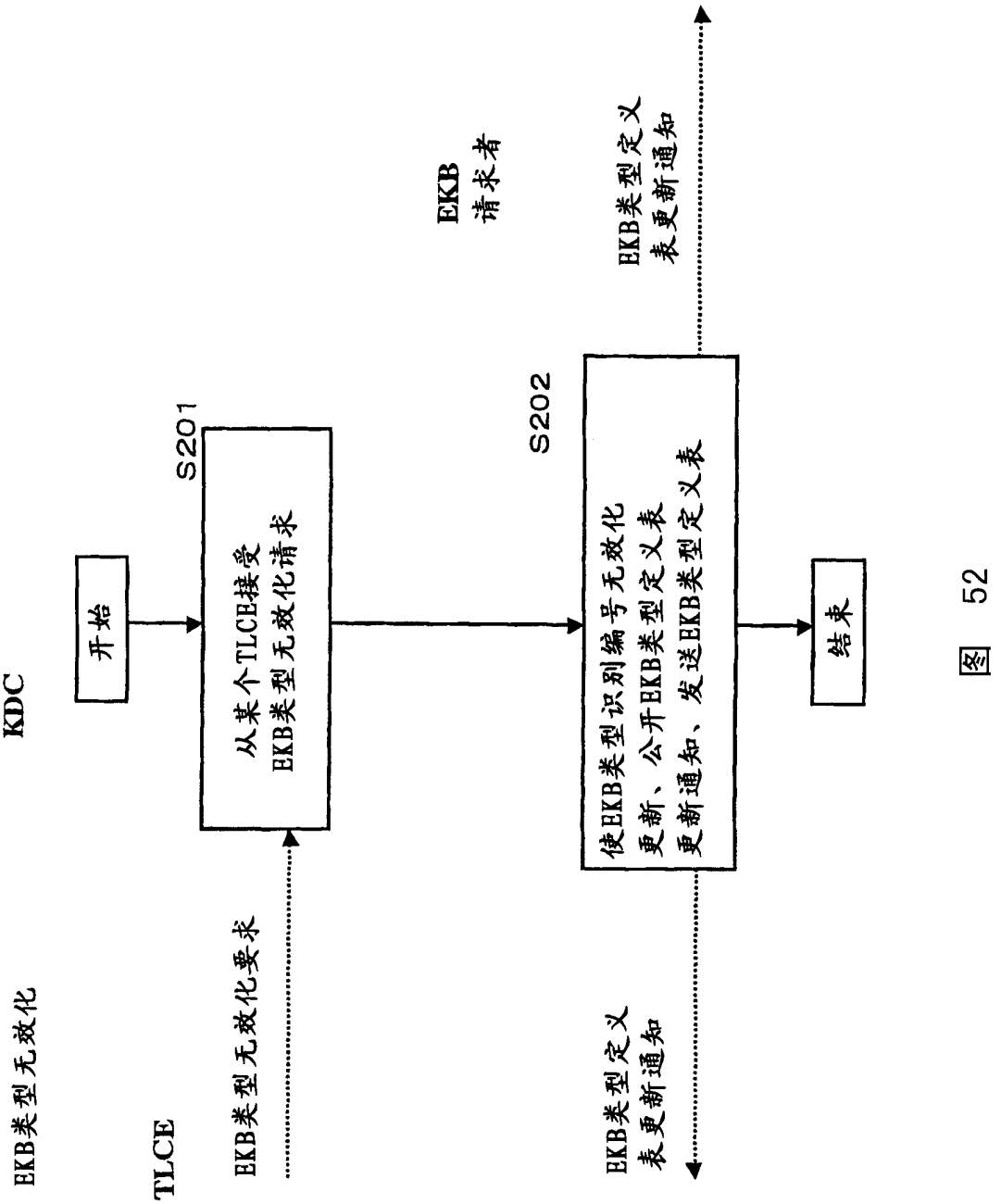

KDC
EKB类型无效化
TLCE
EKB类型无效化要求
开始
S201
从某个TLCE接受
EKB类型无效化请求
EKB
请求者
S202
使EKB类型识别编号无效化
更新、公开EKB类型定义表
更新通知、发送EKB类型定义表
EKB类型定义
表更新通知
EKB类型定义
表更新通知
结束

图 52

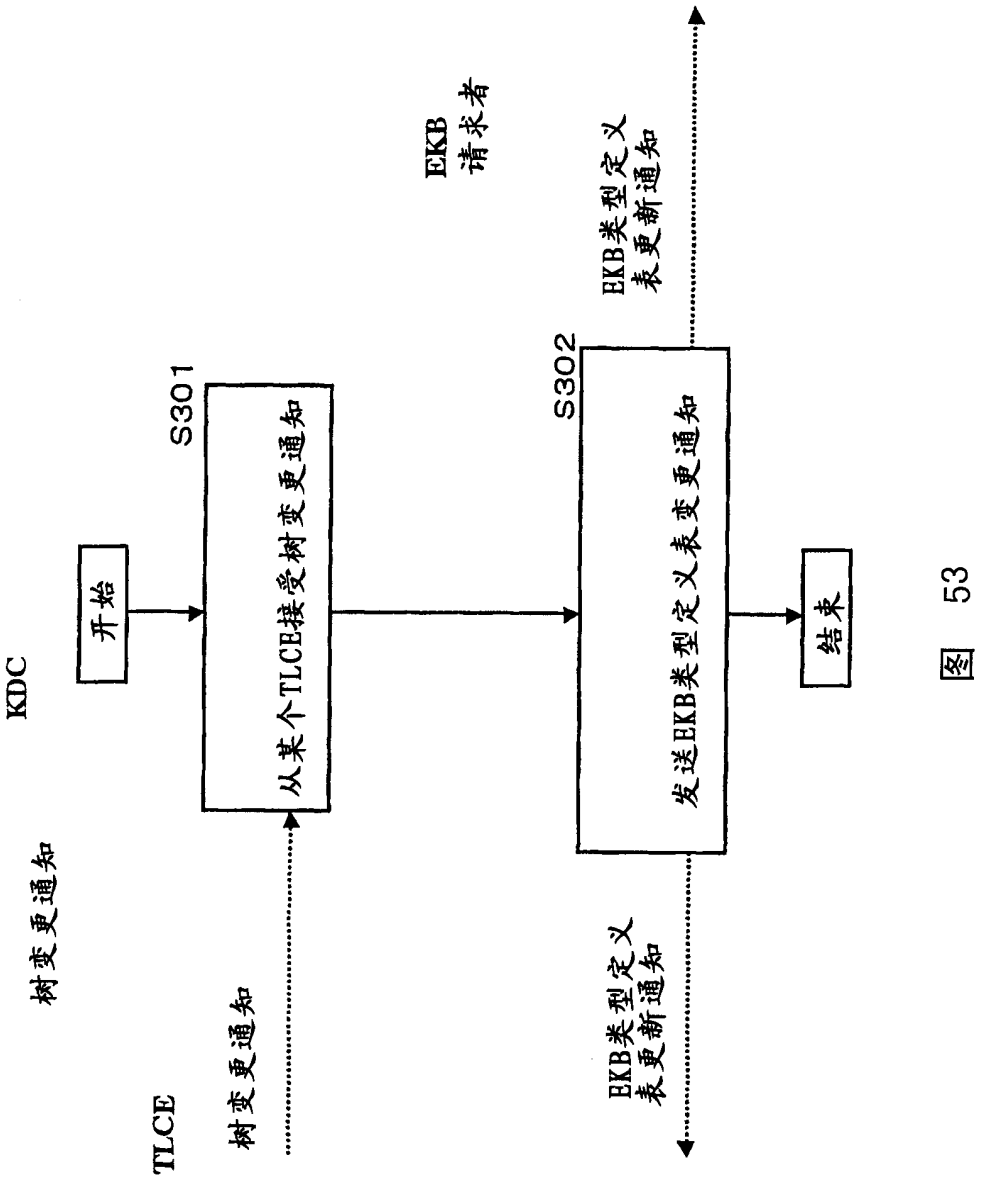

KDC
树变更通知
TLCE
树变更通知
开始
S301
从某个TLCE接受树变更通知
EKB
请求者
S302
发送EKB类型定义表变更通知
EKB类型定义
表更新通知
EKB类型定义
表更新通知
结束

图 53

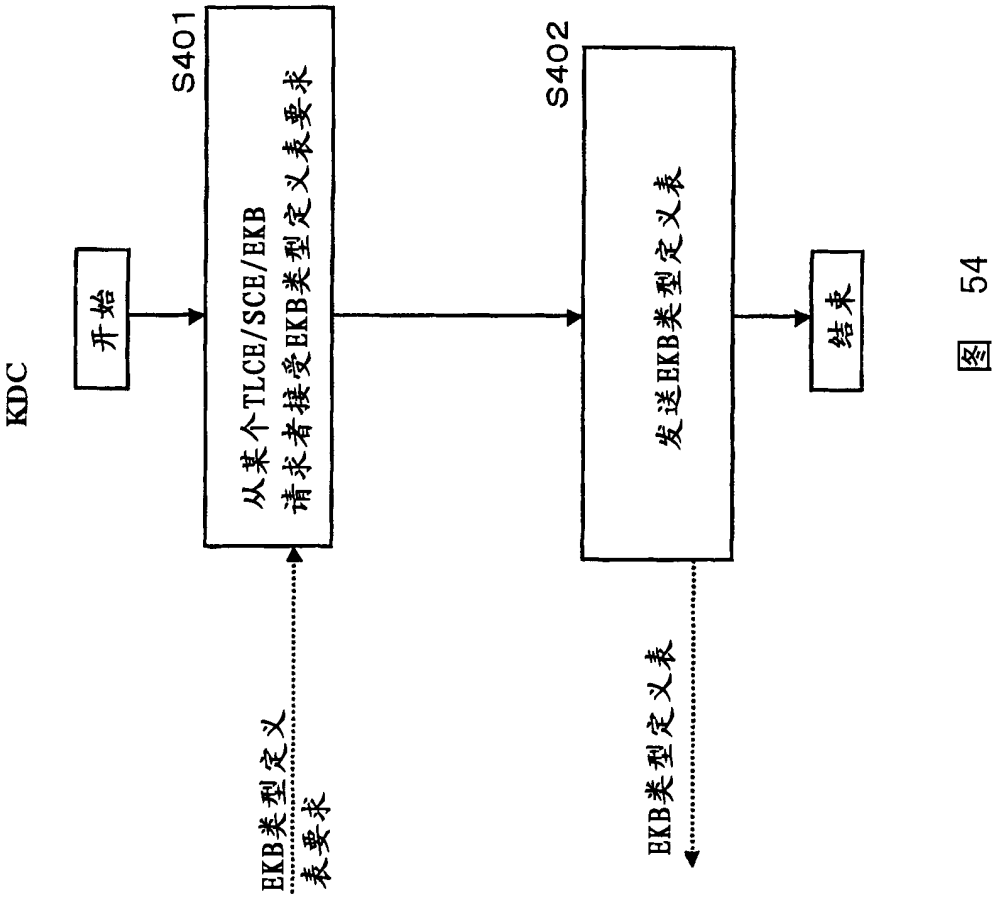

KDC
开始
S401
从某个TLCE/SCE/EKB
请求者接受EKB类型定义表要求
S402
发送EKB类型定义表
结束
EKB类型定义
表要求
EKB类型定义表

图 54

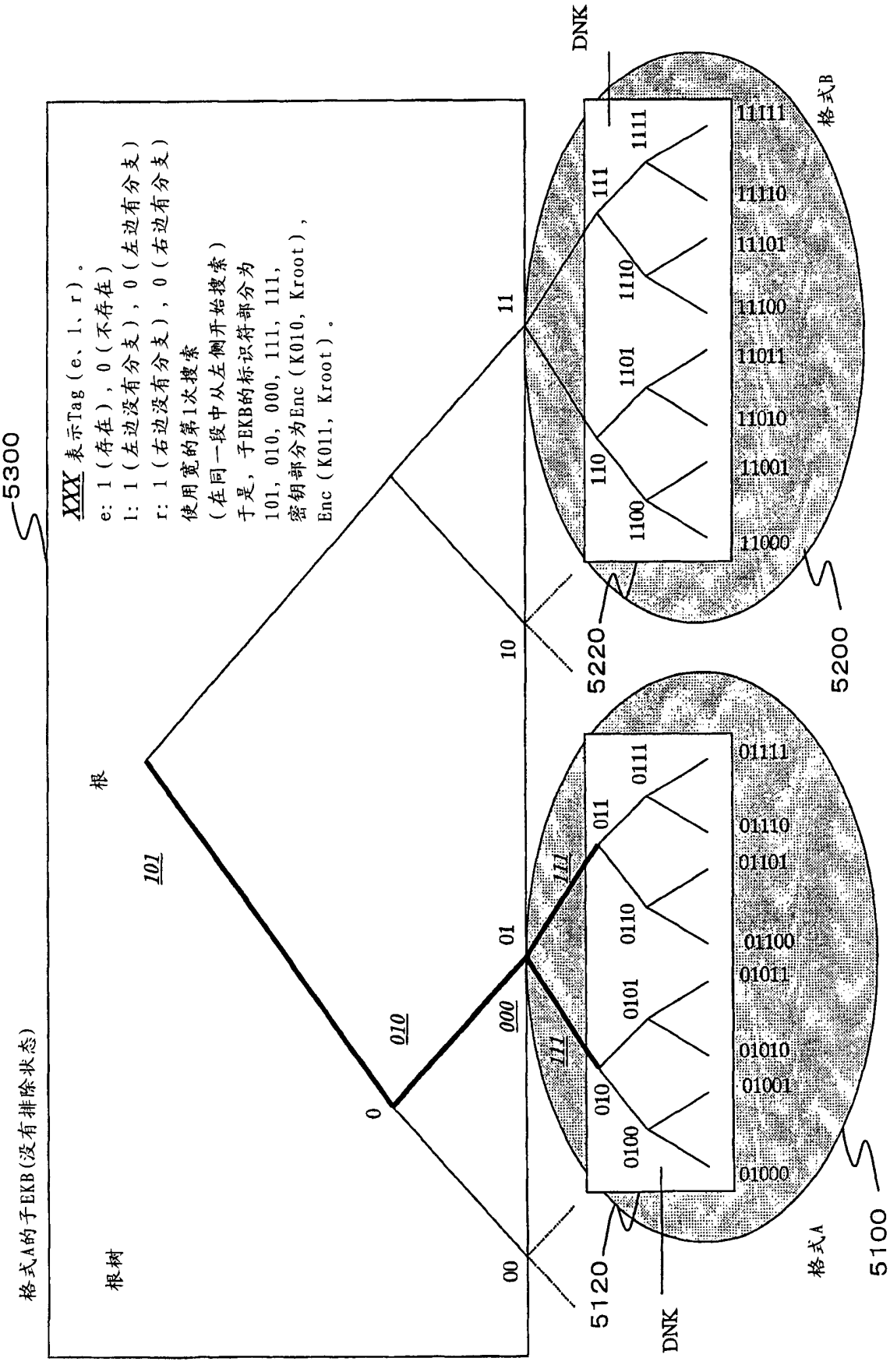

格式A的子EKB(没有排除状态)
5300
根树
根
XXX 表示Tag(e、l、r)。
e: 1(存在), 0(不存在)
l: 1(左边没有分支), 0(左边有分支)
r: 1(右边没有分支), 0(右边有分支)
使用宽的第1次搜索
(在同一段中从左侧开始搜索)
于是, 子EKB的标识符部分为
101, 010, 000, 111, 111,
密钥部分为Enc(K010, Kroot),
Enc(K011, Kroot)。
101
010
000
111
111
0
00
01
10
11
5120
5220
DNK
DNK
格式A
格式B
5100
5200
0100
0101
0110
0111
01000
01001
01010
01011
01100
01101
01110
01111
1100
1101
1110
1111
11000
11001
11010
11011
11100
11101
11110
11111

图 55

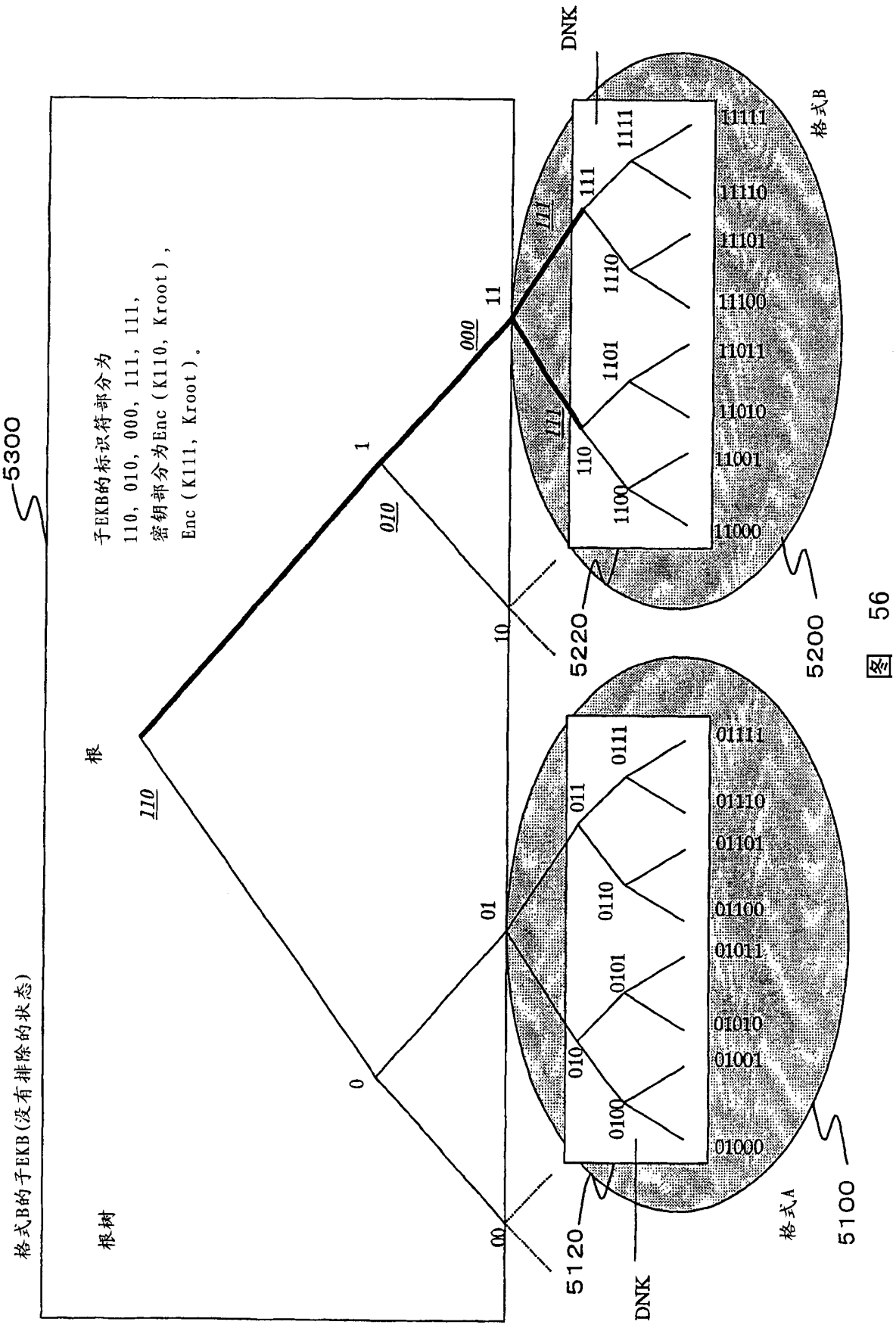

格式B的子EKB(没有排除的状态)
5300
根树
根
子EKB的标识符部分为
110, 010, 000, 111, 111,
密钥部分为Enc(K110, Kroot),
Enc(K111, Kroot)。
110
010
000
111
111
0
1
00
01
10
11
DNK
5120
5100
格式A
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
01111
DNK
5220
5200
格式B
11000
11001
11010
11011
11100
11101
11110
11111

图 56

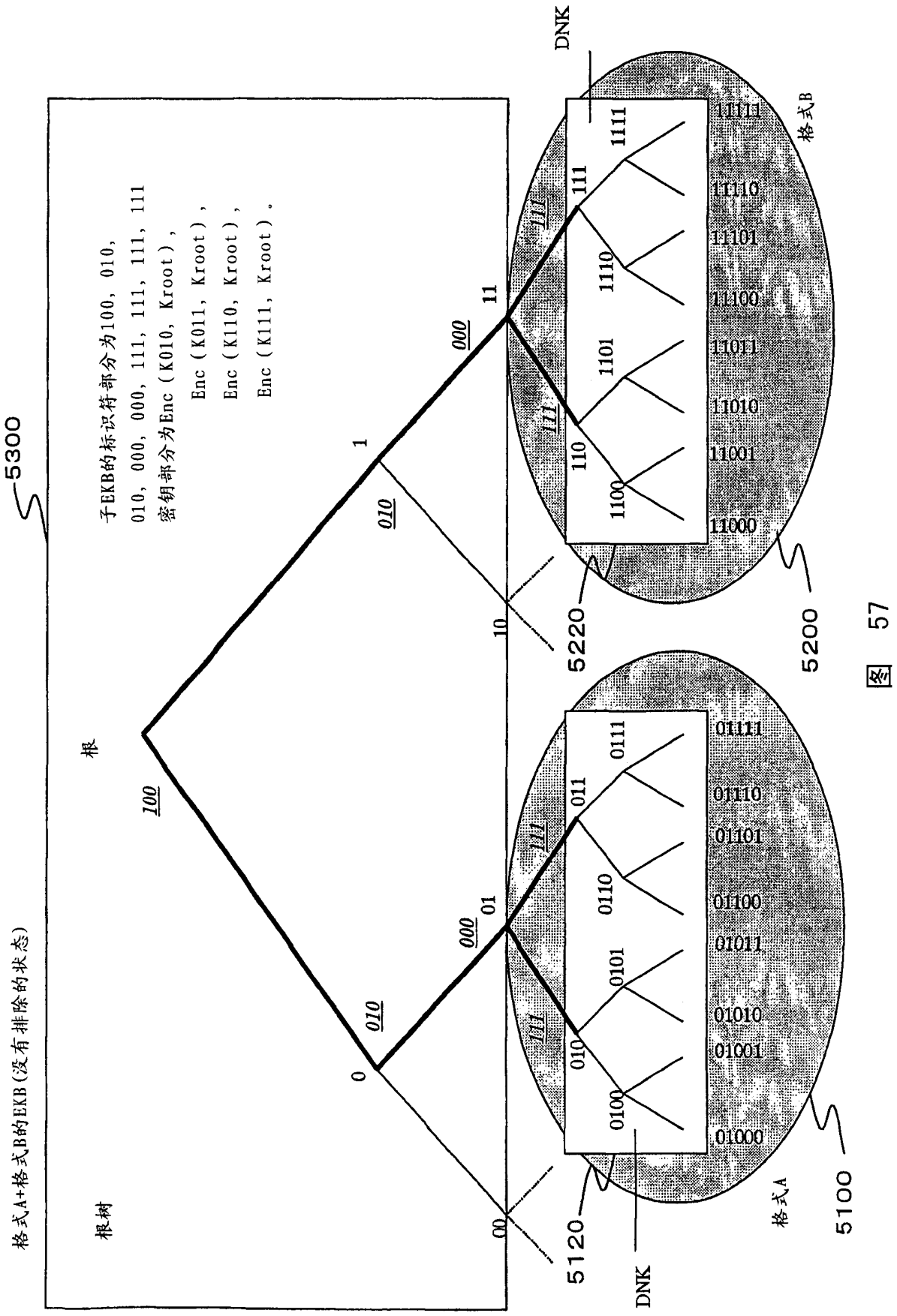

格式A+格式B的EKB(没有排除的状态)
5300
根树
根
子EKB的标识符部分为100, 010,
010, 000, 000, 111, 111, 111, 111
密钥部分为Enc(K010, Kroot),
Enc(K011, Kroot),
Enc(K110, Kroot),
Enc(K111, Kroot)。
100
010
000
111
0
1
00
01
10
11
010
000
111
111
111
111
DNK
DNK
5120
5220
5100
5200
格式A
格式B
01111
01110
01101
01100
01011
01010
01001
01000
0111
0110
0101
0100
011
010
11111
11110
11101
11100
11011
11010
11001
11000
1111
1110
1101
1100
111
110

图 57

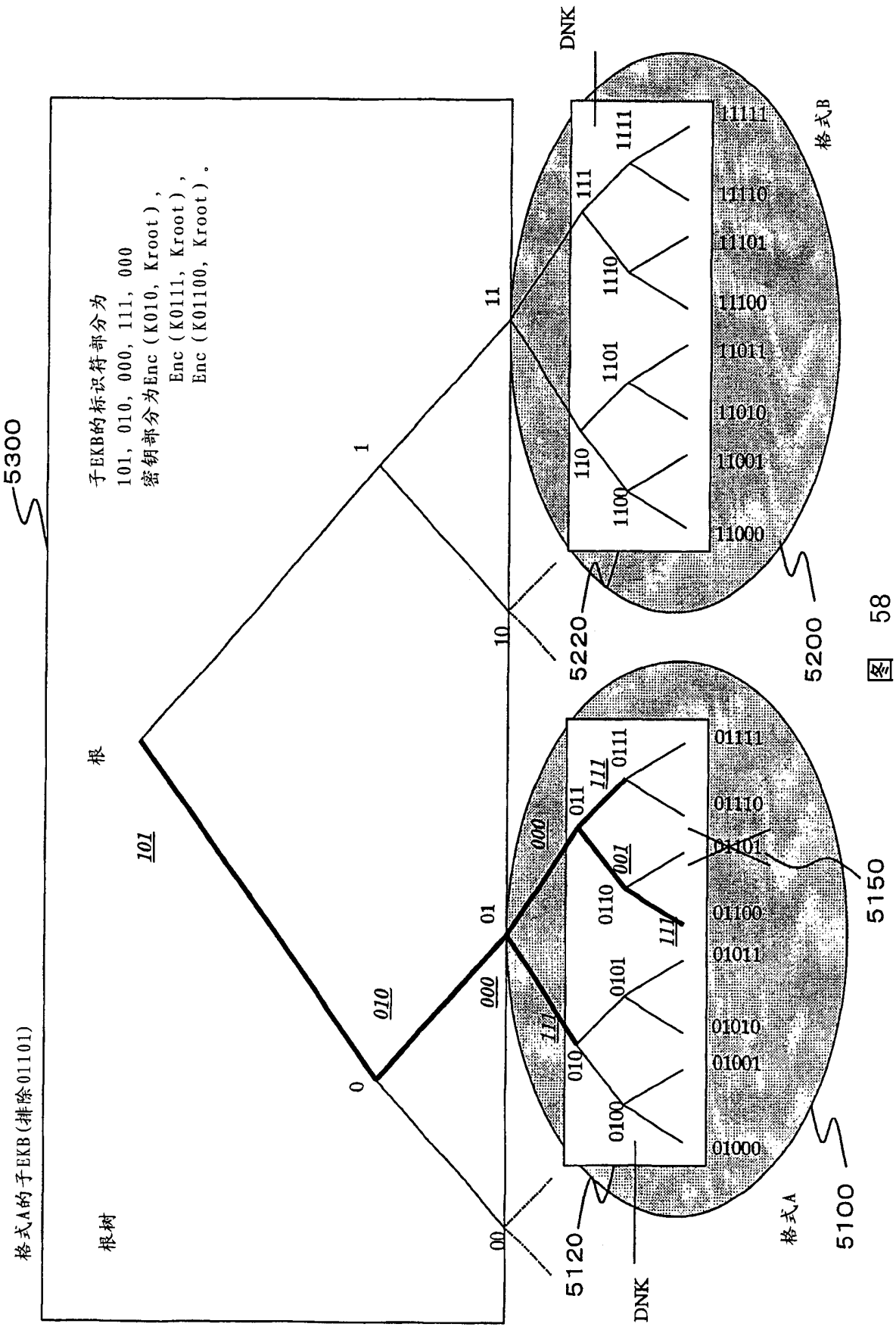

格式A的子EKB(排除01101)
根树
5300
根
101
010
000
111
0
1
00
01
10
11
子EKB的标识符部分为
101, 010, 000, 111, 000
密钥部分为Enc(K010, Kroot),
Enc(K0111, Kroot),
Enc(K01100, Kroot)。
DNK
5120
5100
格式A
01111
01110
01101
01100
01011
01010
01001
01000
011
0111
0110
0101
0100
010
5150
DNK
5220
5200
格式B
11111
11110
11101
11100
11011
11010
11001
11000
111
1111
1110
1101
1100
110

图 58

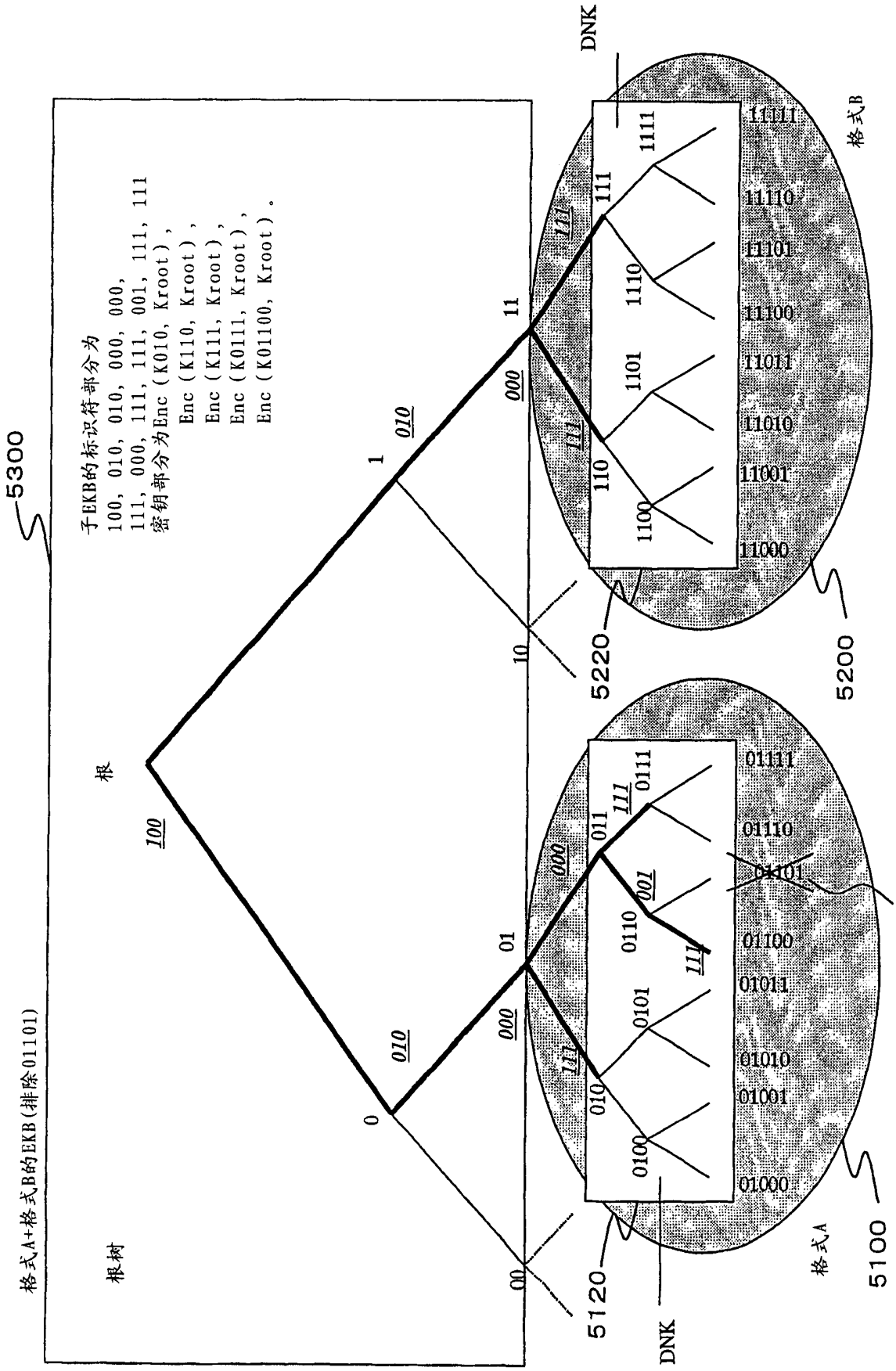

格式A+格式B的EKB(排除01101)
5300
根树
根
子EKB的标识符部分为
100, 010, 010, 000, 000,
111, 000, 111, 111, 001, 111, 111
密钥部分为Enc(K010, Kroot),
Enc(K110, Kroot),
Enc(K111, Kroot),
Enc(K0111, Kroot),
Enc(K01100, Kroot)。
100
010
000
111
00
01
10
11
0
1
010
000
111
DNK
5120
格式A
5100
01111
01110
01101
01100
01011
01010
01001
01000
0111
0110
0101
0100
5150
DNK
5220
格式B
5200
11111
11110
11101
11100
11011
11010
11001
11000
1111
1110
1101
1100

图 59

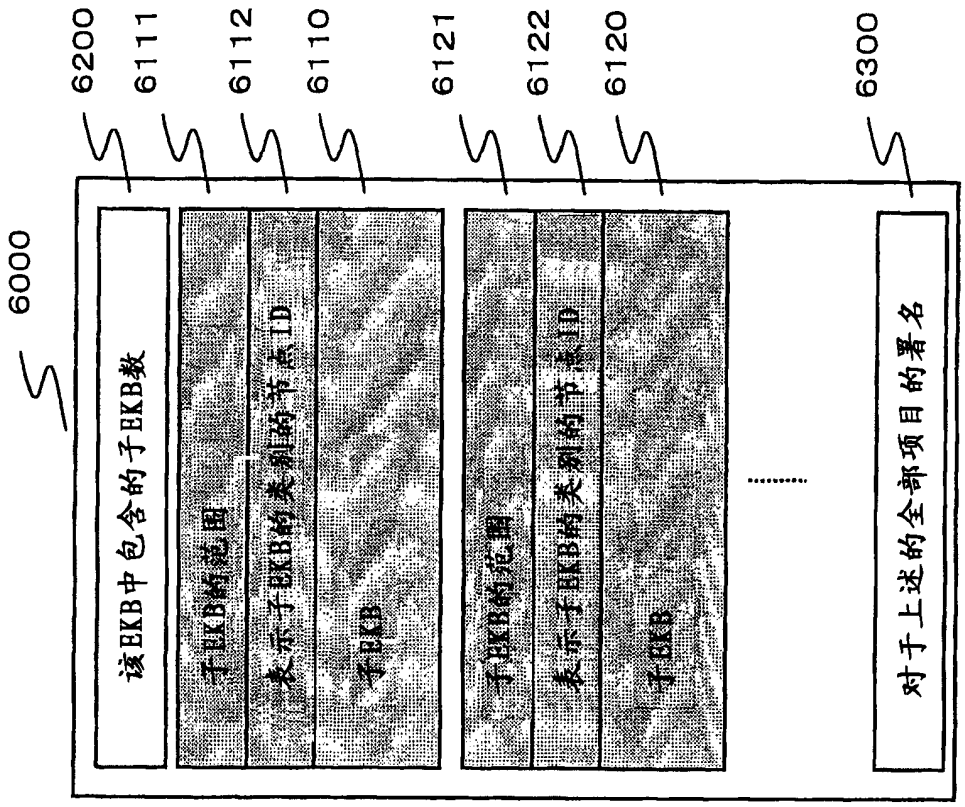

6000
该EKB中包含的子EKB数
6200
子EKB的范围
6111
表示子EKB的类别的节点ID
6112
子EKB
6110
子EKB的范围
6121
表示子EKB的类别的节点ID
6122
子EKB
6120
对于上述的全部项目的署名
6300

图 60

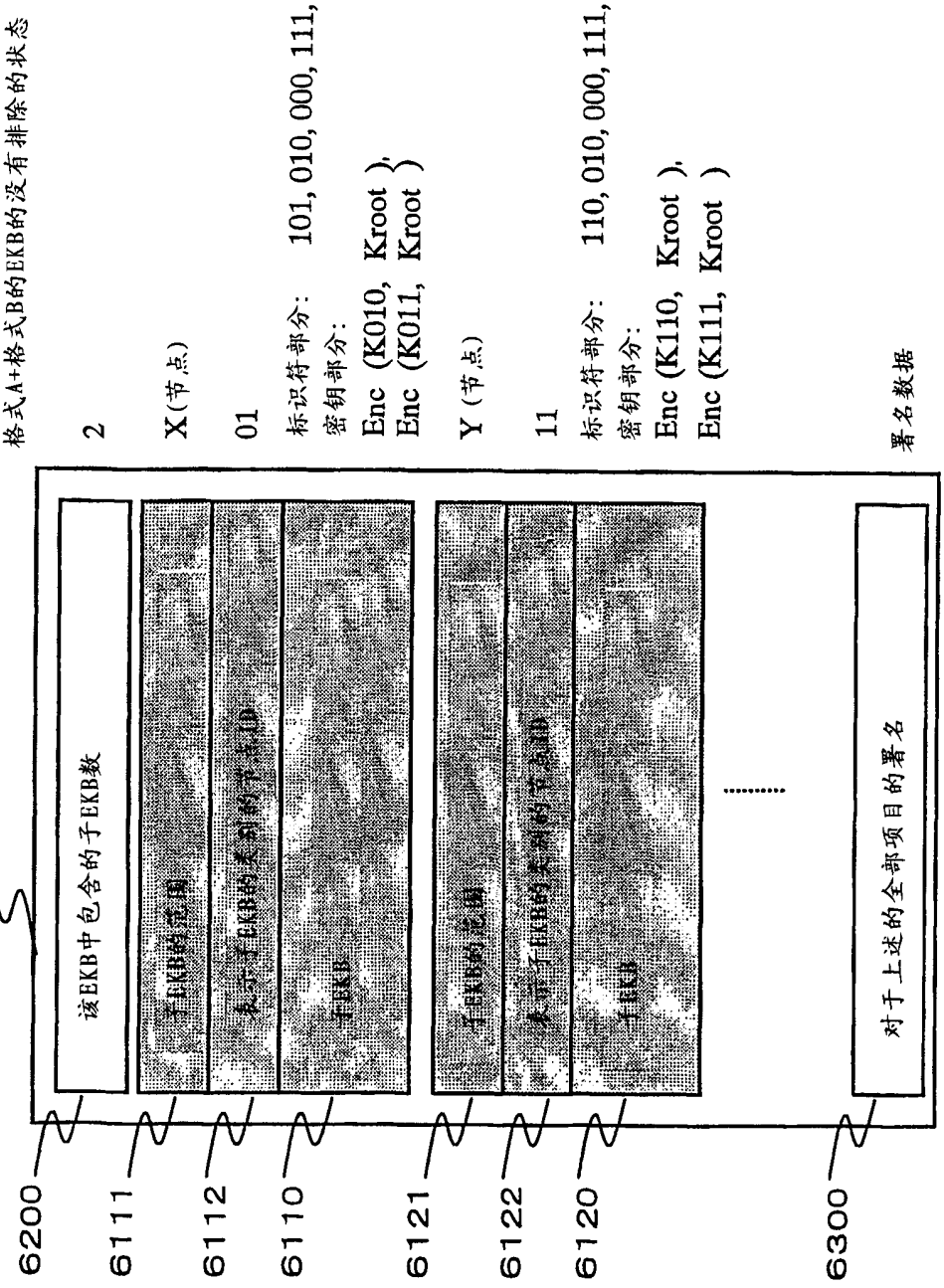

格式A+格式B的EKB的没有排除的状态
6000
该EKB中包含的子EKB数
2
X(节点)
01
标识符部分: 101, 010, 000, 111, 111
密钥部分:
Enc (K010, Kroot),
Enc (K011, Kroot)
Y(节点)
11
标识符部分: 110, 010, 000, 111, 111
密钥部分:
Enc (K110, Kroot),
Enc (K111, Kroot)
署名数据
6200
6111
6112
6110
6121
6122
6120
6300

图 61

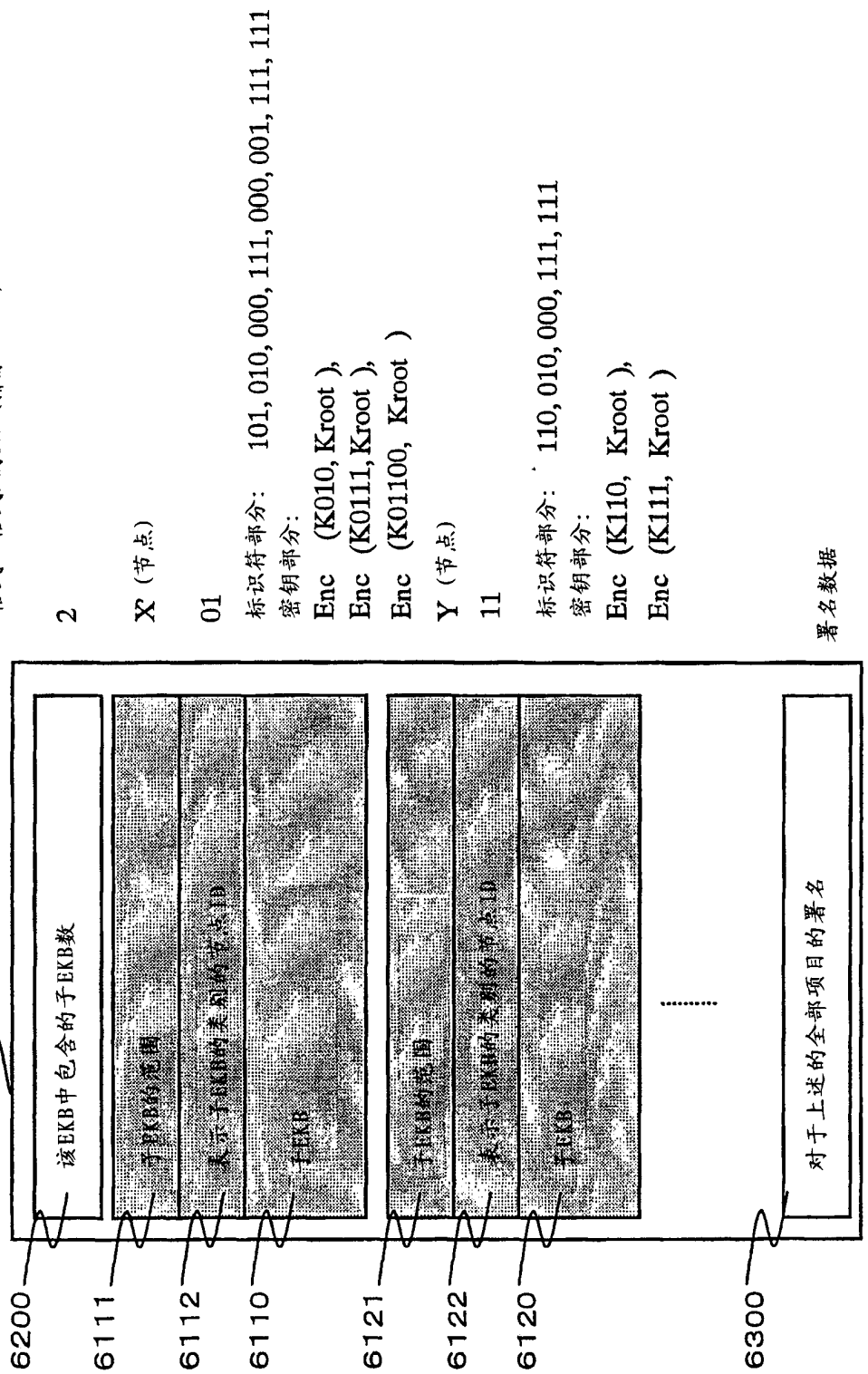

6000
该EKB中包含的子-EKB数
子EKB的范围
表示子EKB的类别的节点ID
子EKB
子EKB的范围
表示子EKB的类别的节点ID
子EKB
对于上述的全部项目的署名
6200
6111
6112
6110
6121
6122
6120
6300
格式A+格式B的EKB(排除01101)
2
X' (节点)
01
标识符部分: 101, 010, 000, 111, 000, 001, 111, 111
密钥部分:
Enc (K010, Kroot),
Enc (K0111, Kroot),
Enc (K01100, Kroot)
Y (节点)
11
标识符部分: 110, 010, 000, 111, 111
密钥部分:
Enc (K110, Kroot),
Enc (K111, Kroot)
署名数据

图 62

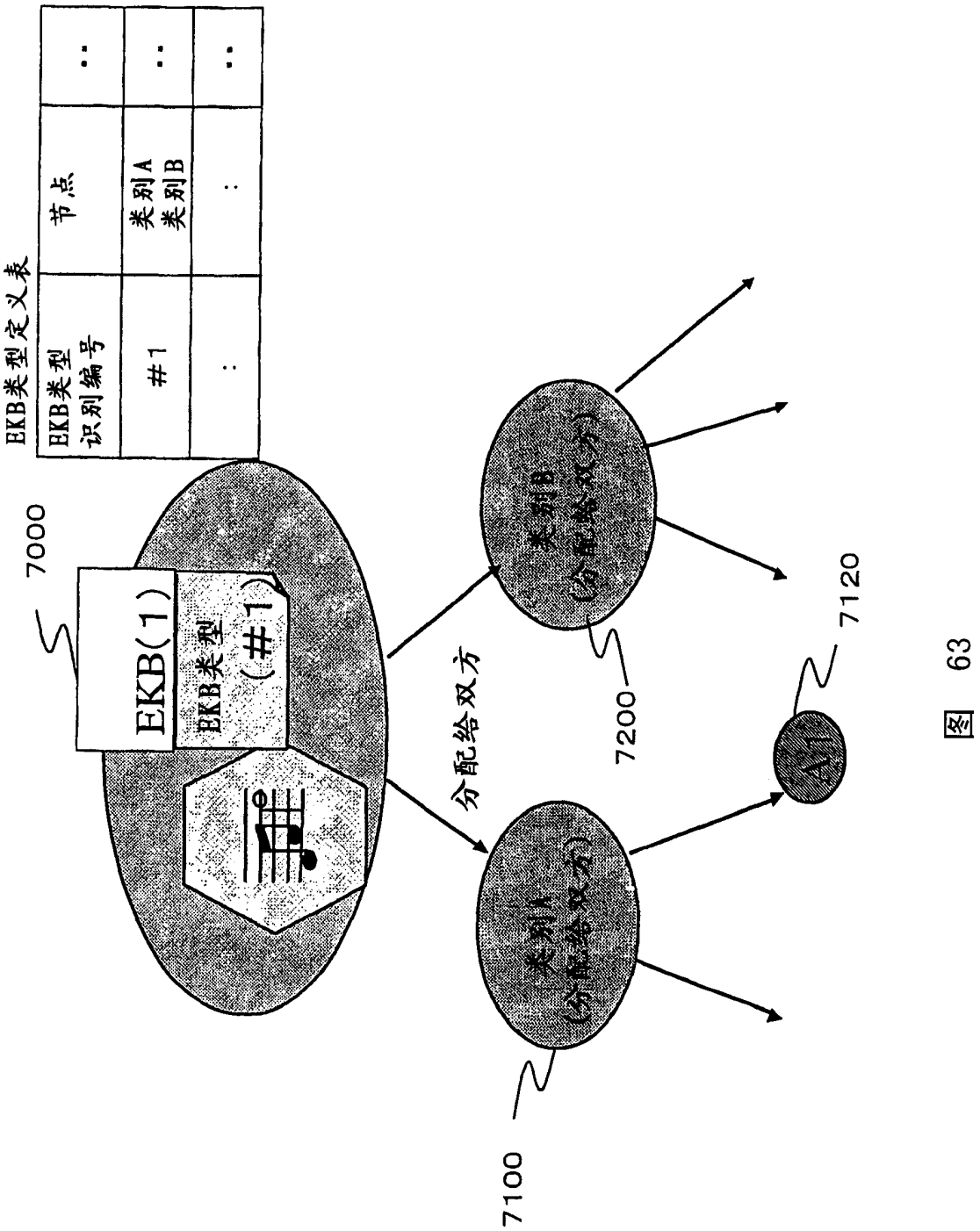

EKB类型定义表
EKB类型识别编号
节点
#1
类别A
类别B
7000
EKB(1)
EKB类型(#1)
分配给双方
类别B(分配给双方)
类别A(分配给双方)
7200
7100
7120
A1

图 63

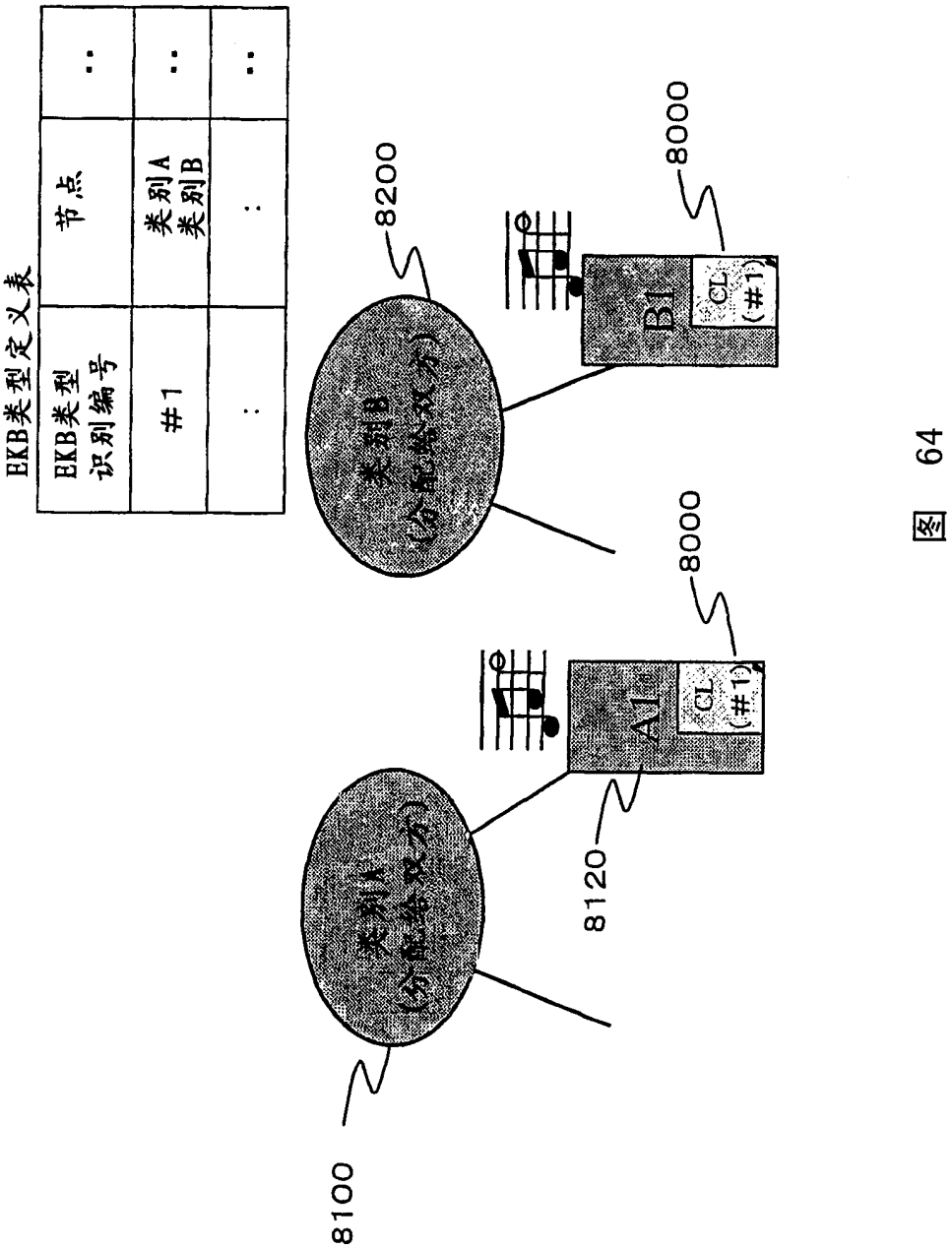

EKB类型定义表
EKB类型识别编号
节点
#1
类别A
类别B
8100
8120
8200
8000
8000
A1
B1
CL
(#1)
CL
(#1)

图 64