(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101536401 B
(45)授权公告日 2013.06.05

(21)申请号 200780042720.2
(22)申请日 2007.10.03
(30)优先权数据
310182/2006 2006.11.16 JP
310226/2006 2006.11.16 JP
(85)PCT申请进入国家阶段日
2009.05.18
(86)PCT申请的申请数据
PCT/JP2007/069387 2007.10.03
(87)PCT申请的公布数据
WO2008/059672 JA 2008.05.22
(73)专利权人 索尼株式会社
地址 日本东京都
(72)发明人 浅野智之 草川雅文
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 郭定辉
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
US 2006/0015514 A1,2006.01.19,1.
US 2004/0255049 A1,2004.12.16,1.
审查员 孙志飞

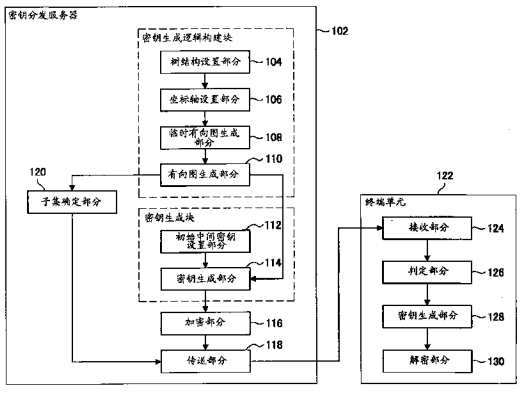
权利要求书17页 说明书51页 附图26页

(54)发明名称

信息处理设备

(57)摘要

公开了信息处理设备、终端、信息处理方法、密钥创建方法和程序，其均能够使用户保存减少了数量的密钥。信息处理设备绘制有向图，所述有向图表示用于导出用以加密内容或内容密钥的集合密钥的加密密钥创建逻辑。在该技术中，将用户终端的集合划分为多个子集，将集合密钥和中间密钥分配给每个子集，并且如果输入与子集相关联的中间密钥，则输出对应于与集合密钥相关联的子集的中间密钥以及对应于与所输入的中间密钥相关联的子集的有向分支。本发明进一步涉及根据预定替换法则、以更短的有向分支替换有向图中包括的有向分支的技术。该技术生成了减少每个用户必须保存的中间密钥的数量的效果。



CN 101536401 B

1. 一种信息处理单元，包括：

有向图获取部分，用于获取通过在由多条有向边组成的临时有向图中以更短的有向边替换组成所述临时有向图的至少一条有向边而生成的有向图；以及

密钥生成部分，用于基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥，

其中，通过从组成所有生成的临时有向图的有向路径提取最长有向路径 LP，从不包括最长有向路径 LP 的所有生成的临时有向图的每个中提取最长有向路径 PLP，从组成临时有向图的有向边中选择给定有向边，并以更短的有向边来替换它，来生成所述有向图，

其中，基于提取的最长有向路径 LP 和最长有向路径 PLP 的长度执行有向边的替换。

2. 根据权利要求 1 所述的信息处理单元，其中

通过以更短的有向边替换组成所述临时有向图的至少一条有向边来生成所述有向图，以便不超过在组成所述临时有向图的多条有向边之中的连续有向边的最大数量。

3. 根据权利要求 1 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

4. 根据权利要求 1 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

5. 根据权利要求 1 所述的信息处理单元，进一步包括：

初始中间密钥设置部分，用于将给定随机数设置为与每个有向图的尾部对应的中间密钥。

6. 根据权利要求 1 所述的信息处理单元，进一步包括：

加密部分，用于使用所述集合密钥来加密内容或内容密钥。

7. 根据权利要求 6 所述的信息处理单元，进一步包括：

传送部分，用于向分别与组成给定二叉树的叶节点 1 到 n 中的一些或全部相关的终端单元传送由所述加密部分加密的内容或内容密钥，其中 n 是自然数。

8. 根据权利要求 1 所述的信息处理单元，其中

所述有向图获取部分获取以将更短的有向边朝向由连续有向边组成的每个有向路径的端点而放置的方式进行替换的有向图。

9. 根据权利要求 7 所述的信息处理单元，进一步包括：

子集确定部分，用于通过将叶节点 1 到 n 的子集定义为 Si，确定允许解密通过使用集合密钥或内容密钥而加密的内容的终端单元的集合 (N\R)，并确定满足集合 (N\R) = S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm。

10. 根据权利要求 9 所述的信息处理单元，其中

所述子集确定部分确定子集 S1 到 Sm 以便最小化 m。

11. 根据权利要求 9 所述的信息处理单元，进一步包括：

传送部分，用于向所述终端单元传送指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。

12. 根据权利要求 1 所述的信息处理单元，进一步包括 ：

解密部分，用于通过使用所述集合密钥来解密内容或内容密钥。

13. 根据权利要求 12 所述的信息处理单元，进一步包括 ：

接收部分，其与组成给定二叉树的一个或多个叶节点 1 到 n 相关联，用于接收使用所述集合密钥而加密的内容或内容密钥，其中 n 是自然数。

14. 根据权利要求 13 所述的信息处理单元，其中

由所述接收部分接收到的经加密的内容或经加密的内容密钥可以由一个或多个信息处理单元来解密，所述一个或多个信息处理单元与作为集合 S 的元素的叶节点相关联，所述集合 S 包括在定义为叶节点 1 到 n 的子集的集合 Si 中与其自身相关联的叶节点。

15. 一种信息处理单元，

在由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位 于左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，

对于自然数 i 和 j，其中 $i \leqslant j$，假设将集合 $(i \rightarrow j)$ 表示为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 $(i \leftarrow j)$ 表示为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 $(1 \rightarrow n)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 $(2 \leftarrow n)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，

设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv \rightarrow rv-1)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv+1 \leftarrow rv)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

所述信息处理单元包括 ：

有向图获取部分，用于获取通过以更短的有向边替换组成临时有向图的至少一个有向边而生成的有向图，所述临时有向图是根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，通过在第一到第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的，其中 $i = 0,1,\ldots\ldots,x-1$ ；以及

密钥生成部分，用于基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

16. 一种信息处理单元，包括 ：

树结构设置部分，用于配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的 编号设置为 rv ；

坐标轴设置部分，用以

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点 ；

临时有向图生成部分，用以

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图 ；以及

有向图生成部分，用于通过以更短的有向边替换剩余的有向边来生成有向图。

17. 根据权利要求 16 所述的信息处理单元，包括：

密钥生成部分，用于基于所述有向图生成用于加密内容或内容密钥的集合密钥。

18. 根据权利要求 17 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

19. 根据权利要求 17 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

20. 一种终端单元，包括：

密钥生成部分，用于基于有向图生成用于解密内容或内容密钥的集合密钥，其中所述有向图通过如下步骤获得：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点；

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；

在由剩余有向边形成的有向路径之中，确定具有组成有向路径的有向边 的最大数量的最长有向路径，以及

通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

21. 根据权利要求 20 所述的终端单元，进一步包括：

解密部分，用于通过使用所述集合密钥来解密经加密的内容或经加密的内容密钥。

22. 根据权利要求 20 所述的终端单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及与位于具有位于所述坐标点的尾部的有向边的头部的坐标点对应的子集 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

23. 根据权利要求 20 所述的终端单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

24. 根据权利要求 21 所述的终端单元，其中

解密部分通过使用所述集合密钥来解密经加密的内容密钥，并使用经解密的内容密钥来解密经加密的内容。

25. 根据权利要求 20 所述的终端单元，包括：

其中将树的叶节点 1 到 n 的子集定义为 Si，以及

当确定了允许解密通过使用所述集合密钥或所述内容密钥而加密的内容的终端单元的集合 (N\R)，确定满足集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，并接收指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息时，

判定部分，用于基于所接收到的信息来判定所述终端单元是否属于子集 S1 到 Sm 中的任意一个，并基于判定结果来判定是否允许经加密的内容的解密。

26. 根据权利要求 25 所述的终端单元，其中

当判定所述终端单元属于子集 S1 到 Sm 中的任意一个时，解密部分通过使用与所述终端单元所属的子集对应的集合密钥来解密内容或内容密钥。

27. 一种信息处理方法，包括：

有向图获取步骤，获取通过在由多条有向边组成的临时有向图中以更短的有向边替换组成所述临时有向图的至少一条有向边而生成的有向图；以及

密钥生成步骤，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥，

其中，通过从组成所有生成的临时有向图的有向路径提取最长有向路径 LP，从不包括最长有向路径 LP 的所有生成的临时有向图的每个中提取最长有向路径 PLP，从组成临时有向图的有向边中选择给定有向边，并以更短的有向边来替换它，来生成所述有向图，

其中，基于提取的最长有向路径 LP 和最长有向路径 PLP 的长度执行有向边的替换。

28. 一种信息处理方法，

在由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，

对于自然数 i 和 j，其中 $i \leqslant j$，假设将集合 $(i \rightarrow j)$ 表示为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 $(i \leftarrow j)$ 表示为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 $(1 \rightarrow n)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 $(2 \leftarrow n)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，

设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv \rightarrow rv-1)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv+1 \leftarrow rv)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

所述信息处理方法包括：

有向图获取步骤，获取通过以更短的有向边替换组成临时有向图的至少一个有向边而生成的有向图，所述临时有向图是根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，通过在第一到第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的，其中 $i = 0,1,\ldots\ldots,x-1$；以及

密钥生成步骤，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

29. 一种信息处理方法，包括：

树结构设置步骤：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

坐标轴设置步骤：

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第 一水平坐标轴的右端的坐标点设置为临时坐标点；

临时有向图生成步骤：

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 $i = 0$ 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加

到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图 ；

最长有向路径确定步骤，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径 ；以及

有向图生成步骤，通过以每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

30. 一种密钥生成方法，包括 ：

密钥生成步骤，基于有向图生成用于解密内容或内容密钥的集合密钥，其中所述有向图通过如下步骤获得 ：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv ；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点 ；

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leq n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；

在由剩余有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及

通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

31. 一种信息处理单元，包括：

有向图获取部分，用于获取通过在由多条有向边组成的临时有向图中，保留在组成所述临时有向图的多条有向边之中较长的有向边而以更短的有向边替换留下的至少一条有向边而生成的有向图；以及

密钥生成部分，用于基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥，

其中，通过从组成所有生成的临时有向图的有向路径提取最长有向路径 LP，从不包括最长有向路径 LP 的所有生成的临时有向图的每个中提取最长有向路径 PLP，从组成临时有向图的有向边中选择给定有向边，并以更短的有向边来替换它，来生成所述有向图，

其中，基于提取的最长有向路径 LP 和最长有向路径 PLP 的长度执行有向边的替换。

32. 根据权利要求 31 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

33. 根据权利要求 31 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

34. 根据权利要求 31 所述的信息处理单元，进一步包括：

加密部分，用于使用所述集合密钥来加密内容或内容密钥。

35. 根据权利要求 34 所述的信息处理单元，进一步包括：

传送部分，用于向分别与组成给定二叉树的叶节点 1 到 n 中的一些或全部相关的终端单元传送由所述加密部分加密的内容或内容密钥，其中 n 是自然数。

36. 根据权利要求 31 所述的信息处理单元，其中

所述有向图获取部分获取以将更短的有向边朝向由连续有向边组成的每个有向路径的端点而放置的方式替换有向边的有向图。

37. 根据权利要求 35 所述的信息处理单元，进一步包括：

子集确定部分，通过将叶节点 1 到 n 的子集定义为 Si，用于确定允许解密通过使用

集合密钥或内容密钥而加密的内容的终端单元的集合 (N\R)，并确定满足集合 (N\R) = S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，以便最小化 m。

38. 根据权利要求 37 所述的信息处理单元，进一步包括：

传送部分，用于向所述终端单元传送指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。

39. 根据权利要求 31 所述的信息处理单元，进一步包括：

解密部分，用于通过使用所述集合密钥来解密内容或内容密钥。

40. 根据权利要求 39 所述的信息处理单元，进一步包括：

接收部分，其与组成给定二叉树的一个或多个叶节点 1 到 n 相关，其中 n 是自然数，用于接收使用所述集合密钥而加密的内容或内容密钥。

41. 根据权利要求 40 所述的信息处理单元，其中

由所述接收部分接收到的经加密的内容或经加密的内容密钥可以由一个或多个信息处理单元来解密，所述一个或多个信息处理单元与作为集合 S 的元素的叶节点相关，所述集合 S 包括在定义为叶节点 1 到 n 的子集的集合 Si 中与其自身相关的叶节点。

42. 一种信息处理单元，用以根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，处理通过在第一和第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的临时有向图，其中 i = 0,1,.....,x-1，

在由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于 左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，

对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，

设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

所述信息处理单元包括：

临时有向图获取部分，用于获取临时有向图；

有向图生成部分，用于通过保留在组成由所述临时有向图获取部分获取的所述临时有

向图的多条有向边之中较长的有向边来生成有向图；

最长有向路径确定部分，用于确定在组成所述有向图的多条有向边之中连续有向边的最大数量；

有向边替换部分，用于通过以更短的有向边替换组成所述有向图的至少一条有向边来重建所述有向图，以便不超过连续有向边的最大数量；以及

密钥生成部分，用于基于由所述有向边替换部分重建的所述有向图，生成用于加密内容或内容密钥的集合密钥。

43. 一种信息处理单元，包括：

树结构设置部分，配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i， i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

坐标轴设置部分，用以

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；以及

将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在所述第一临时坐标点的右侧；

临时有向图生成部分，用以

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 $i = 0$ 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标

轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标 点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴上第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 相关的临时有向图，来生成与集合 (1 → n) 相关的临时有向图；

最长有向路径确定部分，用于在由连续有向边形成的有向路径之中，确定具有组成所述有向路径的有向边的最大数量的最长有向路径；以及

有向图生成部分，用于通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每一条有向路径的有向边来生成有向图。

44. 根据权利要求 43 所述的信息处理单元，包括：

密钥生成部分，用于基于所述有向图生成用于加密内容或内容密钥的集合密钥。

45. 根据权利要求 44 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

46. 根据权利要求 44 所述的信息处理单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

47. 一种终端单元，包括：

密钥生成部分，用于基于有向图生成用于解密内容或内容密钥的集合密钥，其中所述有向图通过如下步骤而获得：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而 将集合 (i ← j) 定义为 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；

将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的右侧，

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了 最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，

通过将具有长度 1 的、具有位于第一水平坐标轴的第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，

在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及

通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

48. 根据权利要求 47 所述的终端单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于所述坐标点的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

49. 根据权利要求 47 所述的终端单元，其中

响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

50. 根据权利要求 48 所述的终端单元，进一步包括：

解密部分，用于使用所述集合密钥来解密经加密的内容密钥，并使用经解密的内容密钥来解密经加密的内容。

51. 根据权利要求 50 所述的终端单元，进一步包括：

其中将树的叶节点 1 到 n 的子集定义为 Si，以及

当确定了允许解密通过使用所述集合密钥或所述内容密钥而加密的内容的终端单元的集合 (N\R)，确定满足集合 (N\R) = S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，并接收指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息时，

判定部分，用于基于所接收到的信息来判定所述终端单元是否属于子集 S1 到 Sm 中的任意一个，并基于判定结果来判定是否允许经加密的内容的解密，其中

当判定所述终端单元属于子集 S1 到 Sm 中的任意一个时，所述解密部分使用与所述终端单元所属的子集对应的集合密钥来解密所述内容或内容密钥。

52. 一种信息处理方法，包括：

有向图获取步骤，在由多条有向边组成的临时有向图中，获取通过在组成所述临时有向图的多条有向边之中保留较长的有向边而以更短的有向边替换留下的至少一条有向边而生成的有向图；以及

密钥生成步骤，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥，

其中，通过从组成所有生成的临时有向图的有向路径提取最长有向路径 LP，从不包括最长有向路径 LP 的所有生成的临时有向图的每个中提取最长有向路径 PLP，从组成临时有向图的有向边中选择给定有向边，并以更短的有向边来替换它，来生成所述有向图，

其中，基于提取的最长有向路径 LP 和最长有向路径 PLP 的长度执行有向边的替换。

53. 一种信息处理方法，用以根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，处理通过在第一和第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的临时有向图，其中 i = 0,1,.....,x-1，

在由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，

对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，

设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与

集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

所述信息处理方法包括：

临时有向图获取步骤，获取临时有向图；

有向图生成步骤，通过在组成由所述临时有向图获取步骤获取的所述临时有向图的多条有向边之中保留较长的有向边来生成有向图；

最长有向路径确定步骤，在组成所述有向图的多条有向边之中，确定连续有向边的最大数量；

有向边替换步骤，通过以更短的有向边替换组成所述有向图的至少一条有向边来重建所述有向图，以便不超过连续有向边的最大数量，以及

密钥生成步骤，基于由所述有向边替换步骤重建的所述有向图，生成用于加密内容或内容密钥的集合密钥。

54. 一种信息处理方法，包括：

树结构设置步骤：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，其中 n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义为 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

坐标轴设置步骤：

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排 列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧，以及

将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点

放置在第一临时坐标点的右侧；

临时有向图生成步骤：

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及

通过将具有长度 1 的、具有位于第一水平坐标轴上第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；

最长有向路径确定步骤，在由连续有向边形成的有向路径之中，确定具 有组成所述有向路径的有向边的最大数量的最长有向路径；以及

有向图生成步骤，通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

55. 一种密钥生成方法，包括：

密钥生成步骤，基于有向图生成用于解密内容或内容密钥的集合密钥，其中所述有向图通过如下步骤而获得：

配置由向其分配了编号 1 到 n 的、n 个叶节点、一个根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，

第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，

对于每个所述中间节点，设置

第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上

的坐标点，以及

第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及

将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；

将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的右侧，

通过

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及

对于每个整数 i ＝ 0 到 x-1，

通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，

通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，

对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及

从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，

来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，

通过将具有长度 1 的、具有位于第一水平坐标轴的第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，

在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及

通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

信息处理设备

技术领域

[0001] 本发明涉及信息处理单元、终端单元、信息处理方法、密钥生成方法和程序。

背景技术

[0002] 如今，涉及通过网络等的内容分发 (contents distribution) 的加密技术的发展吸引了广泛的关注。特别地，安全并有效地分发用于解密经加密的内容的加密密钥的方法吸引了特别的关注。一般而言，如下的方案是必需的：关于分发经加密的内容的一个分发者，存在具有有效接收权利的 n 个 (n 是大于等于 2 的自然数) 接收者，并且在存在于网络上的无限个拦截者之中仅有这 n 个接收者可以解密经加密的内容。进一步，由于具有有效接收权利的接收者的数量 n 随时间变化，因此存在对于在接收者的集合中能够灵活地处理变化的方案的需求。

[0003] 此外，在这种方案的实现中，在分发者中出现涉及加密密钥的生成、保存和分发、内容的加密等的处理负荷，并且自然在接收者中出现涉及解密密钥的保存和接收、内容的解密等的处理负荷。通过各种最近的技术发展 (如，吞吐量信息处理设备的存储容量等的提高、信息传输路径的通信速度的提高)，关于上述加密分发处理负荷的负荷正在相对地降低是事实。然而，由于内容分发服务的消费者的数量的急剧增加以及安全到足以防范有经验的恶意拦截者的加密技术的需求，加密分发而引起的处理负荷相应地增大。

[0004] 在这样的情况下，作为用以通过使用广播信道安全地将信息传送到由分发者任意选择的一组接收者的技术，已经提出了诸如撤销方案 (revocationscheme) 和广播加密方案之类的方案。广播加密方案的一个示例是在下面的非专利文献 1 中公开的加密密钥分发方案，并且所述方案的特征是使用现有的分层树结构，对密钥分发方案进行密钥导出路径 (key derivation path) 的改进。具体地说，该方案 (其中，将接收者的集合看作被划分为多个子集) 通过将不包括在一子集中的接收者添加到某个子集来创建新的子集，并且作为重复该处理的结果而创建子集链，然后沿着所述链导出与每个子集对应的加密密钥。由此可以减少要由接收者保存的密钥的数量、用以生成解密密钥的计算量以及用于密钥分发的通信量 (traffic)。

[0005] [非专利文献 1]Nuttapong Attrapadung and Hideki Imai, ″ SubsetIncremental Chain Based Broadcast Encryption with Shorter Ciphertext ″, The28th Symposium on Information Theory and Its Applications(SITA2005)。

发明内容

[0006] 本发明要解决的问题

[0007] 与诸如 CD 方案 (完整子树方案，Complete Subtree Scheme) 和 SD 方案 (子集差方案，Subset Difference scheme) 之类的密钥分发方案相比，根据上述非专利文献 1 的加密密钥分发方案具有显著的优点。然而，从假设实现的实践角度来看，存在如下问题：在接

收者的数量很大的情况下，在接收者端要由终端单元保存的密钥的数量以及内容解密所需的计算量仍然很大。

[0008] 已经完成本发明来解决以上问题，由此本发明的目标是提供新的、改进的、能够减小在接收者端要由终端单元保存的密钥的数量的信息处理单元、终端单元、信息处理方法、密钥生成方法和程序。

[0009] 解决问题的装置

[0010] 为了解决以上问题，根据本发明的一个方面，提供了信息处理单元，包括：有向图获取部分，在由多条有向边组成的临时有向图中，获取通过以更短的有向边替换组成所述临时有向图的至少一条有向边而生成的有向图；以及密钥生成部分，基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0011] 进一步，为了解决以上问题，根据本发明的一个方面，提供了信息处理单元，在由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，对于自然数 i 和 j，其中 $i \leqslant j$，假设将集合 $(i \rightarrow j)$ 表示为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 $(i \leftarrow j)$ 表示为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集 合 $(1 \rightarrow n)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 $(2 \leftarrow n)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv \rightarrow rv-1)$ 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 $(lv+1 \leftarrow rv)$ 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，所述信息处理单元包括：有向图获取部分，获取通过以更短的有向边替换组成临时有向图的至少一个有向边而生成的有向图，所述临时有向图是根据对于给定整数 k 满足 $n^{(x-1)}/k < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，通过在第一到第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的，其中 $i = 0$，1，.....，x-1；以及密钥生成部分，基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0012] 进一步，为了解决以上问题，根据本发明的一个方面，提供了信息处理单元，包括：树结构设置部分，配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 $(i \rightarrow j)$ 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 $(i \leftarrow j)$ 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；

[0013] 进一步包括坐标轴设置部分，用以设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 $(1 \rightarrow n)$ 中包括的子集相关的、且以包含度从左至右增大

的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第 四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点，

[0014] 进一步包括临时有向图生成部分，用以通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 相关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 相关的临时有向图，来生成与集合 (1 → n) 相关的临时有向图，

[0015] 进一步包括最长有向路径确定部分，用以在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及

[0016] 进一步包括有向图生成部分，用以通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

[0017] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发以及集合密钥的生成，由此当解密所分发的经加密的信息时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，减少要由每个用户保存的密钥的数量。

[0018] 在与集合 (1 → n)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 相关的临时有向图之中，最长有向路径确定部分可以关于不包括最长有向路径的各个临时有向图，确定在每个临时有向图中的最长有向路径。进一步，在对于各个临时有向图的每个临时有向图中，有向图生成部分可以通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

[0019] 信息处理单元可以进一步包括密钥生成部分，用以基于所述有向图生成用于加密内容或内容密钥的集合密钥。

[0020] 响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、

t(S2)、.....、t(Sk)。

[0021] 响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

[0022] 信息处理单元可以进一步包括初始中间密钥设置部分，用以将给定随机数设置为与每个有向图的尾部对应的中间密钥。

[0023] 信息处理单元可以进一步包括加密部分，用以使用集合密钥来解密内容或内容密钥。

[0024] 信息处理单元可以进一步包括传送部分，用以向分别与组成给定二叉树的叶节点 1 到 n(n 是自然数）中的一些或全部相关的终端单元传送由加密部分加密的内容或内容密钥。

[0025] 有向图获取部分可以通过将更短的有向边朝向每个有向路径的尾部放置的方式来替换临时有向图的有向边。

[0026] 信息处理单元可以进一步包括子集确定部分，通过将叶节点 1 到 n 的子集设置为 Si，确定允许解密通过使用集合密钥而加密的内容或内容密钥的终端单元的集合 (N\R)，并确定满足集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm。

[0027] 子集确定部分可疑确定子集 S1 到 Sm 以便最小化 m。

[0028] 信息处理单元可以进一步包括传送部分，用以向终端单元传送指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。

[0029] 信息处理单元可以进一步包括解密部分，用以使用集合密钥来解密内容或内容密钥。

[0030] 信息处理单元可以进一步包括接收部分，其与组成给定二叉树的一个或多个叶节点 1 到 n(n 是自然数）相关，接收使用集合密钥加密的内容或内容密钥。

[0031] 由接收部分接收到的经加密的内容或经加密的内容密钥可以由一个或多 个信息处理单元来解密，所述一个或多个信息处理单元与作为集合 S 的元素的叶节点相关，所述集合 S 包括在定义为叶节点 1 到 n 的子集的集合 Si 中与其自身相关的叶节点。

[0032] 进一步，为了解决以上问题，根据本发明的另一方面，提供了终端单元，包括 :密钥生成部分，基于有向图生成用于解密内容或内容密钥的集合密钥。

[0033] 由终端单元参照的所述有向图通过如下步骤获得 :配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv ；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与

集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点，通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分 别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 相关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0034] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0035] 终端单元可以进一步包括解密部分，用以使用集合密钥来解密经加密的内容或经加密的内容密钥。

[0036] 响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

[0037] 响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

[0038] 解密部分通过使用所述集合密钥来解密经加密的内容密钥，并使用经解密的内容密钥来解密经加密的内容。

[0039] 终端单元进一步包括判定部分，基于所接收到的信息来判定所述终端单元是否属于子集 S1 到 Sm 中的任意一个，并基于判定结果来判定是否允许经加密的内容的解密，其中将树的叶节点 1 到 n 的子集定义为 Si，以及当确定了允许解密通过使用所述集合密钥或所述内容密钥而加密的内容的终端单元的集合 (N\R) 时，确定满足集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，并接收指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。

[0040] 当判定所述终端单元属于子集 S1 到 Sm 中的任意一个时，解密部分通过使用与所述终端单元所属的子集对应的集合密钥来解密内容或内容密钥。

[0041] 进一步，为了解决以上问题，根据本发明的再一方面，提供了信息处理方法，包括：有向图获取步骤，在由多条有向边组成的临时有向图中，获取通过以更短的有向边替换组成所述临时有向图的至少一条有向边而生成的有向图；以及密钥生成步骤，基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0042] 进一步，为了解决以上问题，根据本发明的再一方面，提供了信息处理方法，在由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号定义为 lv，而将分配给位于右端的叶节点的编号定义为 rv，对于自然数 i 和 j，其中 $i \leqslant j$，假设将集合 (i → j) 表示为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 表示为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，所述信息处理方法包括：有向图获取步骤，获取通过以更短的有向边替换组成临时有向图的至少一个有向边而生成的有向图，所述临时有向图是根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，通过在第一到第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的，其中 i = 0，1，.....，x-1；以及密钥生成步骤，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0043] 进一步，为了解决以上问题，根据本发明的再一方面，提供了信息处理单元，包括：树结构设置步骤：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是 自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；坐标轴设置步骤：设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及

设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点；临时有向图生成步骤：通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；最长有向路径确定步骤，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径；以及有向图生成步骤，通过以每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组 成每个有向路径的有向边来生成有向图。

[0044] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0045] 进一步，为了解决以上问题，根据本发明再一方面，提供了密钥生成方法，包括：密钥生成步骤，基于有向图生成用于解密内容或内容密钥的集合密钥。

[0046] 用于密钥生成方法的所述有向图通过如下步骤获得：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ⩽ j，将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义为 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第

一水平坐标轴的右端的坐标点设置为临时坐标点；通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐 标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0047] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0048] 进一步，为了解决以上问题，根据本发明的再一方面，提供了一种程序，使得计算机执行如下功能：树结构设置功能：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；坐标轴设置功能：设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv- → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列 在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点；临时有向图生成功能：通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的

每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；最长有向路径确定功能，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径；以及有向图生成功能，通过以每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

[0049] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0050] 进一步，为了解决以上问题，根据本发明的再一方面，提供了一种程序，使得计算机执行以下功能：密钥生成功能，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0051] 根据所述程序的有向图通过如下步骤获得：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义为 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的 编号设置为 rv；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点；通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 $i = 0$ 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合

(lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0052] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的 计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0053] 进一步，为了解决以上问题，根据本发明的一个方面，提供了信息处理单元，包括：有向图获取部分，在由多条有向边组成的临时有向图中，获取通过在组成所述临时有向图的多条有向边之中保留较长的有向边而以更短的有向边替换留下的至少一条有向边而生成的有向图；以及密钥生成部分，基于由所述有向图获取部分获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0054] 进一步，为了解决以上问题，根据本发明的一个方面，提供了一种信息处理单元，用以根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，处理通过在第一和第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的有向图，其中 i = 0，1，……，x-1，在由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv，对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，所述信息处理单元包括：临时有向图获取部分，获取临时有向图；有向图生成部分，通过在组成由所述临时有向图获取部分获取的所述临时有向图的多条有向边之中保留较长的有向边来生成有向图；最长有向路径确定部分，在组成所述有向图的多条有向边之中，确定连续有向边的最大数量；有向边替换部分，通过以更短的有向边替换组成所述有向图的至少一条有向边来重 建所述有向图，以便不超过连续有向边的最大数量，以及密钥生成部分，基于由所述有向边替换部分重建的所述有向图，生成用于加密内容或内容密钥的集合密钥。

[0055] 进一步，为了解决以上问题，根据本发明的一个方面，提供了信息处理单元，包括：树结构设置部分，配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；坐标轴设置部分，用以设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；以及将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在所述第一临时坐标点的右侧；临时有向图生成部分，用以通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i = 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有 向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴上第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 相关的临时有向图，来生成与集合 (1 → n) 相关的临时有向图；最长有向路径确定部分，在由连续有向边形成的有向路径之中，确定具有组成所述有向路径的有向边的最大数量的最长有向路径；以及有向图生成部分，通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每一条有向路径的有向边来生成有向图。

[0056] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0057] 在与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图之中，最长有向路径确定部分可以关于不包括最长有向路径的各个临时有向图，确定在每个临时有向图中的最长有向路径。进一步，在对于各个临时有向图的每个临时有向图中，有向图生成部分可以通过每个有向路径的有向边的数量不超过最长有向路径的

有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0058] 信息处理单元可以进一步包括密钥生成部分，基于有向图生成用于加密内容或内容密钥的集合密钥。

[0059] 响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

[0060] 响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

[0061] 信息处理单元可以进一步包括加密部分，用以使用所述集合密钥来加密内容或内容密钥。

[0062] 信息处理单元可以进一步包括传送部分，用以向分别与组成给定二叉树的叶节点 1 到 n 中的一些或全部相关的终端单元传送由所述加密部分加密的 内容或内容密钥，其中 n 是自然数。

[0063] 有向图获取部分可以获取以将更短的有向边朝向由连续有向边组成的每个有向路径的端点而放置的方式替换有向边的有向图。

[0064] 信息处理单元可以进一步包括子集确定部分，用以通过将叶节点 1 到 n 的子集定义为 Si，确定允许解密通过使用集合密钥或内容密钥而加密的内容的终端单元的集合 (N\R)，并确定满足集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，以便最小化 m。

[0065] 信息处理单元可以进一步包括传送部分，用以向所述终端单元传送指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。

[0066] 信息处理单元可以进一步包括解密部分，用以通过使用所述集合密钥来解密内容或内容密钥。

[0067] 信息处理单元可以进一步包括接收部分，其与组成给定二叉树的一个或多个叶节点 1 到 n(n 是自然数) 相关，用以接收通过使用所述集合密钥而加密的内容或内容密钥。

[0068] 由所述接收部分接收到的经加密的内容或经加密的内容密钥可以由一个或多个信息处理单元来解密，所述一个或多个信息处理单元与作为集合 S 的元素的叶节点相关，所述集合 S 包括在定义为叶节点 1 到 n 的子集的集合 Si 中与其自身相关的叶节点。

[0069] 进一步，为了解决以上问题，根据本发明的另一方面，提供了终端单元，包括 :密钥生成部分，基于有向图生成用于解密内容或内容密钥的集合密钥。其中所述有向图通过如下步骤而获得 :配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv ;设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集

合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点， 第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的右侧，通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0070] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0071] 响应于与所述有向图中某个坐标点对应的子集 S 的中间密钥 t(S) 的输入，所述密钥生成部分输出对应于与所述坐标点对应的子集 S 的集合密钥 k(S) 以及位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的中间密钥 t(S1)、t(S2)、.....、t(Sk)。

[0072] 响应于与所述有向图中某个坐标点对应的子集 S 的集合密钥 k(S) 的输 入，所述密钥生成部分输出位于具有位于坐标点 S 的尾部的有向边的头部的坐标点 S1、S2、.....、Sk 的集合密钥 k(S1)、k(S2)、.....、k(Sk)。

[0073] 终端单元可以进一步包括解密部分，用以使用所述集合密钥来解密经加密的内容密钥，并使用经解密的内容密钥来解密经加密的内容。

[0074] 终端单元可以进一步包括判定部分，用以基于所接收到的信息来判定所述终端单元是否属于子集 S1 到 Sm 中的任意一个，并基于判定结果来判定是否允许经加密的内容的解密，其中将树的叶节点 1 到 n 的子集定义为 Si，以及当确定了允许解密通过使用所述集合密钥或所述内容密钥而加密的内容的终端单元的集合 (N\R) 时，确定满足集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm 的 m 个子集 S1 到 Sm，并接收指示集合 (N\R) 的信息或指示组成集合 (N\R) 的子集 S1 到 Sm 的信息。当判定所述终端单元属于子集 S1 到 Sm 中的任意一个时，所

述解密部分使用与所述终端单元所属的子集对应的集合密钥来解密所述内容或内容密钥。

[0075] 进一步，为了解决以上问题，根据本发明的另一方面，提供了信息处理方法，包括：有向图获取步骤，在由多条有向边组成的临时有向图中，获取通过在组成所述临时有向图的多条有向边之中保留较长的有向边而以更短的有向边替换留下的至少一条有向边而生成的有向图；以及密钥生成步骤，基于由所述有向图获取步骤获取的有向图，生成用于加密或解密内容或内容密钥的集合密钥。

[0076] 进一步，为了解决以上问题，根据本发明的另一方面，提供了信息处理方法，用以根据对于给定整数 k 满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，处理通过在第一和第四水平坐标轴上排列具有长度 $n^{i/k}$ 的多条有向边而形成的有向图，其中 i ＝ 0，1，……，x-1，在由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树中，其中 n 是自然数，并且其中在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv，对于自然数 i 和 j，其中 i ≤ j，将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与 根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，所述信息处理方法包括：临时有向图获取步骤，获取临时有向图；有向图生成步骤，通过在组成由所述临时有向图获取步骤获取的所述临时有向图的多条有向边之中保留较长的有向边来生成有向图；最长有向路径确定步骤，在组成所述有向图的多条有向边之中，确定连续有向边的最大数量；有向边替换步骤，通过以更短的有向边替换组成所述有向图的至少一条有向边来重建所述有向图，以便不超过连续有向边的最大数量，以及密钥生成步骤，基于由所述有向边替换步骤重建的所述有向图，生成用于加密内容或内容密钥的集合密钥。

[0077] 进一步，为了解决以上问难，根据本发明的再一方面，提供了信息处理方法，包括：树结构设置步骤：配置由向其分配了编号 1 到 n(n 是自然数) 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，并且对于自然数 i 和 j，其中 i ≤ j，通过将集合 (i → j) 定义为 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义为 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；坐标轴设置步骤：设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大

的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧，以及将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的右侧；临时有向图生成步骤：通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平坐标轴上第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；最长有向路径确定步骤，在由连续有向边形成的有向路径之中，确定具有组成所述有向路径的有向边的最大数量的最长有向路径；以及有向图生成步骤，通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

[0078] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0079] 进一步，为了解决以上问题，根据本发明的再一方面，提供了密钥生成方法，包括：密钥生成步骤，基于有向图生成用于解密内容或内容密钥的集合密钥。所述有向图通过如下步骤而获得：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 i ⩽ j，将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义为 ({j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将 分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四

水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的右侧，通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0080] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的 计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0081] 进一步，为了解决以上问题，根据本发明的再一方面，提供了一种程序，使计算机执行如下功能：树结构设置功能：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，其中 n 是自然数，并且对于自然数 i 和 j，其中 i ⩽ j，通过将集合 (i → j) 定义为 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义为 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；坐标轴设置功能：设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧，以及将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点的

右侧；临时有向图生成功能：通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，以及通过将具有长度 1 的、具有位于第一水平 坐标轴上第一临时坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图；最长有向路径确定功能，在由连续有向边形成的有向路径之中，确定具有组成所述有向路径的有向边的最大数量的最长有向路径；以及有向图生成功能，通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边来生成有向图。

[0082] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0083] 进一步，为了解决以上问题，根据本发明的再一方面，提供了一种程序，使得计算机执行密钥生成功能，基于有向图生成用于解密内容或内容密钥的集合密钥。所述有向图通过以下步骤而获得：配置由向其分配了编号 1 到 n 的、n 个叶节点、根节点以及不同于根节点和叶节点的多个中间节点组成的二叉树，n 是自然数，并且对于自然数 i 和 j，其中 $i \leqslant j$，将集合 (i → j) 定义为 {{i},{i,i+1},...,{i,i+1,...,j-1,j}}，而将集合 (i ← j) 定义为 {{j},{j,j-1},...,{j,j-1,...,i+1,i}}，在位于某个中间节点 v 或某个根节点 v 之下的多个叶节点之中，将分配给位于左端的叶节点的编号设置为 lv，而将分配给位于右端的叶节点的编号设置为 rv；设置第一水平坐标轴，所述第一水平坐标轴与根节点相关，并且具有分别与集合 (1 → n) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，设置第二水平坐标轴，所述第二水平坐标轴与根节点相关，并且具有分别与集合 (2 ← n) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，对于每个所述中间节点，设置第三水平坐标轴，所述第三水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv → rv-1) 中包括的子集相关的、且以包含度从左至右增大的方式排列在水平坐标轴上的坐标点，以及设置第四水平坐标轴，所述第四水平坐标轴与某个中间节点 v 相关，并且具有分别与集合 (lv+1 ← rv) 中包括的子集相关的、且以包含度从右至左增大的方式排列在水平坐标轴上的坐标点，以及将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧；将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置 在第一临时坐标点的右侧，通过设置给定整数 k，计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x，以及对于每个整数 i ＝ 0 到 x-1，通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边来形成具有位于第一和第三水平坐标轴的最左侧坐标点的尾部的有向路径，通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边来形成具有位于第二和第四水

平坐标轴的最右侧坐标点的尾部的有向路径，对于第一到第四水平坐标轴中的每个，排除具有位于临时坐标点的尾部或头部的所有有向边，以及从到达第一到第四水平坐标轴上的每个坐标点的有向边中排除除了最长有向边之外的有向边，来生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图，通过将具有长度 1 的、具有位于第一水平坐标轴的右端的坐标点的头部的有向边添加到与集合 (1 → n-1) 有关的临时有向图，来生成与集合 (1 → n) 有关的临时有向图，在由连续有向边形成的有向路径之中，确定具有组成有向路径的有向边的最大数量的最长有向路径，以及通过每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边替换组成每个有向路径的有向边。

[0084] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案使能基于上述有向图的中间密钥的分发和集合密钥的生成，由此当解密所分发的经加密的内容时，在不增大对于每个用户（终端单元）来说用以生成解密密钥所需的计算量的最差值的情况下，能够减少要由每个用户保存的密钥的数量。

[0085] 因此，通过应用以上技术，可以提供新的、改进的信息处理单元、终端单元、信息处理方法、密钥生成方法和程序，其能够在接收者端减少要由终端单元保存的密钥数量，并且能够减少用于导出加密密钥所需的计算量。

[0086] 本发明的优点

[0087] 如在上文中所述，根据本发明，可以在接收者端减少要由终端单元保存的密钥数量。

附图说明

[0088] 图 1 是示出了根据本发明的一个实施例的加密密钥分发系统的说明图；

[0089] 图 2 是示出了根据所述实施例的密钥分发服务器和接收器的配置的框图；

[0090] 图 3 是示出了根据基本方案的二叉树结构的说明图；

[0091] 图 4 是示出了根据基本方案的有向图的说明图；

[0092] 图 5 是示出了根据基本方案的有向图计算方法的流程图；

[0093] 图 6 是示出了根据基本方案的中间密钥分发方法的流程图；

[0094] 图 7 是示出了根据基本方案的集合密钥生成方法的流程图；

[0095] 图 8 是示出了根据本发明的第一实施例的密钥分发服务器和终端单元的配置的框图；

[0096] 图 9 是示出了根据所述实施例的有向图生成方法的基本构思的说明图；

[0097] 图 10 是示出了根据所述实施例的有向图生成方法的流程图；

[0098] 图 11 是示出了根据所述实施例的（临时）有向图生成方法的流程图；

[0099] 图 12 是示出了根据所述实施例的有向图生成方法 (LP 确定) 的流程图；

[0100] 图 13 是示出了根据所述实施例的有向图生成方法 (PLP 确定) 的流程图；

[0101] 图 14 是示出了根据所述实施例的有向图生成方法的流程图；

[0102] 图 15 是示出了根据所述实施例的有向图的一个示例 (k = 6) 的说明图；

[0103] 图 16 是示出了根据基本方案的有向图的一个示例 (k = 3) 的说明图；

[0104] 图 17 是示出了根据所述实施例的有向图的一个示例 (k = 3) 的说明图；

[0105] 图 18 是示出了基本方案与根据所述实施例的密钥分发方案之间的比较的比较表；

[0106] 图 19 是示出了根据本发明的第二实施例的信息处理单元和终端单元的配置的框图；

[0107] 图 20 是示出了根据所述实施例的临时有向图生成方法的流程图；

[0108] 图 21 是示出了根据所述实施例的临时有向图的一个示例 (k = 6) 的说明图；

[0109] 图 22 是示出了根据所述实施例的有向图生成方法的概要的流程图；

[0110] 图 23 是示出了根据所述实施例的有向图生成方法 (LP 确定) 的流程图；

[0111] 图 24 是示出了根据所述实施例的有向图生成方法 (PLP 确定) 的流程图；

[0112] 图 25 是示出了根据所述实施例的有向图生成方法的流程图；

[0113] 图 26 是示出了根据所述实施例的有向图的一个示例 (k = 6) 的说明图；

[0114] 图 27 是示出了基本方案与根据所述实施例的密钥分发方案之间的比较的比较表；

[0115] 图 28 是示出了根据本发明的一个实施例的加密密钥分发系统的一个应用的说明图；以及

[0116] 图 29 是示出了根据本发明的一个实施例的加密密钥分发系统的一个应 用的说明图。

[0117] 附图标记说明

[0118] 100 加密密钥分发系统

[0119] 102 密钥分发服务器

[0120] 104 树结构设置部分

[0121] 106 坐标轴设置部分

[0122] 108 临时有向图生成部分

[0123] 110 有向图生成部分

[0124] 112 初始中间密钥设置部分

[0125] 114 密钥生成部分

[0126] 116 加密部分

[0127] 118 传送部分

[0128] 120 子集确定部分

[0129] 122 终端单元

[0130] 124 接收部分

[0131] 126 判定部分

[0132] 128 密钥生成部分

[0133] 130 解密部分

[0134] 202 控制器

[0135] 204 处理单元

[0136] 206 输入 / 输出接口

[0137] 208 安全存储部分

[0138] 210 主存储部分

[0139] 212 网络接口

[0140] 216 媒体接口

[0141] 218 信息媒体

[0142] 152 密钥分发服务器

[0143] 154 树结构设置部分

[0144] 156 坐标轴设置部分

[0145] 158 临时有向图生成部分

[0146] 160 有向图生成部分

[0147] 162 初始中间密钥设置部分

[0148] 164 密钥生成部分

[0149] 166 加密部分

[0150] 168 传送部分

[0151] 170 子集确定部分

[0152] 172 终端单元

[0153] 174 接收部分

[0154] 176 判定部分

[0155] 178 密钥生成部分

[0156] 180 解密部分

具体实施方式

[0157] 在下文中，将参照附图详细描述本发明的优选实施例。注意，在该说明书和附图中，具有基本上相同功能和配置的元件以相同的附图标记来表示，并省略其重复的说明。尽管为了描述的目的在一些部分中以正常字体书写下标，但是它表示相同的东西。例如，注意，BTR 和 BT_R 表示相同的东西。

[0158] < 第一实施例 >

[0159] [加密密钥分发系统 100 的配置]

[0160] 在下文中，描述根据本发明的第一实施例的加密密钥分发系统 100 的配置。图 1 是示出了根据所述实施例的加密密钥分发系统 100 的配置的说明图。

[0161] 参照图 1，加密密钥分发系统 100 包括 ：密钥分发服务器 102，被配置为根据所述实施例的信息处理单元的示例 ；多个终端单元 122，其分别由多个用户所有 ；以及网络，其将密钥分发服务器 102 与终端单元 122 进行连接。

[0162] 上述网络是连接密钥分发服务器 102 与终端单元 122 以便允许双路通信或单路通信的通信网络。由诸如因特网、电话线网络、卫星通信网和广播信道之类的公共网络、诸如 WAN(广域网，Wide Area Network)、LAN(局域网，Local Area Network)、IP-VPN(网际协议虚拟专用通信网，InternetProtocol-Virtual Private Network) 和无线 LAN 之类的专线通信网等配置该网络，例如有线或无线。

[0163] 由具有服务器功能的计算机单元等配置密钥分发服务器 102，并且可以 通过网络向外部单元传送各种信息。例如，密钥分发服务器 102 可以以广播加密方案生成加密密钥，并向终端单元 122 分发加密密钥。进一步，根据本实施例的密钥分发服务器 102 配备有作

为提供内容分发服务（如视频分发服务和电子音乐分发服务）的内容分发服务器的功能，并且它可以向终端单元 122 分发内容。当然，密钥分发服务器 102 和内容分发服务器可以被配置为分离的单元。

[0164] 例如，所述内容可以是诸如由运动图像或静止图像集合成的视频内容（如视频、电视节目、视频节目和图表）、音频内容（如音乐、讲座和电台节目）、游戏内容、文档内容、软件之类的任何内容数据。视频内容不仅可以包含视频数据，还可以包含音频数据。

[0165] 终端单元 122 是能够通过网络与外部单元进行数据通信的密钥分发服务器，并且其由每个用户所有。尽管由诸如图中所示的个人计算机（在下文中称为“PC”）之类的计算机单元（笔记本型或台式）来配置终端单元 122，但是其不限于此，并且可以由诸如 PDA（个人数字助理）、家用视频游戏机、DVD/HDD 记录器和电视机之类的家用信息设备、电视广播调谐器或解码器等来配置终端单元 122，只要它具有通过网络的通信功能即可。进一步，例如，终端单元 122 可以是诸如便携式视频游戏机、蜂窝电话、便携式视频 / 音频播放器、PDA 和 PHS 之类的、能够由用户携带的便携式设备。

[0166] 终端单元 122 可以从密钥分发服务器 102 接收各种信息。例如，终端单元 122 可以接收从密钥分发服务器 102 分发的内容。在内容分发时，密钥分发服务器 102 可以加密各种电子数据，并将它们进行分发。例如，密钥分发服务器 102 可以生成用于加密内容的内容密钥，并将其进行分发。例如，内容密钥可以由伪随机数发生器生成的随机数（伪随机数）、给定字符串或序列等来表示。通过使用内容密钥，密钥分发服务器 102 可以通过给定加密逻辑来加密内容。进一步，密钥分发服务器 102 可以向任意终端单元 122 分发内容密钥或与内容密钥对应的解密密钥。另一方面，终端单元 122 可以使用从密钥分发服务器 102 接收到的、内容密钥或与内容密钥对应的解密密钥来解密经加密的内容。

[0167] 用于生成内容密钥的伪随机数发生器是能够通过输入给定的种子值 (seed value) 而输出长间隔伪随机数序列的单元或程序，并且通常使用诸如线性同余方法或马其赛特旋转 (Mersenne Twister) 方法之类的逻辑来实现。 可应用于本实施例的伪随机数发生器当前不限于此，并且使用其他逻辑可以生成伪随机数，或者它可以是能够生成包含特殊信息或条件的伪随机数序列的单元或程序。

[0168] 进一步，根据本实施例的密钥分发服务器 102 不仅加密内容，还加密内容密钥，并将其进行分发。的确，加密并分发内容确保了一定程度的安全级别。然而，为了在大量用户之中灵活地处理被许可具有使用内容的权力的用户（在下文中称为“许可用户”）的加入和删除，加密内容密钥并将其进行分发的方法是更有利的。在这种情况下，在该实施例中，密钥分发服务器 102 首先生成用于加密和解密内容密钥的多个集合密钥。多个集合密钥分别与从大量用户中提取出的许可用户的多个子集相关，如在后面所述的那样。具体地说，密钥分发服务器 102 使用设置成只有许可用户的集合才可以解密内容密钥的集合密钥来加密内容密钥，并向所有用户的终端单元 122 分发经加密的内容密钥。在该配置中，仅许可用户的终端单元 122 可以解密经加密的内容密钥，然后通过使用内容密钥来解密经加密的内容，由此使得内容可视等。在许可用户的集合变化的情况下，密钥分发服务器 102 通过改变要用于加密内容密钥的集合密钥可以处理所述改变。为了建立以上加密密钥分发逻辑，必须配置密钥分发服务器 102 等，以便实现与集合密钥的生成和分发相关的算法。

[0169] 在下文中，首先描述根据本实施例的密钥分发服务器 102 和终端单元 122 的配置

的示例性硬件配置。其次，描述与根据本实施例的加密密钥分发逻辑有关的基本技术。第三，详细描述根据本实施例的密钥分发服务器 102 和终端单元 122 的配置，并具体地描述与基本技术在配置和效果上的差别。最后，描述根据本实施例的加密密钥分发系统的应用。

[0170] [密钥分发服务器 102 和终端单元 122 的硬件配置]

[0171] 首先参照图 2，在下文中描述根据本实施例的密钥分发服务器 102 和终端单元 122 的示例性硬件配置。图 2 示出了能够执行根据本实施例的密钥分发服务器 102 和终端单元 122 的功能的硬件配置的示例。

[0172] 例如，密钥分发服务器 102 和终端单元 122 包括控制器 202、处理单元 204、输入 / 输出接口 206、安全存储部分 208、主存储部分 210、网络接口 212 和媒体接口 216。

[0173] (控制器 202)

[0174] 控制器 202 通过总线连接到其他元件，并且它主要用以基于在主存储部分 210 中存储的程序和数据来控制所述单元的每个部分。可以由诸如 CPU(中央处理单元) 之类的处理单元来配置控制器 202。

[0175] (处理单元 204(密钥分发服务器 102))

[0176] 例如，密钥分发服务器 102 中包括的处理单元 204 可以执行内容的加密、内容密钥的加密、集合密钥的生成和用于生成集合密钥的中间密钥的导出。由此，处理单元 204 可以用作基于给定数据 (种子值等) 生成伪随机数的伪随机数发生器，并且处理单元 204 还可以基于给定算法加密内容或内容密钥。可以将给定算法作为由处理单元 204 可读的程序存储在主存储部分 210 中。进一步，可以将给定信息存储在主存储部分 210 或安全存储部分 208 中。处理单元 204 可以在主存储部分 210 或安全存储部分 208 中记录执行以上处理的输出结果。可以由诸如 CPU 之类的处理单元来配置处理单元 204，或者处理单元 204 可以与上述控制器 202 整体地形成。

[0177] (处理单元 204(终端单元 122))

[0178] 另一方面，例如，终端单元 122 中包括的处理单元 204 可以执行内容的解密、内容密钥的解密、集合密钥的生成和用于生成集合密钥的中间密钥的生成。由此，处理单元 204 可以用作基于给定数据 (种子值等) 生成伪随机数的伪随机数发生器，并且处理单元 204 还可以基于给定算法解密内容或内容密钥。可以将给定算法作为由处理单元 204 可读的程序存储在主存储部分 210 中。进一步，可以将给定信息存储在主存储部分 210 或安全存储部分 208 中。处理单元 204 可以记录在主存储部分 210 或安全存储部分 208 中执行以上处理的输出结果。可以由诸如 CPU 之类的处理单元来配置处理单元 204，或者处理单元 204 可以与上述控制器 202 整体地形成。

[0179] (输入 / 输出接口 206)

[0180] 输入 / 输出接口 206 主要连接到用于用户输入信息的输入设备和用以输出内容的处理结果或描述的输出设备。例如，输入设备可以是键盘、鼠标、轨迹球、触摸笔、键区、触摸板等，并且它可以经由有线或无线连接到输入 / 输出接口 206。在一些情况下，输入设备可以是经由有线或无线连接的便携式电子设备 (如蜂窝电话或 PDA(个人数字助理))。另一方面，例如，输出设备可以是显示单元 (如显示器)、音频输出设备 (如扬声器) 等，并且它可以经由有线或无线连接到输入 / 输出接口 206。输入 / 输出设备可以内置在密钥分 发服务器 102 或终端单元 122 中或者与密钥分发服务器 102 或终端单元 122 集成。

[0181] 输入 / 输出接口 206 通过总线连接到其他元件，并且它可以向主存储部分 210 等传送经由输入 / 输出接口 206 输入的信息。相反，输入 / 输出接口 206 可以向输出设备输出在主存储部分 210 等中存储的信息、经由网络接口 212 等输入的信息或通过在处理单元 204 等中处理这些信息而获得的结果。

[0182] （安全存储部分 208）

[0183] 安全存储部分 208 主要安全地存储隐藏所需的信息，如内容密钥、集合密钥和中间密钥。例如，可以由磁存储单元（如硬盘）、光存储单元（如光盘）、磁光存储单元、半导体存储单元等来配置安全存储部分 208。进一步，例如，可以由抗干扰 (tamper-resistant) 存储单元来配置安全存储部分 208。

[0184] （主存储部分 210）

[0185] 例如，主存储部分 210 可以存储用于控制其他元件的控制程序、用于加密内容、内容密钥等的加密程序、用于解密经加密的内容、内容密钥等的解密程序、用于生成集合密钥或中间密钥的密钥生成程序等。进一步，主存储部分 210 可以临时或永久地存储从处理单元 204 输出的计算结果或存储从输入 / 输出接口 206、网络接口 212、媒体接口 216 等输入的信息。例如，可以由磁存储单元（如硬盘）、光存储单元（如光盘）、磁光存储单元、半导体存储单元等来配置主存储部分 210。进一步，主存储部分 210 可以与安全存储部分 208 整体地形成。

[0186] （网络接口 212）

[0187] 例如，网络接口 212 连接到网络上的另一个通信单元等，并且例如，它是用于传送和接收诸如经加密的内容或内容密钥、集合密钥和中间密钥的信息、与加密有关的参数信息和与许可用户的集合有关的信息的接口装置。网络接口 212 通过总线连接到其他元件，并且它可以向其他元件传送从网络上的外部单元接收到的信息，或者向网络上的外部单元传送由其他元件保存的信息。

[0188] （媒体接口 216）

[0189] 媒体接口 216 是用于通过可拆卸地连接信息媒体 218 来读和写信息的接口，并且它通过总线连接到其他元件。例如，媒体接口 216 可以从所连接的信息媒体 218 读信息，并且将其传送到其他元件，或者将从其他元件提供的 信息写入信息媒体 218。例如，信息媒体 218 可以是诸如光盘、磁盘和半导体存储器之类的便携式存储媒体（可拆卸存储媒体）、在不通过网络的情况下在相对短的距离内经由有线或无线连接的信息终端的存储媒体等。

[0190] 在前文中，描述了能够实现根据本实施例的密钥分发服务器 102 和终端单元 122 的功能的硬件配置的示例。通过使用通用组件来配置以上元件中的每个，或者可以由专用于每个元件的功能的硬件来配置以上元件中的每个。由此当执行本实施例时，根据技术水平，可以合适地改变要使用的硬件配置。进一步，上述硬件配置仅为示例，当然其不限于此。例如，可以由相同的处理单元来配置控制器 202 和处理单元 204，并且可以由相同的存储单元来配置安全存储部分 208 和主存储部分 210。进一步，视使用而定，取消媒体接口 216、输入 / 输出接口 206 等的配置是可行的。在下文中，详细描述由具有上述硬件配置的密钥分发服务器 102 和终端单元 122 实现的加密密钥分发方案。

[0191] [根据基本技术的加密密钥分发方案]

[0192] 在提供根据本实施例的加密密钥分发方案的详细说明之前，在下文中描述形成用

于实现本实施例的基础的技术问题。配置本实施例，以便通过向下述基本技术添加改进来获得更多显著的优点。因此，与改进有关的技术是本实施例的特征。由此，要注意的是，尽管本实施例遵循在下文中所述的技术问题的基本构思，但是本实施例的本质被并入了改进的部分，并且配置是明显不同的，而且还存在与基本技术在优点上的明显区别。

[0193] 将在下文中描述的根据基本技术的加密密钥分发方案称为基本方案。基本方案将要向其分发内容的用户的终端单元的集合划分为多个子集，然后通过分配到每一子集的集合密钥来加密内容密钥，并将其进行分发。基本方案提供了用于解决关于要选择哪一子集、如何生成集合密钥和如何分发集合密钥以便减少用于加密密钥分发的通信量、要由每个用户保存的解密密钥的数量、每个用户用以生成解密密钥所需的计算量等问题的一种手段。参照图 3 到图 7，在下文中描述基本方案。

[0194] （树结构的设置）

[0195] 在基本方案中，将作为内容分发目标的终端单元（用户）的集合看作被划分为多个子集。参照图 3，在下文中描述根据基本方案划分子集的一种方式。尽管划分子集的方式当前不止一种，但是在基本方案中采用利用二叉树 划分子集的方式。示意性地，基本方案考虑节点之间的位置关系，向形成二叉树的每个节点分配一个给定子集，由此以给定组合广泛地选择用户的子集，如在下面详细描述的那样。通过图 3 所示的二叉树的示例将更清楚地理解这种选择方法的优点。参照图 3，在下文中描述构建二叉树的方法。

[0196] 首先，将在以下的描述中使用的集合定义如下。

[0197] -所有终端单元（用户）的集合 N = {1,2,.....,n}(n 是 2 的幂）

[0198] 对于自然数 i 和 j(i ≤ j)：

[0199] -[i,j] = {i,i+1,i+2,...,j}

[0200] -(i → i) = (i ← i) = {{i}}

[0201] -(i → j) = {{i},{i,i+1},...,{i,i+1,...,j}}

[0202] = {[i,i],[i,i+1],[i,i+2],...,[i,j}

[0203] -(i ← j) = {{j},{j,j-1},...,{j,j-1,...,i}}

[0204] = [j,j],[j-1,j],[j-2,j],...,[i,j]}

[0205] 在下文中，将位于二叉树 (BT) 的底部的节点称为叶节点，将位于顶部的节点称为根节点，并且将在根节点和叶节点之间的节点称为中间节点。叶节点与各个终端单元对应。进一步，为了描述的方便，在下文中假设终端单元和用户处于一一对应，并且在一些情况下由词语“用户”来表示与叶节点相关的“终端单元”。图 3 示出了 BT 的叶节点的数量 n = 64 的示例。

[0206] 首先，以叶节点的数量是 n(= 64) 的方式创建 BT。然后，从左至右向各个叶节点分配编号 1、2、.....、n。

[0207] 接着，定义用于调整 (regulate) 要分配给某个中间节点 v 的子集的索引 lv 和 rv。在位于某个中间节点 v 下方的叶节点之中，将分配给最左侧叶节点的编号定义为 lv，而将分配给最右侧叶节点的编号定义为 rv。注意，v 可以是分配给各个中间节点的顺序编号。由此，中间节点 v 指示具有索引 v 的 BT 的中间节点。

[0208] 然后，通过将 BT 的中间节点分类为两集合来定义 BT 的中间节点。在 BT 的中间节点之中，将位于父节点左侧的中间节点的集合定义为 BTL，而将位于父节点右侧的中间节点

的集合定义为 BTR。本文所指的父子关系指示在 BT 上连接的节点的分层关系，并且它意味着父节点位于上层而子节点位于下层的关系。

[0209] 进一步，与各个叶节点相关的用户集合的子集与 BT 的根节点相关。首 先，将集合 (1 → n) 和集合 (2 ← n) 与根节点相关联。由于所有叶节点均在根节点的下层连接，因此由广泛地或选择性地包括那些叶节点的集合表示根节点。具体地说，将集合 (1 → 64) 和集合 (2 ← 64) 与图 3 的根节点相关联。例如，考虑集合 (1 → 64)。集合 (1 → 64) 包括子集 [1,1]、[1,2]、.....、[1,64] 作为其元素。例如，为了表示所有用户 (叶节点)，可以使用子集 [1,64]，并且其被作为集合 (1 → 64) 的元素而包括。进一步，为了表示除了具有编号 16 之外的所有用户，可以使用子集 [1,15] 和 [17,64]，并且其分别被作为集合 (1 → 64) 和集合 (2 ← 64) 的元素而包括。以这种方式，位于根节点的下层的叶节点 (用户) 的组合可以由相关联的集合的子集表示。

[0210] 然后，将用户集合的子集与 BT 的中间节点相关联。首先，将集合 (lv+1 ← rv) 与属于上述集合 BTL 的中间节点 v 相关联。另一方面，将集合 (lv → rv-1) 与属于上述集合 BTR 的中间节点 v 相关联。当然，这些集合与 BT 的所有中间节点 v 相关联。参照图 3，在各个中间节点附近来指示这些集合。例如，关于与集合 (2 ← 4) 相关联的中间节点，分别与集合 (2 ← 2) 和集合 (3 → 3) 相关联的两个中间节点存在于所述中间节点的下层，并且具有编号 1 到 4 的叶节点被进一步连接到其。当表示除了具有编号 3 的一个之外的那些叶节点的组合时，可以由子集的群 {[1,1],[2,2],[4,4]} 或 {[1,2],[4,4]} 来表示。虽然子集 [1,1] 和 [1,2] 是与根节点相关的集合 (1 → 64) 的元素时，但子集 [2,2] 和 [4,4] 分别是集合 (2 ← 2) 和集合 (2 ← 4) 的元素。

[0211] 以这种方式，基本方案通过使用二叉树 BT 定义了用户集合的子集。该方法使得能够以各种组合表示用户的子集。将由那些子集组成的全集称为集合系统 Φ，并将其定义为下面的表达式 (1)。由此，下面的表达式 (1) 在数学上表示由以上方法构建的二叉树。

[0212] [表达式 1]

[0213]

$$\Phi = \bigcup_{v \in BTL} (lv+1 \leftarrow rv) \cup \bigcup_{v \in BTR} (lv \rightarrow rv-1) \cup (1 \rightarrow n) \cup (2 \leftarrow n) \quad \cdots (1)$$

[0214] 在上文中描述了配置调整子集的二叉树的方法。基本方案的基本构思是对于各个子集设置用于加密内容密钥的集合密钥，通过使用各个集合密钥来加密内容密钥，并将其分发到所有用户。通过定义如上所述的子集，至少调整了用于分类用户的组合的一种方式。在下文中，描述通过使用这些子集来 生成集合密钥的算法。

[0215] (有向图的生成)

[0216] 在下文中参照图 4 描述生成表示用于生成集合密钥的算法的有向图的方法。然而，在此之前，在下文中描述用于加密内容密钥的集合密钥与用于生成集合密钥的中间密钥之间的关系。

[0217] 如在上面简要地提到的那样，基本方案使用生成集合密钥的特定伪随机数发生器 PRSG(伪随机序列发生器)。当输入与某个子集 S0 对应的中间密钥 t(S0) 时，PRSG 输出与子集 S0 对应的集合密钥 k(S0) 以及与子集 S1、S2、.....、Sk(其与子集 S0 有关) 对应的中间密钥 t(S1)、t(S2)、.....、t(Sk)。当然，集合 S0 和 S1、S2、.....、Sk 是构成集合系

统 Φ 的任意子集。由此，PRSG 是密钥生成单元。基本方案的特征是调整 PRSG 的输入和输出之间关系的逻辑。在下文中描述调整集合 S0 和集合 S1、S2、.....、Sk 之间关系的有向图。

[0218] 将用于下面的描述的符号定义如下：

[0219] - 与子集 Si 对应的中间密钥：t(Si)

[0220] - 与子集 Si 对应的集合密钥：k(Si)

[0221] - 内容密钥：mek

[0222] - 伪随机数发生器：PRSG

[0223] （注意，将 t(S0) 的输入表示为 PRSG(t(S0))。另一方面，将来自 PRSG 的输出表示为 t(S1)||...||t(Sk)||k(S0) ← PRSG(t(S0))）

[0224] - 有向图：H

[0225] （注意，将与集合 (i ← j) 对应的有向图表示为 H(i ← j)）

[0226] - 有向边：E

[0227] - 有向路径：P

[0228] 首先，确定参数 k(k 是自然数)。为了简化，假设在该示例中 k|log(n)（在下文中，log 的底数是 2)。由于参数 k 最终影响要由终端单元 122 保存的中间密钥的数量以及生成集合密钥所需的计算量，因此必须根据情况合适地设置参数 k。在图 4 中，例如，设置 k = 6。

[0229] 接着，在下文中描述绘制有向图的特定方式。首先，作为图示，描述与属于 BTR 的中间节点 v 对应的有向图 H(lv → rv-1)。

[0230] （步骤 1）设置用于构建有向图 H(lv → rv-1) 的水平坐标轴。在水平坐标 轴上，将形成集合 (lv → rv-1) 的元素的子集 Si 作为坐标点分配。以包含度从左至右变大的方式排列形成坐标点的子集 Si。例如，采用有向图 H(5 → 7) = H({[5,5],[5,6],[5,7]}) 作为示例，坐标轴具有从左侧顺序地向其分配了子集 [5,5]、[5,6]、[5,7] 的三个坐标点。

[0231] 如果在第一和第三水平坐标轴上右向有向图 H 的起点所位于的垂直线是 x，则有向图 H 与垂直线 y 的交叉点表示 [x,y]，而如果在第二和第四水平坐标轴上左向有向图 H 的起点所位于的垂直线是 z，则有向图 H 与垂直线 y 的交叉点表示 [y,z]。

[0232] 此后，将用作起点的临时坐标点置于位于坐标轴最左侧的坐标点的左侧，并且将用作终点的临时坐标点置于位于坐标轴最右侧的坐标点的右侧。在以这种方式设置的坐标轴中，从左端的临时坐标点（起点）到右端的临时坐标点（终点）的长度 Lv 为 Lv = rv-lv+1。

[0233] （步骤 2）设置构成有向图 H(lv → rv-1) 的有向边。

[0234] (S2-1) 计算满足 $n^{(x-1)/k} < Lv \leqslant n^{x/k}$ 的整数 x。整数 x 满足 $1 \leqslant x \leqslant k$。

[0235] (S2-2) 通过从 0 到 x-1 改变计数 i 来执行以下操作。从水平坐标轴的左端处的起点开始，重复设置延伸到距离坐标点 $n^{i/k}$ 的坐标点的右向有向边（跳到距离坐标点 $n^{i/k}$ 的坐标点）直到有向边的头达到水平坐标轴的右端的终点或者下一待设置的头超过终点为止。

[0236] （步骤 3）删除其尾或头位于临时坐标点的所有有向边。

[0237] （步骤 4）如果存在达到某个坐标点的多个有向边，则仅留下最长有向边，并删除除了所述最长有向边之外的所有有向边。

[0238] 在执行了以上步骤(步骤1)到(步骤4)之后,完成了有向图H(1v→rv-1)。例如,参照位于作为示例的图4的顶部起第三层上右侧的有向图H(33→63),有向图H(33→63)的实质是由作为拱形曲线和连接到拱形曲线的一端并在水平方向中延伸的直线的有向边组成的一组线。进一步,构成有向图H(33→63)曲线和直线是有向边。有向边的一端与垂直线的交叉点是坐标点。尽管在图4中没有清楚地示出水平坐标轴,但是水平坐标轴由垂直线与有向边的一端之间的一组交叉点组成。进一步,在有向图H(33→63)上描绘了轮廓箭头,并且其指示有向边的方向。具体地说,它表示构成有向图H(33→63)的所有有向边均为向右。

[0239] 以与有向图H(1v→rv-1)相同的方式,设置与属于BTL的中间节点v相关联的有向图H(1v+1←rv)和与根节点相关联的有向图H(1→n)和H(2←n)。注意,当设置有向图H(1v+1←rv)和H(2←n)的坐标轴时,以包含度从右至左变大的方式在水平坐标轴上排列子集Si,并且有向边的方向是向左。进一步,通过将有向边E([1,n-1],[1,n])添加到有向图H(1→n-1),生成有向图H(1→n)。另一方面,通过与有向图H(1v+1←rv)相同的方法设置有向图H(2←n)。

[0240] 通过采用图4的有向图H(1→64)作为示例,在下文中提供附加说明。首先,在有向图H(1→64)的水平坐标轴中,最左侧坐标点(与垂直线1的交叉点)是[1,1]={1},在其右侧附近的坐标点(与垂直线2的交叉点)是[1,2]={1,2},并且再在其右侧附近的坐标点是[1,3]={1,2,3}。进一步,每个有向图紧上方或紧下方的箭头指示构成该有向图H的所有有向边的方向。例如,有向图H(1→64)具有从坐标点[1,1]到[1,2]的一条有向边以及从坐标点[1,2]延伸到[1,3]和[1,4]的两条有向边。进一步,在图4的顶部描绘的黑点从左侧起分别表示有向图H(2→2)、H(3→3)、.....、H(63→63)。

[0241] 在上文中描述了配置有向图H的方法。图4示出了通过上述方法绘制与BT的中间节点和根节点对应的有向图H的结果。该示例是n=64且k=6的情况。在下文中描述通过使用有向图H来生成集合密钥的逻辑。

[0242] (集合密钥的生成)

[0243] 如之前所述的那样,基本方案通过使用分配给组成以上集合系统Φ的每个子集Si的集合密钥k(Si)来加密内容密钥mek,并将其进行分发。由此,上述有向图H的每个坐标点均与由一个或多个用户组成的子集Si对应,并且向其分配集合密钥k(Si)。进一步,还将中间密钥t(Si)分配给上述每个子集Si,并将其用于生成集合密钥k(Si)。

[0244] 顺便提及,由于在(2-2)的上述处理中重复次数是x,其中1≤x≤k,因此最多k条有向边源自有向图H的每个坐标点。作为源自某个坐标点(子集S0)的一个或多于一个有向边的目的地的坐标点的子集是以对某个坐标点的接近度为顺序(以有向边的短度为顺序)的S1、S2、.....、Sk。注意,如果源自坐标点(子集S0)的有向边的数量为q(q<k),则将Sq+1、Sq+2、.....、Sk作为哑元(dummy)对待,实际上不使用它们。

[0245] 基本方案使用响应于λ位输入而输出(k+1)λ位输出的上述PRSG,以便生成集合密钥k(Si)。如果输入与某个坐标点(子集S0)对应的中间密钥t(S0),则PRSG输出与在其尾部位于某个坐标点的有向边的头部的各个坐标点(子集S1、S2、.....、Sk)对应的中间密钥t(S1)、t(S2)、.....、t(Sk)以及对于子集S0的集合密钥k(S0)。由此,t(S1)||...||t(Sk)||k(S0)←PRSG(t(S0))。通过将PRSG的输出从左侧划界为每个都具有λ位,

获得了中间密钥 t(S1)、t(S2)、.....、t(Sk) 和集合密钥 k(S0)。

[0246] 例如，参照图 4 的有向图 H(1 → 64)，并将注意力集中在坐标点（子集 S0）= [1,8]（从左端起第八个坐标点），四条有向边源自坐标点 S0，其头位于 S1 = [1,9]、S2 = [1,10]、S3 = [1,12] 和 S4 = [1,16]。因此，如果将中间密钥 t(S0) 输入到 PRSG，则可以获得 k(S0)、t(S1)、t(S2)、t(S3) 和 t(S4)。进一步，如果将所获得的 t(S4) 输入到 PRSG，则可以获得与 S11 = [1,7]、S12 = [1,18]、S13 = [1,20]、S14 = [1,24] 和 S15 = [1,32] 对应的 k(S4) 以及 t(S11)、t(S12)、t(S13)、t(S14) 和 t(S15)。以这种方式，可以通过重复地使用 PRSG 来计算多个集合密钥 k(Si)。

[0247] 为了提高安全性的目的使用中间密钥。在存在降低用于集合密钥生成的处理量的需求同时不特别需要关注安全性的情况下，在不使用中间密钥的情况下直接从某个集合密钥计算另一个集合密钥是可行的。例如，在以上示例中，当向 PRSG 输入子集 S0 的集合密钥 k(S0) 时的输出可以是 k(S1)、k(S2)、k(S3) 和 k(S4)，其用作各个子集 S1 到 S4 的集合密钥。

[0248] 如从以上示例容易推断的那样，利用某个中间密钥，通过 PRSG 的重复使用，可以导出与有向边链可达到的坐标点对应的中间密钥以及集合密钥，所述有向边链从与某个中间密钥对应的坐标点延伸。因此，每个用户只需要保存最小数量的中间密钥，其可以导出与包括用户的子集对应的所有中间密钥。另一方面，如果生成用于加密内容密钥的集合密钥的密钥分发服务器至少保存与每个有向图 H 的初始坐标点对应的中间密钥，则通过使用 PRSG 重复地执行处理，可以导出与有向图的其他坐标点对应的集合密钥。

[0249] 由此，在密钥分发系统的建立时，密钥分发系统的管理员对于密钥分发服务器中每个有向图 H 的初始坐标点（根），设置 λ 位随机数，例如，作为中间密钥。有向图 H 的初始坐标点（根）是有向边起源但没有有向边到达的坐标点。例如，图 4 中有向图 H(1 → 64) 初始坐标点是水平坐标轴的左端的坐标点 [1,1]。

[0250] 以上描述了生成集合密钥的方法。上述集合密钥生成方法不仅用在内容密钥的传送端的密钥生成服务器中，而且用在接收端的终端单元中。

[0251] （中间密钥的分发）

[0252] 在下文中描述从密钥分发服务器向每个用户的终端单元的中间密钥的分发。如之前简要提到的那样，必须向每个用户的终端单元提供能够导出与包括用户的终端单元的所有子集对应的集合密钥的多个中间密钥。当然，必须避免提供使能与不包括用户的终端单元的子集对应的集合密钥的导出的中间密钥，并且优选的是所提供的中间密钥的数量在存储器容量的有效性方面是最小的。

[0253] 据此，中间密钥的分发者提取具有用户 u 的终端单元所属的子集（在下文中也称为“用户 u 所属的子集”或“包括用户 u 的子集”）作为元素的所有有向图 H。然后，如果在与有向图 H 的初始坐标点（根）对应的子集中包括用户 u，则分发者只向用户 u 的终端单元提供与初始坐标点对应的中间密钥。另一方面，如果用户 u 属于与有向图 H 的初始坐标点不同的坐标点对应的任意子集，则分发者寻找这样的子集 S0，即：在子集 S0 中包括用户 u，而在作为子集 S0 之父的子集 parent(S0) 中不包括用户 u，并且向用户 u 的终端单元提供子集 S0 的中间密钥 t(S0)。换句话说，如果与初始坐标点不同且与包括用户 u 的子集对应的多个坐标点存在于有向图 H 中，则分发者从那些坐标点中提取这样的坐标点 S0，即：在与到

达与子集S0对应的坐标点的有向边的尾部对应的子集parent(S0)中不包括用户u，并且向用户u的终端单元提供坐标点(S0)的中间密钥t(S0)。如果存在多个这样的坐标点S0，则提供各个坐标点的中间密钥t(S0)。由有向边确定坐标点的父子关系，并且位于有向边尾部的坐标点用作位于头部的坐标点之父，而位于有向边的头部的坐标点用作位于尾部的坐标点之子。在下文中，将位于到达某个坐标点S0的有向边的尾部的坐标点parent(S0)称为父坐标点。如果某个坐标点S0是有向图H的起点，则不存在父坐标点，而如果它不是有向图H的起点，则仅存在一个父坐标点。在一个有向图H中，在一些情况下，可以存在多个这样的坐标点，即：在与其对应的子集中包括用户u，而在与其父坐标点对应的子集中不包括用户u。

[0254] 参照图4的示例，在下文中具体描述中间密钥的分发方法。

[0255] (示例1)考虑分发至用户1的中间密钥。首先，作为搜索具有用户1所属的子集作为元素的有向图H的结果，仅发现有向图H(1→64)。用户1属于作为有向图H(1→64)的初始坐标点的子集[1,1]。由此，仅向用户1提供中间密钥t{[1,1])。

[0256] (示例2)考虑分发至用户3的中间密钥。首先，作为搜索具有用户3所属的子集作为元素的有向图H的结果，发现有向图H(1→64)、H(2←64)、H(2←32)、H(2←16)、H(2←8)、H(2←4)和H(3→3)。观察有向图H(1→64)，用户3不属于初始坐标点的子集[1,1]，而属于位于第三及后续点的子集[1,3]、[1,4]、.....、[1,64]。在这些坐标点之中，其父坐标点不包括用户3的坐标点仅为[1,3]和[1,4]。具体地说，在作为包括用户3的坐标点[1,3]和[1,4]的父坐标点parent([1,3])和parent([1,4])的坐标点[1,2]中不包括用户3。因此，向用户3提供t([1,3])和t([1,4])作为与有向图H(1→64)对应的中间密钥。以相同的方式，对于其他有向图H(2←64)，H(2←32)，H(2←16)，H(2←8)，H(2←4)和H(3→3)选择对应的中间密钥，并将其提供给用户3。结果，向用户3提供共计八个中间密钥。

[0257] 参照图5简要地总结直到将中间密钥分发至每个用户的终端单元为止的处理。图5是示出了在系统建立时密钥分发服务器中中间密钥分发的处理流程的流程图。

[0258] 如图5所示，密钥分发系统的密钥分发服务器首先设置参数等。例如，密钥分发服务器确定用户的数量n、集合密钥和中间密钥的位数λ、给定参数k、通过PRSG的伪随机数生成算法等，并将它们公布(publish)到所有用户的终端单元(S102)。接着，密钥分发服务器将用户集合划分为给定子集，然后确定并公布由并集(union)表示的集合系统Φ(参照以上表达式(1))(S104)。然后，确定并公布有向图H和形成各个有向图H的有向边T(步骤S106)。进一步，确定与组成集合系统Φ的各个子集对应的中间密钥(S108)。此后，向每个用户的终端单元122分发必要的中间密钥，以便每个用户可以导出与包括用户的子集对应的集合密钥(S110)。

[0259] 在上文中描述了中间密钥的分发方法。如果使用以上分发方法，则分发用以生成集合密钥的、对于每个许可用户的终端单元所需的最小数量的中间密钥，由此使得能够减少密钥分发服务器与终端单元之间的通信量，并且能够减少每个用户的终端单元中用于中间密钥的存储器容量。

[0260] (内容密钥的分发)

[0261] 在下文中描述通过密钥分发服务器分发经加密的内容密钥mek的方法。首先，密

钥分发服务器通过使用仅可以由许可用户的终端单元 122 生成的集合密钥来加密内容密钥 mek。具体地说，密钥分发服务器确定要排除的用户 （在下文中称为排除用户）的终端单元的集合 R，然后通过从所有用户的终端单元 1 到 n 的集合 N 中排除掉排除用户的终端单元的集合 R（在下文中称为“排除用户的集合 (R)”），来确定许可用户的终端单元的集合 N\R（在下文中称为“许可用户的集合 (N\R)”）。然后，通过从组成集合系统 Φ 的子集中选择的子集 Si（i ＝ 1、2、.....、m）的并集来表示许可用户的集合 (N\R) ＝ S1 ∪ S2 ∪ ... ∪ Sm。尽管存在子集 Si 的大量组合，但是选择具有最小值 m 的子集 Si。在以这种方式选择子集 Si 之后，密钥分发服务器通过使用与每个子集 Si 对应的集合密钥 k(Si) 来加密内容密钥 mek。具体地说，通过集合密钥 k(S1)、k(S2)、.....、k(Sm) 来加密内容密钥 mek，并且内容密钥 mek 变为 m 个经加密的内容密钥 mek。然后，将 m 个经加密的内容密钥 mek 分发至所有用户的终端单元 1 到 n。此时，还将指示许可用户的集合 N\R 的信息或指示 m 个子集 Si 的信息分发至所有用户的终端单元 1 到 n。

[0262] 参照图 6 简要地总结经加密的内容密钥 mek 的分发的处理流程。图 6 是示出了用于内容密钥的分发的处理流程的流程图。

[0263] 如图 6 所示，密钥分发服务器首先确定排除用户的集合 R，并获取许可用户的集合 N\R(S112)。接着，从组成集合系统 Φ 的子集中以使得 m 值最小的方式选择具有并集 N\R 的 m 个子集 Si（i ＝ 1、2、.....、m）(S114)。然后，通过使用分别与所选择的子集 Si 对应的集合密钥 k(Si) 来加密内容密钥 mek(S116)。进一步，向所有用户的终端单元 1 到 n 分发指示许可用户的集合 N\R 或各个子集 Si 的信息以及 m 个经加密的内容密钥 mek(S118)。

[0264] 在上文中描述了内容密钥 mek 的加密方法和分发方法。如果使用以上加密方法，则以集合密钥的数量是所需的最小值的方式有效地选择子集 Si。由于通过使用最小所需数量的集合密钥来由此加密内容密钥 mek，因此可以节省加密所需的计算量，并且还可以减少要分发的经加密的内容密钥 mek 的数量，由此减少通信量。

[0265] （内容密钥的解密）

[0266] 在下文中描述每个用户的终端单元中经加密的内容密钥的解密处理。解密处理是这样的处理：终端单元基于从上述密钥分发服务器接收到的、指示许可用户的集合 N\R 或 m 个子集 Si 的信息以及 m 个密文，来获取内容密钥 mek。

[0267] 终端单元从上述密钥分发服务器接收经加密的内容密钥以及指示许可用 户的集合 N\R 的信息或表示 m 个子集 Si 的信息。进一步，终端单元分析所述信息，并判定其是否属于 m 个子集 Si 中的任意一个。如果终端单元不属于子集中的任意一个，则结束解密处理，因为它是排除用户的终端单元。另一方面，如果终端单元发现其所属的子集 Si，则它通过使用上述 PRSG 导出与子集 Si 对应的集合密钥 k(Si)。PRSG 的配置如之前描述的那样。

[0268] 在该步骤中，如果在系统建立时预先从密钥分发服务器向终端单元提供与以上子集 Si 对应的中间密钥 t(Si) 并将其预先保存，则通过向 PRSG 输入中间密钥 t(Si) 可以导出与以上子集 Si 对应的集合密钥 k(Si)。另一方面，如果终端单元不保存相关的中间密钥 t(Si)，则终端单元通过重复地向 PRSG 输入所保存的中间密钥可以导出期望的集合密钥 k(Si)。进一步，终端单元通过使用以这种方式导出的集合密钥 k(Si) 解密经加密的内容密钥 mek。

[0269] 参照图 4 的示例具体描述终端单元中上述集合密钥 k(Si) 的导出。在用户 3 的终

端单元中，假设选择“1,8”作为其所属的子集。如上所述，用户 3 的终端单元保存子集 [1,4] 的中间密钥。参照图 4 的有向图 H(1 → 64)，设置从坐标点 [1,4] 向坐标点 [1,8] 延伸的有向边，并且该有向边在其尾部位于坐标点 [1,4] 的有向边之中具有第三最短长度（跳跃距离）。由此，在向 PRSG 输入用于子集 [1,4] 的中间密钥 t([1,4]) 时的输出之中，从顶部起的第三 λ 位部分是用于子集 [1,8] 的中间密钥 t([1,8])。终端单元从 PRSG 的输出中提取中间密钥 t([1,8])，并将其再次输入到 PRSG，并提取最终的 λ 位部分，由此获取期望的集合密钥 k([1,8])。

[0270] 同样地，在用户 1 的终端单元中，假设选择 [1,8] 作为其所属的子集。用户 1 的终端单元保存子集 [1,1] 的中间密钥。在这种情况下，终端单元 122 通过从向 PRSG 输入用于 [1,1] 的中间密钥 t([1,1]) 时的输出中提取从顶部起第一 λ 位部分（与中间密钥 t([1,2]) 对应），然后从向 PRSG 输入中间密钥 t([1,2]) 时的输出中提取从顶部起第二 λ 位部分（与中间密钥 t([1,4]) 对应），进一步从向 PRSG 输入中间密钥 t([1,4]) 时的输出中提取从顶部起第三 λ 位部分（与中间密钥 t([1,8]) 对应），并最终从向 PRSG 输入中间密钥 t([1,8]) 时的输出中提取最后部分（与集合密钥 k([1,8]) 对应），可以获取期望的集合密钥 k([1,8])。

[0271] 参照图 7 总结用于在每个用户的终端单元中解密经加密的内容密钥 mek 的处理流程。图 7 是示出了在每个用户的终端单元中用于内容密钥的解密的处理流程的流程图。

[0272] 如图 7 所示，每个用户的终端单元首先从密钥分发服务器接收 m 个经加密的内容密钥 mek 和指示许可用户的集合 N\R 的信息或者指示 m 个子集 Si(i = 1,2,.....,m) 的信息 (S120)。接着，终端单元基于所述信息搜索其所属的子集 Si(S122)，并判定其是否属于 m 个子集 Si 中的任意一个（步骤 S124)。

[0273] 结果，如果终端单元发现其所属的子集 Si，则它通过使用以上 PRSG 导出与子集 Si 对应的集合密钥 k(Si)(S126)。PRSG 的配置如之前所述的那样。如果在建立时由密钥分发服务器向终端单元提供与子集 Si 对应的中间密钥 t(Si) 并将其预先保存，则它通过一次性地使用 PRSG 可以导出集合密钥 k(Si)。另一方面，如果终端单元不保存相关的中间密钥 t(Si)，则它通过重复地使用 PRSG 可以导出期望的集合密钥 k(Si)。此后，终端单元通过使用以这种方式导出的集合密钥 k(Si) 解密经加密的内容密钥 mek(S128)。

[0274] 另一方面，如果终端单元在步骤 S124 判定它不属于子集 Si 中的任意一个，则终端单元显示并输出从允许访问内容的终端单元中将其排除（即，它是排除用户）(S130)，并结束内容密钥的解密处理。

[0275] 在上文中描述了在终端单元中内容密钥的解密方法。通过利用用于生成中间密钥和集合密钥的 PRSG，基于与有向图 H 有关的信息执行以上解密方案。由此，在每个用户的终端单元中与有向图有关的信息和 PRSG 也是必需的。然而，使用 PRSG 的方法使得能够最小化要由每个用户的终端单元保存的中间密钥的数量。

[0276] 在上文中描述了根据所述实施例的基本技术的加密密钥分发方案。通过利用基本方案，要由每个用户的终端单元保存的中间密钥的数量是 O(k*log(n))，并且生成集合密钥所需的计算量 (PRSG 的操作次数）不超过 $(2k-1)*(n^{1/k}-1)$。然而，根据基本技术的加密密钥分发方案（如在下面描述的图 13 所示）存在如下问题 :要由每个用户的终端单元保存的中间密钥的数量仍然很大。

[0277] 进一步，当解密经加密的内容密钥 mek 时终端单元所需的计算量的决定因素取决于为了导出期望的中间密钥而执行 PRSG 的次数。最差的值由有向图 H 中从初始坐标点（根）到最远的最终坐标点（没有有向边源自的叶）有向边的数量（即，跳跃的数量）表示。在图 4 所示的示例中，为了从有向图 H(1 → 64) 的初始坐标点 [1,1] 达到最终的坐标点 [1,64]，必须穿过十一条有向边（执行十一次跳跃），这意味着执行 PRSG 十一次。由此，根据基本技术的加密密钥分发方案存在另一个问题 :PRSG 的执行次数太多，并且由此用于导出中间密钥的计算量很大。

[0278] 本发明的发明人已经进行了解决以上问题的广泛研究，并开发出了根据本发明的第一实施例的加密密钥分发方案（如在下文中所述）。根据本实施例的加密密钥分发方案通过以更短的有向边替换了组成有向图的一条有向边而重建了有向图，由此实现了要由终端单元 122 保存的中间密钥的数量的减少。在下文中，详细描述要执行根据本实施例的加密密钥分发方案的密钥分发服务器 102 和终端单元 122 的功能性配置，以及加密密钥分发方案的特征和优点。

[0279] [密钥分发服务器 102 的配置]

[0280] 参照图 8，在下文中详细描述根据本实施例的密钥分发服务器 102 的配置。图 8 是示出了根据本实施例的密钥分发服务器 102 和终端单元 122 的配置的框图。

[0281] 如图 8 所示，密钥分发服务器 102 由树结构设置部分 104、坐标轴设置部分 106、临时有向图生成部分 108、有向图生成部分 110、初始中间密钥设置部分 112、密钥生成部分 114、加密部分 116、传送部分 118 和子集确定部分 120 组成。特别地，将树结构设置部分 104、坐标轴设置部分 106、临时有向图生成部分 108 和有向图生成部分 110 统称为密钥生成逻辑构建块。同样地，将初始中间密钥设置部分 112 和密钥生成部分 114 统称为密钥生成块。

[0282] 在下文中描述组成密钥生成逻辑构建块的元件。密钥生成逻辑构建块执行与上述 [基本技术描述] 中（树结构的设置）和（有向图的生成）对应的处理。

[0283] （树结构设置部分 104）

[0284] 树结构设置部分 104 配置由向其分配了编号 1 到 n(n 是自然数）的 n 个叶节点、根节点和多个除了根节点和叶节点之外的中间节点组成的二叉树，并在位于某个中间节点 v 或根节点 v 的下层的多个叶节点之中，将位于左端的叶节点的编号设置为 lv，将位于右端的叶节点的编号设置为 rv。进一步，树结构设置部分 104 将集合 (1 → n) 和集合 (2 ← n) 分配给根节点，并且如果某个中间节点 v 位于其父节点的左侧，则将集合 (lv+1 ← rv) 分配给中间节点，如果中间节点 v 位于其父节点的右侧，则将集合 (lv → rv-1) 分配给中间节点。

[0285] 如上所述，树结构设置部分 104 具有能够构造 m 层树结构并且假设 m ＝ 2 （二叉树）的情况的配置，例如，可以构造与根据基本方案的二叉树结构（图 3）相同的树结构。由此，由树结构设置部分 104 构造的树结构的每个节点的意义与根据之前所述的基本方案构建的二叉树结构的每个节点的意义基本上相同。尽管为了描述的方便起见，在下文中仅描述二叉树结构，但是其不限于此。

[0286] （坐标轴设置部分 106）

[0287] 坐标轴设置部分 106 设置与根节点对应的第一水平坐标轴，其上与集合 (1 → n)

中包括的各个子集相关的坐标点在所述水平坐标轴上以包含度从左至右变大的方式排列。接着，坐标轴设置部分 106 设置与根节点对应的第二水平坐标轴，其上与集合 (2 ← n) 中包括的各个子集相关的坐标点在所述水平坐标轴上以包含度从右至左变大的方式排列。然后，对于每个中间节点，坐标轴设置部分 106 设置与某个中间节点 v 对应的第三水平坐标轴，其上与集合 (lv → rv-1) 中包括的各个子集相关的坐标点在所述水平坐标轴上以包含度从左至右变大的方式排列，并且设置与某个中间节点 v 对应的第四水平坐标轴，其上与集合 (lv+1 ← rv) 中包括的各个子集相关的坐标点在所述水平坐标轴上以包含度从右至左变大的方式排列。进一步，坐标轴设置部分 106 将一个临时坐标点放置在位于第一到第四水平坐标轴的左端的坐标点的左侧和位于第二到第四水平坐标轴的右端的坐标点的右侧，并将位于第一水平坐标轴的右端的坐标点设置为临时坐标点。

[0288] 如上所述，坐标轴设置部分 106 设置用于构建与由树结构设置部分 104 配置的树结构的各个节点对应的有向图的坐标轴。第一水平坐标轴表示与集合 (1 → n) 的坐标轴，第二水平坐标轴表示与集合 (2 ← n) 对应的坐标轴，第三水平坐标轴表示与集合 (lv → rv-1) 的坐标轴，而第四水平坐标轴表示与集合 (lv+1 ← rv) 对应的坐标轴。由于对于每个中间节点 v 设置第三水平坐标轴和第四水平坐标轴，因此分别设置多个坐标轴。具体地说，设置与中间节点的数量相同的第三水平坐标轴和第四水平坐标轴的数量。

[0289] (临时有向图生成部分 108)

[0290] 临时有向图生成部分 108 设置给定整数 k，并计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x。接着，对于每个整数 i ＝ 0 到 x-1，临时有向图生成部分 108 通过连接 (couple) 具有长度 $n^{i/k}$ 的一条或多条右向有向边，形成其起点位于第一和第三坐标轴上的最左侧的坐标点的有向路径，并进一 步通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边，形成其起点位于第二和第四坐标轴上的最右侧的坐标点的有向路径。然后，临时有向图生成部分 108 对于第一到第四水平坐标轴中的每个，排除其尾部或头部位于每个临时坐标点的所有有向边。进一步，临时有向图生成部分 108 从到达第一到第四水平坐标轴上每个坐标点的有向边中，排除除了最长有向边之外的有向边，由此生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图 I’(1 → n-1)、I’(2 ← n)、I’(lv+1 ← rv) 和 I’(lv → rv-1)。此后，临时有向图生成部分 108 将具有长度 1 的有向边 (其头部是位于第一水平坐标轴的右端的坐标点) 添加到与集合 (1 → n-1) 有关的临时有向图 I’(1 → n-1)，由此生成与集合 (1 → n) 有关的临时有向图 I’(1 → n)。

[0291] 如上所述，临时有向图生成部分 108 生成临时有向图 I’作为生成期望的有向图 I 的预处理。临时有向图 I’与基本方案中的有向图 H 对应。

[0292] (有向图生成部分 110)

[0293] 有向图生成部分 110 在由连续的有向边形成的有向路径之中，确定具有形成有向路径的最大数量的有向边的最长有向路径。确定最长有向路径的处理可以由最长有向路径确定部分来执行，例如所述最长有向路径确定部分可以包括在有向图生成部分 110 中。进一步，有向图生成部分 110 以每个有向路径的有向边的数量不超过最长有向路径的有向边的数量的方式，以更短的有向边来替换形成每个有向路径的有向边，由此生成有向图。

[0294] 如上所述，有向图生成部分 110 以更短的有向边来替换组成临时有向图 I’的有向边，由此构建临时有向图 I’并生成期望的有向图 I。在下文中详细描述与由有向图生成部

分 110 执行的临时有向图 I’的重建有关的技术构思和处理流程。

[0295] 首先，参照图 9 描述与有向图生成部分 110 的处理有关的基本概念。图 9 是示意性地示出了有向图生成部分 110 的处理的说明图。

[0296] 参照图 9，绘出了两个有向图 Q’(A → G) 和 Q(A → G)（其为了说明的目的而创建）。有向图 Q’(A → G) 与基本方案对应，而有向图 Q(A → G) 与本实施例对应。进一步，除了每个有向图之外还绘出了多条垂直线，并且将标记 A 到 G 中的任意一个分配给每一条垂直线。标记 A 到 G 分别表示用户的终端单元。在基本方案的以上描述中，通过将标记 1 到 n 分配给用户来给出说明，并且它们与其对应。因此，从左侧将子集 [A,A]、[A,B]、.....、[A,G] 分配给每个 坐标轴的坐标点。进一步，在每个坐标点下，描述要由与每一条垂直线对应的用户保存的中间密钥的数量。

[0297] 作为基本方案的描述中提到的事项的回顾，首先简要描述有向图 Q’(A → G)。有向图 Q’(A → G) 由具有长度 1 的四条有向边($A\Rightarrow B, B\Rightarrow C, D\Rightarrow E, F\Rightarrow G$)、具有长度 2 的一条有向边$(B\Rightarrow D)$以及具有长度 4 的一条有向边$(B\Rightarrow F)$组成。考虑从坐标点 [A,A] 到坐标点 [A,G] 的有向路径 P([A,A],[A,G])，有向路径 P([A,A],[A,G]) 通过由具有长度 1 的有向边$(A\Rightarrow B)$、具有长度 4 的有向边 $(B\Rightarrow F)$以及具有长度 1 的有向边$(F\Rightarrow G)$组成的有向边链表示。

[0298] 因此，具有中间密钥 t([A, A]) 的用户 A(1) 通过向 PRSG 输入中间密钥 t([A, A]) 可以导出中间密钥 t([A,B])，(2) 通过向 PRSG 输入中间密钥 t([A,B]) 可以导出中间密钥 t([A,C])、t([A,D]) 和 t([A,F])，以及 (3) 通过向 PRSG 输入中间密钥 t([A,F]) 可以导出中间密钥 t([A, G])。由此，对于用户 A 来说必须执行 PRSG 与形成有向路径 P([A, A], [A, G]) 的有向边的数量相同的次数，以便导出与有向路径 P([A,A],[A,G]) 的终点对应的中间密钥 t([A,G])。这是确定用户的计算量的次数。在有向图 Q’(A → G) 的情况下，由于有向路径 P([A,A],[A,G]) 和有向路径 P([A,A],[A,E]) 具有最小数量的有向边，因此那些有向路径的长度与用户的计算量的最差值对应。

[0299] 另一方面，每个用户应该能够生成与用户所属的子集对应的所有中间密钥。由于该原因，要由用户预先保存的中间密钥应该是这样的：要通过重复使用 PRSG 生成的多个中间密钥包括与其所属子集对应的全部中间密钥。进一步，应该选择要由每个用户保存的中间密钥，以便最小化其数量。由此，用户通过参照有向图，从与用户所属的子集对应的坐标点中选择坐标点，以便与到达所述坐标点的有向边的尾部对应的子集不包括所述用户，并保存与所述坐标点对应的中间密钥。

[0300] 例如，通过参照有向图 Q’(A → G) 来考虑要由用户 C 保存的中间密钥。用户 C 所属的子集是 [A, C]、[A, D]、.....、[A, G]。将注意力集中在有向图 Q’(A → G)，达到子集 [A, C]、[A, D]、[A, F] 的有向边的尾部全部是坐标点 [A, B]，其不包括用户 C。由此，用户 C 需要保存中间密钥 t([A,C])、t([A,D]) 和 t([A,F])。实际上，要由每个用户保存的中间密钥的数量由与每个用户对应的垂直线与有向图之间的交叉点的数量表示。例如，由于交叉点的数量为 2，因此用户 D 需要保存两个中间密钥。通过以上方法，在每个有向图下，计算并描述要由 每个用户保存的中间密钥的数量。

[0301] 以上说明仅简要描述了有向图的意义。基于以上说明，在下文中描述本实施例的基本概念。如已经提到的那样，本实施例旨在减少密钥的数量而不增加计算量。考虑到此

情况，在下文中描述所采取的用以减少密钥数量的方法。

[0302] 现在重新参照图 9。如果采用基于有向图 Q'(A → G) 的密钥分发方案，则存在具有最多三个密钥的用户 C。进一步，要由所有用户保存的密钥的数量是 11。然后，将有向图 Q'(A → G) 改变到 Q(A → G)。具体地说，以从坐标点 [A,D] 延伸到 [A,F] 的有向边 E([A,D],[A,F]) 替换从坐标点 [A,B] 延伸到 [A,F] 的有向边 E([A,B],[A,F])。如果进行了这样的改变，则要由每个用户保存的密钥数量的最大值是 2，其与用户 C 和用户 E 对应。进一步，要由所有用户保存的密钥的数量是 9。由此，在改变之前和之后密钥的数量减少。然而，在该改变的示例中，没有考虑计算量。因此，有向图 Q(A → G) 在从坐标点 [A,A] 到 [A,G] 有向路径 P([A,A],[A,G]) 中包括四条有向边，并且与有向图 Q'(A → G) 相比计算量的最差值略有增加。

[0303] 据此，本实施例提供了在不进行导致超出计算量的最差值的有向图改变的条件下，基于图 9 所示的基本概念能够减少密钥数量的有向图生成部分 110 的配置。参照图 10 到图 14，在下文中具体描述通过有向图生成部分 110 生成有向图 I 的方法。

[0304] 首先参照图 10，简要地描述通过有向图生成部分 110 的有向图生成方法的概要。图 10 是示出了生成有向图的处理流程的示例的流程图。

[0305] 首先，有向图生成部分 110 使用由临时有向图生成部分 108 生成的临时有向图 I'，以便生成期望的有向图 I。如之前所述的那样，临时有向图 I' 是以与通过基本方案的有向图 H 相同的方式而生成的。执行通过临时有向图生成部分 108 的临时有向图 I' 的生成作为第一步骤 (S140)。

[0306] 然后，有向图生成部分 110 从组成所有生成的临时有向图 I' 的有向路径提取最长有向路径 LP(Longest Path，最长路径)(S142)。例如，可以由包括在有向图生成部分 110 中的最长有向路径生成部分来执行提取有向路径 LP 的步骤。进一步，从不包括最长有向路径 LP 的所有生成的临时有向图 I' 的每个中提取最长有向路径 PLP(Partially Longest Path，部分最长路径)(S144)。由此，从临时有向图 I' 中提取有向路径 PLP。此后，从组成临时 有向图 I' 的有向边中选择给定有向边，并以更短的有向边来替换它 (S146)。此时，有向图生成部分 110 在不增大计算量的最差值的上述条件下，基于提取的有向路径 LP 和有向路径 PLP 的长度执行有向边的替换。进一步，例如，可以由有向图生成部分 110 中包括的有向边替换部分来执行上述有向边替换步骤。

[0307] 在上文中描述了由有向图生成部分 110 进行的有向图生成步骤的概要。如上所述，有向图生成部分 110 从由临时有向图生成部分 108 生成的临时有向图 I' 中提取有向路径 LP 和有向路径 PLP，然后基于那些有向路径的长度选择并替换给定有向边，由此生成期望的有向图。在下文中给出与上述每个步骤对应的更详细的说明。

[0308] 首先参照图 11，描述临时有向图 I' 的生成步骤。注意，在下文中仅描述临时有向图 I' 之中与中间节点 v 对应的有向图 I'(lv → rv-1)。首先，临时有向图生成部分 108 设置给定整数 k，定义 Lv = rv-lv+1，并计算满足 $n^{(x-1)/k} < Lv \leq n^{x/k}$ 的整数 x(S150)。临时有向图生成部分 108 通过将计数 i 从 0 改变到 x-1 来执行下面的操作。从水平坐标轴的左端的起点开始，重复延伸到远离所述坐标点 $n^{i/k}$ 的坐标点的右向有向边的设置 (跳跃到远离所述坐标点 $n^{i/k}$ 的坐标点)，直到有向边的头部达到水平坐标轴的右端的终点或者下一个要设置的有向边的头部超过终点为止 (S152)。然后，临时有向图生成部分 108 消除其尾部

或头部位于临时坐标点的所有有向边 (S154)。进一步，临时有向图生成部分 108 在达到坐标轴上的各个坐标点的有向边之中，消除除了最长有向边之外的有向边 (S156)。

[0309] 接着参照图 12，在下文中描述提取最长有向路径 LP(S160) 的步骤。在描述最长有向路径 LP 之前，定义两个表达式如下。

[0310] -DDT :表示最长有向路径 LP 的长度。

[0311] -J(a,b) :表示存在于某个有向路径中的具有长度 b 的、数量为 a 的连续有向边。

[0312] (例如，采用图 9 所示的有向图 Q' (A → G) 作为示例，由于有向路径 P([A,A],[A,G])) 由具有长度 1 的一条有向边、具有长度 4 的一条有向边和具有长度 1 的一条有向边组成，因此将其表示为 J(1,1)、J(1,4)、J(1,1))。

[0313] 有向图生成部分 110 可以对于组成临时有向图 I' 的每一条有向路径计算 J(a,b)。例如，考虑从临时有向图 I' (1 → n) 的坐标点 [1,1] 延伸到 [1,n] 的有向路径 P([1,1],[1,n])，将有向路径 P([1,1],[1,n]) 表示为 $J(n^{1/k}-1,1)$，$J(n^{1/k}-1,n^{1/k})$，...，$J(n^{1/k}-1,n^{(k-2)/k})$，$J(n^{1/k}-2,n^{(k-1)/k})$，$J(n^{1/k}-1,n^{(k-2)/k})$，...，$J(n^{1/k}-1,n^{1/k})$，$J(n^{1/k},1)$。在由上述临时有向图生成部分 108 生成的临时有向图 I' 的情况下，最长有向路径 LP 是组成临时有向图 I' (1 → n) 的有向路径 P([1,1],[1,n])。有向图生成部分 110 可以提取最长有向路径 LP 或唯一地提取组成临时有向图 I' (1 → n) 的有向路径 P([1,1],[1,n])，并且在一些情况下，有向图生成部分 110 可以计算组成临时有向图 I' 的所有有向路径的长度，并从它们之中选择最长有向路径 LP。此时，将最长有向路径 LP 的长度 DDT 表示为 $DDT = (2k-1)*(n^{1/k}-1)$。此后，有向图生成部分 110 向形成最长有向路径 LP 的所有有向边设置表示有效的激活标记 (active mark)。

[0314] 接着，参照图 13，描述计算与根节点和各个中间节点对应的每个临时有向图 I' 的最长有向路径 PLP(除了包括最长有向路径 LP 的图) 的步骤。图 13 是示出了有向路径 PLP 的计算步骤的流程图。

[0315] 在对于每个有向图提取最长有向路径 PLP 的步骤的描述之前，定义如下两个表达式。

[0316] -CP(Current Path) :所考虑的有向路径 (将其称为当前路径)

[0317] -#JP(CP) :在有向路径中包括的有向边的数量。

[0318] 有向图生成部分 110 基于下述算法提取有向路径 PLP。

[0319] (步骤 1) 有向图生成部分 110 确定从有向图 I' 的起点到终点的当前路径 CP。如果所考虑的有向图是有向图 I' (a → b)，则将有向路径 P([a,a],[a,b]) 设置为当前路径 CP，而如果是有向图 I' (a ← b)，则将有向路径 P([b,b],[a,b]) 设置为当前路径 CP(S162)。

[0320] (步骤 2) 有向图生成部分 110 在形成当前路径 CP 的有向边之中提取最长有向边，并将其长度设置为 J(S164)。

[0321] (步骤 3) 有向图生成部分 110 判定 J ≤ 1 是否成立 (S 166)，并且如果 J ≤ 1，则将当前路径 CP 确定为有向路径 PLP，并向形成有向路径 PLP 的所有有向边设置激活标记 (S176)。

[0322] (步骤 4) 如果 J > 1，则有向图生成部分 110 判定 $\#JP(CP)+n^{1/k}-1 \leq DDT$ 是否成立 (S 168)，并且如果 $\#JP(CP)+n^{1/k}-1 \leq DDT$ 不成立，则将当前路径 CP 确定为有向路径 PLP，并向形成有向路径 PLP 的所有有向边设置激活标记 (S176)。

[0323] （步骤 5）如果 #JP(CP)+$n^{1/k}$-1 ≤ DDT，则有向图生成部分 110 计算满足 J = $n^{j/k}$ 的自然数 j(S170)。

[0324] （步骤 6）有向图生成部分 110 在具有形成当前路径 CP 的长度为 J 的有向边之中，提取距离当前路径 CP 的起点最远的有向边 (S172)。

[0325] （步骤 7）有向图生成部分 110 紧接在从（步骤 6）中提取的有向边的尾部延伸的、具有长度 $n^{(j-1)/k}$ 的数量为 $n^{1/k-1}$ 的有向边之后，添加具有长度 $n^{(j-1)/k}$ 的一条有向边，并移除在（步骤 6）中提取的有向边 (S174)。此后，进行到（步骤 1）并重复以上步骤。

[0326] 如果执行有向边的进一步替换，则当从有向图 I’的起点到终点的有向路径由全部具有长度 1 的有向边组成时，或者当形成有向路径的有向边的数量超过 DDT 时，在上述（步骤 1）到（步骤 6）中出现的处理的循环结束。通过以上处理，可以对于每个有向图设置最长有向路径 PLP。

[0327] 然后参照图 14，在下文中描述替换给定有向边的步骤。在该步骤中，在形成有向路径的有向边的数量不超过 DDT 的条件下，对于每个有向图构建用以以更短的有向边替换给定有向边的处理的算法。

[0328] 有向图生成部分 110 基于以下算法替换有向边。

[0329] （步骤 1）有向图生成部分 110 在组成有向图 I’的有向边之中，提取被设置为激活、还没有被处理（没有设置完成）且最长的有向边。进一步，有向图生成部分 110 将所提取的有向边的长度设置为 J’。如果存在具有长度 J’的多条有向边，则有向图生成部分 110 选择距离有向图 I’的起点最远的有向边 (S180)。将所选择的有向边称为 WJ(Working Jump，工作跳跃），将有向边 WJ 的起点称为 WJS，并且将终点称为 WJE。进一步，将形成从有向图 I’的起点到达 WJS 的有向路径的有向边的数量表示为 D。

[0330] （步骤 2）有向图生成部分 110 判定有向边 WJ 的长度 J’是否为 J’≤ 1(S182)，如果 J’≤ 1，则将仅由被设置为激活的有向边组成的有向图设置为期望的有向图 I(S202)。如果 J’ > 1，则进行到（步骤 3）。

[0331] （步骤 3）如果有向边 WJ 的长度 J’为 J’ > 1，则有向图生成部分 110 将从 WJS 到达 (WJE-1) 的有向路径设置为当前路径 CP(S184)。(WJE-1) 是紧接在 WJE 之前的坐标点。

[0332] （步骤 4）有向图生成部分 110 在形成当前路径 CP 的有向边之中提取最长有向边，并将其长度设置为 J(S186)。

[0333] （步骤 5）有向图生成部分 110 判定所提取的有向边的长度 J 是否为 J ≤ 1(S188)，并且如果 J ≤ 1，则向形成当前路径 CP 的所有有向边设置激活 (S198) 并向有向边 WJ 设置完成 (done)(S200)。此后，再次从（步骤 1）的处理开始。如果 J > 1，则进行到（步骤 6）。

[0334] （步骤 6）如果 J > 1，则有向图生成部分 110 判定 #JP(CP)+$n^{1/k}$-1 ≤ DDT-D 是否成立 (S190)，并且如果 #JP(CP)+$n^{1/k}$-1 > DDT-D，则向形成当前路径 CP 的所有有向边设置激活 (S198)，并向有向边 WJ 设置完成 (S200)。此后，再次开始从（步骤 1）的处理。如果 #JP(CP)+$n^{1/k}$-1 ≤ DDT-D，则进行到（步骤 7）。

[0335] （步骤 7）如果 #JP(CP)+$n^{1/k}$-1 ≤ DDT-D，则有向图生成部分 110 计算满足 J = $n^{j/k}$ 的自然数 j(S192)。

[0336] （步骤 8）有向图生成部分 110 在形成当前路径 CP 的具有长度 J 的有向边之中，提取距离当前路径 CP 的起点最远的有向边 (S194)。

[0337] （步骤9）有向图生成部分110紧接在从（步骤8）中提取的有向边的尾部延伸的、具有长度$n^{(j-1)/k}$的数量为$n^{1/k-1}$的有向边之后，添加具有长度$n^{(j-1)/k}$的一条有向边，并移除在（步骤8）中提取的有向边（S196）。此后，进行到（步骤3）并重复以上步骤。

[0338] 如果执行有向边的进一步替换，则当从WJS到WJE-1的有向路径由全部具有长度1的有向边组成时，或者当形成从WJS到WJE-1的有向路径的有向边的数量超过DDT时，在上述（步骤3）到（步骤9）中出现的处理的循环结束。另一方面，当没有对组成有向图I'的任意有向边设置完成，并且不存在具有长度2或更长的有向边时，在上述（步骤1）到（步骤5）或（步骤6）中出现的处理的循环结束。通过以上处理，可以生成期望的有向图I。

[0339] 最后，示出了通过使用上述有向图生成方法而生成的有向图I的示例。图15示出了在基于具有叶节点数n＝64的完全二叉树（如图3所示）设置参数k＝6的情况下的有向图I。

[0340] 首先，将基于基本方案生成的有向图H（图4）与根据本实施例的有向图I（图15）进行比较，如下两点是显而易见的。(1)与有向图H相比，在有向图I中，具有长度2或更长的有向边的数量减少，并且从一个坐标点延伸的有向边的数量减少。(2)组成有向图I的任意有向路径不超过有向图H的最长有向路径LP(P[1,1]，[1,64])的长度。由此，确认生成了能够在不增加生 成集合密钥所需的计算量的最差值的情况下减少要由用户保存的中间密钥的数量的有向图I。

[0341] 同样地，关于设置参数k＝3的情况进行比较。在基于基本方案的密钥分发方案中，要分发到每个用户的中间密钥的数量是O(k*log(n))，并且随着参数k减小，要由每个用户保存的密钥的数量也减少。然而，存在如下问题：参数k的减小引起了计算量的增加。考虑到该问题，具体地进行当参数k减小时的效果的研究。图16示出了基于基本方案生成的有向图H，而图17示出了根据本实施例的有向图I。

[0342] 将通过使用相同的基本方案生成的有向图H（图4：k＝6，图16：k＝3）进行比较，在具有k＝3的有向图H中，具有长度2或更长的有向边的数量减少，并且从一个坐标点延伸的有向边的数量减少。然而，在k＝3的情况下，形成有向图H的最长有向路径LP([1,1],[1,64])的有向边的数量是15，其大于k＝6的情况下的有向边的数量（有向边的数量＝11）。然后，关于k＝3的相同情况将根据基本方案的有向图H（图16）与根据本实施例的有向图I（图17）进行比较，尽管形成最长有向路径LP的有向边的数量是15（其是相同的），但是有向图I中具有长度2或更长的有向边的数量更少。由此确认，不论参数k如何都可以获得本实施例的效果。

[0343] 为了更加量化地理解根据本实施例减少密钥数量的效果，在图18中的表格中示出了在基本方案（由现有方案表示）与本实施例之间的比较结果。参照图18，在k＝6的情况下，对所有用户减少要保存的密钥数量。当然，这对于密钥总数和密钥平均数是相同的。进一步，将基本方案(k＝3)和本实施例的方案(k＝6)进行比较，要由每个用户保存的密钥数量几乎相同。比较示出了通过应用本实施例可以减少计算量而又同时保持几乎相同的密钥数量的效果。尽管由于在用户数量n只有n＝64那么小的实现中获得以上结果，因此要减少的密钥数量的绝对值似乎不大，但是由于用户数量的量级相差悬殊，因此在实现环境中减少的效果是非常明显的。

[0344] 在上文中描述了能够在不增大生成集合密钥所需的计算量的最差值的情况下，减

少要由用户保存的中间密钥的数量的有向图的生成逻辑。上述密钥生成逻辑（有向图）的构造主要由组成密钥分发服务器 102 的密钥生成逻辑构建块执行。然而，为了基于以上密钥生成逻辑来执行加密密钥分发，其他元件是必需的。由此，重新参照图 8 在下文中描述其他元件。

[0345] 重新参照图 8，除了上述密钥生成逻辑构建块之外，密钥分发服务器 102 还包括初始中间密钥设置部分 112、密钥生成部分 114、加密部分 116、传送部分 118 和子集确定部分 120。

[0346] （初始中间密钥设置部分 112）

[0347] 初始中间密钥设置部分 112 对于与树的每个中间节点对应的每个有向图 I，生成与有向图 I 的初始坐标点对应的中间密钥。例如，初始中间密钥设置部分 112 可以使用伪随机数发生器来生成随机数，并将随机数设置为与以上初始坐标点（根）对应的每个中间密钥，或者可以将给定数值设置为每个中间密钥。

[0348] （密钥生成部分 114）

[0349] 对于组成有向图 I 的某个有向边，当输入分配给由有向边的尾部指示的坐标点的给定中间密钥时，密钥生成部分 114 输出与由有向边的尾部表示的坐标点对应的集合密钥以及与从有向边的尾部延伸的所有有向边的头部对应的中间密钥。由此，密钥生成部分 114 与基本方案的 PRSG 对应。然而，密钥生成部分 114 与基本方案的 PRSG 的不同在于：它基于由有向图生成部分 110 生成的有向图 I 输出中间密钥。如果将密钥生成部分 114 表示为与 PRSG 相同，则当输入与有向图 I 的某个坐标点 S0 对应的中间密钥 t(S0) 时，输出与其尾部位于所述坐标点的有向边的头部对应的中间密钥 t(S1)、t(S2)、.....、t(Sm)（与子集 S0 对应）以及集合密钥 k(S0)。注意，m 表示其尾部位于某个坐标点 S0 的有向边的数量。

[0350] （传送部分 118）

[0351] 传送部分 118 将由加密部分 116 加密的内容密钥（将在后面描述）传送到与叶节点对应的所有用户。传送部分 118 通过参照上述有向图 I 向每个用户分发中间密钥。此时，传送部分 118 可以以每个用户可以导出与其所属的子集对应所有中间密钥的方式分发最小所需数量的中间密钥。具体地说，传送部分 118 可以从组成集合系统 Φ（参照以上表达式 (1)）的子集中提取中间密钥的分发目的地用户所属的子集，从与所提取的子集对应的有向图 I 的坐标点中选择一个坐标点，以便在与达到所述坐标点的有向边的尾部对应的子集中不包括分发目的地用户，并仅将与所选择的坐标点对应的中间密钥分发至分发目的地用户。然而，如果中间密钥的分发目的地用户所属的子集与有向图 I 的初始坐标点对应，则传送部分 118 可以仅将与初始坐标点对应的 中间密钥分发至分发目的地用户。进一步，传送部分 118 可以用作向每个用户分发有向图 I 的信息的有向图信息分发部分。具体地说，当输入每个中间密钥时，传送部分 118 可以分发与基于有向图 I 输出给定中间密钥和集合密钥的 PRSG 的密钥生成算法（如密钥生成程序）有关的信息。

[0352] 通过使用不同于用于内容分发的信道的通信信道，可以在内容的分发之前执行中间密钥的分发。例如，在终端单元的制造工厂中制造终端时，可以从密钥分发服务器 102 输出每个终端的中间密钥，并将其记录在记录媒体上，并且可以将从记录媒体中读取的每个终端单元的中间密钥存储到对应的终端单元中。

[0353] （加密部分 116）

[0354] 加密部分 116 通过使用集合密钥加密内容密钥。尽管内容密钥的数量是 1，但是存在与组成集合系统 Φ 的子集数量相同的集合密钥的数量。在组成集合系统 Φ 的所有子集之中，加密部分 116 通过使用与由子集确定部分 120 选择的子集对应的每个集合密钥，来加密内容密钥（将在后面描述）。由此，加密部分 116 生成与各个集合密钥对应的经加密的内容密钥。因此，如果所选择的子集的数量是 m，则生成 m 个经加密的内容密钥。可替代地，加密部分 116 可以加密内容。例如，加密部分 116 可以使用内容密钥来加密内容或者可以使用上述各个集合密钥来加密内容。然而，使用集合密钥来加密内容的配置是本实施例的可替代的示例。

[0355] （子集确定部分 120）

[0356] 子集确定部分 120 确定应该对其禁止内容或内容密钥的解密的排除用户的集合 (R)，并通过使用从与有向图 I 的坐标点对应的子集中选择的给定子集的并集，从所有用户的集合 (N) 中消除排除用户的集合 (R)，来定义许可用户的集合 (N\R)，然后以组成许可用户的集合 (N\R) 的子集数量最小的方式确定组成许可用户的集合 (N\R) 的一组子集。子集确定部分 120 可以由如下部分组成：许可用户集合确定部分，用于确定许可用户的集合 (N\R)；以及许可用户子集确定部分，用于确定组成许可用户的集合 (N\R) 的一组子集。

[0357] 在以上述方式由子集确定部分 120 确定组成许可用户的集合的子集 (S1、S2、.....、Sm) 之后，传送部分 118 向每个用户分发许可用户的集合 (N\R) 或组成许可用户的集合 (N\R) 的子集 (S1、S2、.....、Sm)。进一步，加密部分 116 使用与由子集确定部分 120 确定的子集 (S1、S2、.....、Sm) 对应的集合密钥，来加密内容或内容密钥，并且传送部分 118 将经加密的内容或内容密钥分发至每个用户。

[0358] 在上文中描述了根据本发明的优选实施例的密钥分发服务器 102 的配置。如上所述，本实施例的特征主要是密钥生成逻辑构建块的配置。特别地，本实施例具有在用于生成确定密钥生成逻辑的有向图的有向图生成部分 110 的配置方面的特征。根据本实施例的有向图生成部分 110 可以生成能够在不增加对于每个用户来说用以生成集合密钥所需的计算量的情况下，减少要由每个用户保存的中间密钥的数量。结果，可以节省每个用户的终端单元用以保存中间密钥所需的存储器容量，并且还可以降低向每个用户的终端单元分发中间密钥的分发成本。

[0359] [终端单元 122 的配置]

[0360] 参照图 8，在下文中描述根据本实施例的终端单元 122 的配置。

[0361] 参照图 8，终端单元 122 包括接收部分 124、判定部分 126、密钥生成部分 128 和解密部分 130。

[0362] （接收部分 124）

[0363] 接收部分 124 接收从密钥分发服务器 102 中包括的传送部分 118 传送的信息。例如，接收部分 124 从密钥分发服务器 102 接收所分发的内容、经加密的内容密钥、给定中间密钥、与有向图 I 相关的信息、与许可用户相关的信息等。进一步，接收部分 124 可以从多个信息源收集信息，而不是仅从单一信息源接收信息。例如，接收部分 124 可以从多个通过有线或无线网络连接的信息源（如密钥分发服务器 102）或者在不通过网络的情况下直接或间接连接的信息源（如诸如光盘单元、磁盘单元和便携式终端单元之类的信息媒体）获取信息。由于接收部分 124 当然可以从另一终端单元 122 接收信息，因此可以将其进行配

置以便与例如属于相同分发目的地组的另一终端单元 122 共享有向图 I 的信息。在这种情况下，相同分发目的地组意味着授权为从相同或多个密钥分发服务器 102 分发的内容的查看用户 (viewer user) 的组，这与上述树结构的叶节点对应的用户的集合对应。进一步，可以预先向终端单元提供上述中间密钥，并将其存储在终端单元中。

[0364] （判定部分 126）

[0365] 判定部分 126 判定它是否作为与用于加密的集合密钥对应的任意子集中 的元素而包括。由于终端单元 122 仅保存用于生成与其所属的子集对应的集合密钥的中间密钥，因此必须基于与由密钥分发服务器 102 使用的、用以加密内容或内容密钥的集合密钥有关的信息，预先判定其所属的子集是否包括在与集合密钥对应的子集中。这样的判定由判定部分 126 进行。以与内容密钥相同的定时或不同的定时，从密钥分发服务器 102 分发与用于加密的集合密钥有关的信息，并由接收部分 124 接收所述信息。如果判定与其所属的子集对应的集合密钥不包括在用于加密的集合密钥中，则终端单元 122 结束内容密钥的处理，而不执行使用其自身保存的中间密钥来生成集合密钥的处理。相反，如果发现了与其所属的子集对应的集合密钥，则终端单元 122 通过利用 PRSG，使用其自身保存的中间密钥来生成集合密钥。

[0366] （密钥生成部分 128）

[0367] 对于组成有向图 I 的某个有向边，当输入分配给由有向边的尾部所表示的坐标点的给定中间密钥时，密钥生成部分 128 输出与由有向边的尾部所表示的坐标点对应的集合密钥以及与从有向边的尾部延伸的所有有向边的头部对应的中间密钥。由此，密钥生成部分 128 与密钥分发服务器 102 中包括的密钥生成部分 114 对应。如果将密钥生成部分 128 表示为 PRSG，如果输入与有向图 I 的某个坐标点 S0 对应的中间密钥 t(S0)，则输出与其尾部位于坐标点 S0 的有向边的头部对应的中间密钥 t(S1)、t(S2)、.....、t(Sm) 以及集合密钥 k(S0)。注意，m 表示其尾部位于某个坐标点 S0 的有向边的数量。可以从密钥分发服务器 102 获取有向图 I 的信息，或者将其存储在终端单元 122 中包括的存储部分（未示出）中。

[0368] （解密部分 130）

[0369] 解密部分 130 使用集合密钥来解密内容密钥。具体地说，解密部分 130 从与集合密钥对应的子集中提取将它作为元素包括的子集，并使用与所述子集对应的集合密钥来解密内容或内容密钥。

[0370] 在上文中描述了根据本实施例的终端单元 122 的配置。如上所述，终端单元 122 可以基于由上述密钥分发服务器 102 中包括的有向图生成部分 110 生成的特殊的密钥生成逻辑（有向图 I）来生成期望的集合密钥。结果，对于终端单元 122 来说，可以减少生成用以解密内容密钥的集合密钥所需保存的中间密钥的数量。

[0371] 〈第二实施例〉

[0372] 接着，描述根据本发明的第二实施例的加密密钥分发方案。根据本实施例的加密密钥分发方案通过生成由更长的有向边组成的临时有向图，然后以更短的有向边来替换组成临时有向图的有向边以由此重建有向图，能够减少对于终端单元 122 来说、用以生成集合密钥所需的计算量，同时减少要由终端单元 122 保存的中间密钥的数量。在下文中，详细描述执行根据本实施例的加密密钥分发方案的密钥分发服务器 152 的功能性配置、加密密

钥分发方案的特征和优点。与上述第一实施例的主要区别在于密钥分发服务器 152 的功能性配置。由此，由相同的符号表示与上述第一实施例中的组件基本上相同的组件，并省略冗余说明。

[0373] [密钥分发服务器 152 的配置]

[0374] 参照图 19，在下文中详细描述根据本实施例的密钥分发服务器 152 的配置。图 19 是示出了根据本实施例的密钥分发服务器 152 和终端单元 122 的配置的框图。

[0375] 如图 19 所示，密钥分发服务器 152 由树结构设置部分 154、坐标轴设置部分 156、临时有向图生成部分 158、有向图生成部分 160、初始中间密钥设置部分 162、密钥生成部分 164、加密部分 166、传送部分 168 和子集确定部分 170 组成。特别地，将树结构设置部分 154、坐标轴设置部分 156、临时有向图生成部分 158 和有向图生成部分 160 统称为密钥生成逻辑构建块。同样地，将初始中间密钥设置部分 162 和密钥生成部分 164 统称为密钥生成块。

[0376] 在下文中描述组成密钥生成逻辑构建块的元件。密钥生成逻辑构建块执行与上述 [基本技术描述] 中的（树结构的设置）和（有向图的生成）对应的处理。

[0377] （树结构设置部分 154）

[0378] 树结构设置部分 154 配置由向其分配了编号 1 到 n(n 是自然数）的 n 个叶节点、根节点和多个除了根节点和叶节点之外的中间节点组成的二叉树，并在位于某个中间节点 v 或根节点 v 的下层的多个叶节点之中，将位于左端的叶节点的编号设置为 lv，将位于右端的叶节点的编号设置为 rv。进一步，树结构设置部分 154 将集合 (1 → n) 和集合 (2 ← n) 分配给根节点，并且如果某个中间节点 v 位于其父节点的左侧，则将集合 (lv+1 ← rv) 分配给中间节点，如果中间节点 v 位于其父节点的右侧，则将集合 (lv → rv-1) 分配给中间节点。

[0379] 如上所述，树结构设置部分 154 具有能够构造 m 层树结构并且假设 m ＝ 2 （二叉树）的情况的配置，例如，可以构造与根据基本方案的二叉树结构（图 3）相同的树结构。由此，由树结构设置部分 154 构造的树结构的每个节点的意义与根据之前所述的基本方案构建的二叉树结构的每个节点的意义基本上相同。尽管为了描述的方便起见，在下文中仅描述二叉树结构，但是其不限于此。

[0380] （坐标轴设置部分 156）

[0381] 坐标轴设置部分 156 设置第一水平坐标轴，其上与集合 (1 → n) 中包括的各个子集相关的坐标点以包含度向右变大的方式排列。接着，坐标轴设置部分 156 设置第二水平坐标轴，其上与集合 (2 ← n) 中包括的各个子集相关的坐标点以包含度向左变大的方式排列。然后，对于每个中间节点 v，坐标轴设置部分 156 设置第三水平坐标轴，其上与集合 (lv → rv-1) 中包括的各个子集相关的坐标点以包含度向右变大的方式排列。进一步，对于每个中间节点 v，坐标轴设置部分 156 设置第四水平坐标轴，其上与集合 (lv+1 ← rv) 中包括的各个子集相关的坐标点在所述水平坐标轴上以包含度向左变大的方式排列。此后，坐标轴设置部分 156 将两个临时坐标点均放置在位于第三水平坐标轴的右端的坐标点的右侧以及位于第二和第四水平坐标轴的左端的坐标点的左侧。进一步，坐标轴设置部分 156 将位于第一水平坐标轴的右端的坐标点设置为第一临时坐标点，并将第二临时坐标点放置在第一临时坐标点右侧。

[0382] 如上所述，坐标轴设置部分 156 设置用于构建与由树结构设置部分 154 配置的树结构的各个节点对应的有向图的坐标轴。第一水平坐标轴表示与集合 (1 → n) 的坐标轴，第二水平坐标轴表示与集合 (2 ← n) 对应的坐标轴，第三水平坐标轴表示与集合 (lv → rv-1) 的坐标轴，而第四水平坐标轴表示与集合 (lv+1 ← rv) 对应的坐标轴。由于对于每个中间节点 v 设置第三水平坐标轴和第四水平坐标轴，因此分别设置多个坐标轴。具体地说，设置与中间节点的数量相同的第三水平坐标轴和第四水平坐标轴的数量。

[0383] (临时有向图生成部分 158)

[0384] 临时有向图生成部分 158 设置给定整数 k，并计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x。接着，对于每个整数 i ＝ 0 到 x-1，临时有向图生成部分 158 通过连接具有长度 $n^{i/k}$ 的一条或多条右向有向边，形成其尾部位于第一和第三坐标轴上的最左侧的坐标点的有向路径，并进一步通过连接具有长度 $n^{i/k}$ 的一条或多条左向有向边，形成其尾部位于第二和第四坐标轴上 的最右侧的坐标点的有向路径。然后，临时有向图生成部分 158 对于第一到第四水平坐标轴中的每个，排除其尾部或头部位于临时坐标点的所有有向边。进一步，临时有向图生成部分 158 从到达第一到第四水平坐标轴上每个坐标点的有向边中，排除除了最长有向边之外的有向边，由此生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 ← rv) 和集合 (lv → rv-1) 有关的临时有向图。此后，临时有向图生成部分 158 将具有长度 1 的有向边 (其头部是位于第一水平坐标轴的右端的坐标点) 添加到与集合 (1 → n-1) 有关的临时有向图，由此生成与集合 (1 → n) 有关的临时有向图。

[0385] 如上所述，临时有向图生成部分 158 通过与基本方案类似的方法生成有向图。然而，与基本方案的有向图相比，临时有向图生成部分 158 可以生成由更长的有向边组成的有向图。这减少了对于每个用户来说、用以导出集合密钥所需的计算量 (如后面所述)。在下文中参照图 20 详细描述由临时有向图生成部分 158 执行的处理的处理流程。图 20 是示出了由临时有向图生成部分 158 进行的有向图生成的处理流程的流程图。

[0386] 参照图 20，临时有向图生成部分 158 通过下述步骤生成有向图。通过例证的方式描述生成与集合 (lv → rv-1) 对应的临时有向图 I’(lv → rv-1) 的方法。

[0387] (步骤 1 ;S240) 临时有向图生成部分 158 通过将集合 (lv → rv-1) 中包括的各个子集以包含度从左至右变大的方式排列，而将其放置在水平直线 (水平坐标轴) 上。准确地说，临时有向图生成部分 158 将作为集合 (lv → rv-1) 的元素的子集分配给水平坐标轴上的各个坐标点，并以所分配的子集的包含度向右变大的方式放置坐标点。然后，临时有向图生成部分 158 将两个临时坐标点放置在位于水平坐标轴上最右侧的坐标点的右侧。从坐标轴上最左侧坐标点到最右侧坐标点的距离 Lv 为 Lv ＝ rv-lv+1。此时，临时有向图生成部分 158 计算满足 $n^{(x-1)/k} < Lv \leqslant n^{x/k}$ 的整数 x(1 ⩽ x ⩽ k)。

[0388] (步骤 2 ;S242) 临时有向图生成部分 158 将整数值 i 设置为计数，并通过从 0 变化到 x-1 的计数 i 执行如下操作。从水平坐标轴的左端处的起点开始，临时有向图生成部分 158 重复延伸到远离所述坐标点 $n^{i/k}$ 的坐标点的右向有向边的设置 (跳跃到远离所述坐标点 $n^{i/k}$ 的坐标点)，直到有向边的头部达到水平坐标轴上其右端或左端的临时坐标点为止或者下一个要设置的有向边的头部超过任意临时坐标点为止。

[0389] (步骤 3 ;S244) 临时有向图生成部分 158 从在 (步骤 2) 中创建的有向 边中删除到达临时坐标点的所有有向边。

[0390] （步骤 4 ;S246) 如果存在到达某个坐标点的多个有向边，则临时有向图生成部分 158 删除除了最长有向边之外的所有有向边。

[0391] 通过以上处理，临时有向图生成部分 158 可以由与基本方案相比更长的有向边组成的有向图。进一步，对于组成树结构的所有中间节点和根节点，临时有向图生成部分 158 通过与以上临时有向图 I’(lv → rv-1) 相同的方法生成有向图。例如，临时有向图生成部分 158 生成与某个中间节点 v 对应的临时有向图 I’(lv → rv-1)，并进一步生成与根节点对应的临时有向图 I’(1 → n) 和 I(2 ← n)。在水平坐标轴上形成临时有向图 I’(lv+1 → rv) 和 I(2 ← n)，在所述水平坐标轴上以每个图中包括的子集的包含度在“向左方向”中变大的方式排列坐标点。由此，颠倒由以上（步骤 1) 设置的水平坐标轴上的坐标点排列规则。进一步，将用于组成临时有向图 I’(lv+1 → rv) 和 I(2 ← n) 的两个临时坐标点放置在位于水平坐标轴上最左侧的坐标点的左侧。通过将有向边 E([1,n-1],[1,n]) 添加到有向图 I(1 → n-1) 来生成有向图 I(1 → n)。

[0392] 通过利用上述有向图生成方法，生成图 21 中所示的临时有向图 I’。图 21 示出了基于如图 3 所示具有叶节点数 n ＝ 64 的完全二叉树，当设置参数 k ＝ 6 时形成的临时有向图 I’。

[0393] （有向图生成部分 160)

[0394] 有向图生成部分 160 在由多条所连接的有向边组成的有向路径之中，确定具有形成有向路径的有向边的最大数量的最长有向路径。然后，有向图生成部分 160 通过以更短的有向边的集合来替换形成每个有向路径的有向边来重建每个有向路径，以便不超过形成最长有向路径的有向边的数量，并生成由重建的有向路径组成的有向图。

[0395] 如上所述，有向图生成部分 160 基于由临时有向图生成部分 158 构建的临时有向图 I’生成期望的有向图 I。具体地说，尽管基本方案仅可以生成基本上与临时有向图 I’基本上相同的有向图 H，但是根据本实施例的密钥分发服务器 152 可以生成表示更有效的集合密钥生成逻辑的有向图 I，这是因为它包括有向图生成部分 160。在下文中详细描述由有向图生成部分 160 执行的处理的处理流程。

[0396] 参照图 22，简要地描述由有向图生成部分 160 进行的有向图生成方法的概要。图 22 是示出了生成有向图的处理流程的示例的流程图。

[0397] 首先，有向图生成部分 160 使用由临时有向图生成部分 158 生成的临时有向图 I’，以便生成期望的有向图 I。

[0398] 然后，有向图生成部分 160 从形成所有生成的临时有向图 I’的有向路径中提取最长有向路径 LP(Longest Path)(S250)。例如，提取有向路径 LP 的步骤可以由有向图生成部分 160 中包括的最长有向路径生成部分来执行。进一步，从不包括最长有向路径 LP 的所有生成的临时有向图 I’的每个中提取最长有向路径 PLP(Partially Longest Path，部分最长路径)(S252)。因此，从每个临时有向图 I’提取有向路径 PLP。此后，从组成临时有向图 I’的有向边中选择给定有向边，并以更短的有向边来替换它 (S254)。此时，有向图生成部分 160 在上述计算量的最差值不增加的条件下，基于所提取的有向路径 LP 和有向路径 PLP 的长度，执行有向边的替换。例如，上述给定有向边选择步骤可以由有向图生成部分 160 中包括的替换有向边选择部分来执行。进一步，例如，上述有向边替换步骤可以由有向图生成部分 160 中包括的有向边替换部分来执行。

[0399] 在上文中描述了由有向图生成部分 160 进行的有向图生成步骤的概要。如上所述，有向图生成部分 160 从由临时有向图生成部分 158 生成的临时有向图 I’中提取有向路径 LP 和有向路径 PLP，然后基于那些有向路径的长度选择并替换给定有向边，由此生成期望的有向图。在下文中给出与上述每个步骤对应的更详细的说明。

[0400] 首先参照图 23，在下文中描述提取最长有向路径 LP(S260) 的步骤。在最长有向路径 LP 的描述之前，定义如下两个表达式。

[0401] -DDT :表示最长有向路径 LP 的长度。

[0402] -J(a，b) :表示在某个有向路径中具有长度 b 的、数量为 a 的连续有向边。

[0403] 有向图生成部分 160 可以对于组成临时有向图 I’的每个有向路径计算 J(a,b)。例如，考虑从临时有向图 I’(1 → n) 的坐标点 [1,1] 到 [1,n] 的有向路径 P([1,1]，[1,n])，将有向路径 P([1,1]，[1,n]) 表示为 $J(n^{1/k}-1, n^{(k-1)/k})$，$J(n^{1/k}-1, n^{(k-2)/k})$，...，$J(n^{1/k}, 1)$。在由上述临时有向图生成部分 158 生成的临时有向图 I’的情况下，有向路径 LP 是组成临时有向图 I’(1 → n) 的有向路径 P([1,1]，[1,n])。有向图生成部分 160 可以提取最长有向路径 LP 或唯一地提取组成临时有向图 I’(1 → n) 的有向路径 P([1,1]，[1,n])，并且在一些情况下，有向图生成部分 160 可以计算组成临时有向图 I’(1 → n) 的所有有向路径的长度，并从其中选择最长 有向路径 LP。此时，将最长有向路径 LP 的长度 DDT 表示为 $DDT = k*(n^{1/k}-1)$。此后，有向图生成部分 160 向形成最长有向路径 LP 的所有有向边设置表示有效的激活标记。

[0404] 接着，参照图 24 描述对于与根节点和各个中间节点的每个临时有向图 I’(除了包括最长有向路径 LP 的图) 计算最长有向路径 PLP 的步骤。图 24 是示出了有向路径 PLP 的计算步骤的流程图。

[0405] 在描述对于每个有向图提取最长有向路径 PLP 的步骤之前，定义如下两个表达式。

[0406] -CP(Current Path) :所考虑的有向路径 (将其称为当前路径)

[0407] -#JP(CP) :有向路径中包括的有向边的数量。

[0408] 有向图生成部分 160 基于下述算法提取有向路径 PLP。

[0409] (步骤 1) 有向图生成部分 160 确定从有向图 I’的起点到终点的当前路径 CP。如果所考虑的有向图是有向图 I’(a → b)，则将有向路径 P([a,a]，[a,b]) 设置为当前路径 CP，而如果是有向图 I’(a ← b)，则将有向路径 P([b,b]，[a,b]) 设置为当前路径 CP(S262)。

[0410] (步骤 2) 有向图生成部分 160 在形成当前路径 CP 的有向边之中提取最长有向边，并将其长度设置为 J(S264)。

[0411] (步骤 3) 有向图生成部分 160 判定 J ≤ 1 是否成立 (S266)，并且如果 J ≤ 1，则将当前路径 CP 确定为有向路径 PLP，并向形成有向路径 PLP 的所有有向边设置激活标记 (S276)。

[0412] (步骤 4) 如果 J > 1，则有向图生成部分 160 判定 $\#JP(CP)+n^{1/k}-1 \leq DDT$ 是否成立 (S168)，并且如果 $\#JP(CP)+n^{1/k}-1 \leq DDT$ 不成立，则将当前路径 CP 确定为有向路径 PLP，并向形成有向路径 PLP 的所有有向边设置激活标记 (S276)。

[0413] (步骤 5) 如果 $\#JP(CP)+n^{1/k}-1 \leq DDT$，则有向图生成部分 160 计算满足 $J = n^{j/k}$ 的自然数 j(S270)。

[0414] （步骤6）有向图生成部分160在具有形成当前路径CP的长度J的有向边之中，提取距离当前路径CP的起点最远的有向边（S272）。

[0415] （步骤7）有向图生成部分160紧接在从（步骤6）中提取的有向边的尾部延伸的、具有长度$n^{(j-1)/k}$的数量为$n^{1/k}-1$的有向边之后，添加具有长度$n^{(j-1)/k}$的一条有向边，并移除在（步骤6）中提取的有向边（S174）。此后，进行 到（步骤1）并重复以上步骤。

[0416] 如果执行有向边的进一步替换，则当从有向图I’的起点到终点的有向路径由全部具有长度1的有向边组成时，或者当形成有向路径的有向边的数量超过DDT时，在上述（步骤1）到（步骤6）中出现的处理的循环结束。通过以上处理，可以对于每个有向图设置最长有向路径PLP。

[0417] 参照图25，在下文中描述替换给定有向边的步骤。在该步骤中，在形成有向路径的有向边的数量不超过DDT的条件下，对于每个有向路径，构建以更短的有向边替换给定有向边的处理的算法。

[0418] 有向图生成部分160基于以下算法替换有向边。

[0419] （步骤1）有向图生成部分160在组成有向图I’的有向边之中，提取被设置为激活、还没有被处理（没有设置完成）且最长的有向边。进一步，有向图生成部分160将所提取的有向边的长度设置为J’。如果存在具有长度J’的多条有向边，则有向图生成部分160选择距离有向图I’的起点最远的有向边（S280）。将所选择的有向边称为WJ(Working Jump)，将有向边WJ的起点称为WJS，并且将终点称为WJE。进一步，将形成从有向图I’的起点到达WJS的有向路径的有向边的数量表示为D。

[0420] （步骤2）有向图生成部分160判定有向边WJ的长度J’是否为J’≤1(S282)，如果J’≤1，则将仅由被设置为激活的有向边组成的有向图设置为期望的有向图I(S302)。如果J’＞1，则进行到（步骤3）。

[0421] （步骤3）如果有向边WJ的长度J’为J’＞1，则有向图生成部分160将从WJS到达(WJE-1)的有向路径设置为当前路径CP(S284)。(WJE-1)是紧接在WJE之前的坐标点。

[0422] （步骤4）有向图生成部分160在形成当前路径CP的有向边之中提取最长有向边，并将其长度设置为J(S286)。

[0423] （步骤5）有向图生成部分160判定所提取的有向边的长度J是否为J≤1(S288)，并且如果J≤1，则向形成当前路径CP的所有有向边设置激活（S298）并向有向边WJ设置完成（S300）。此后，再次从（步骤1）的处理开始。

[0424] （步骤6）如果J＞1，则有向图生成部分160判定$\#JP(CP)+n^{1/k}-1 \leq DDT-D$是否成立（S290），并且如果$\#JP(CP)+n^{1/k}-1 > DDT-D$，则向形成当前路径CP的所有有向边设置激活（S298），并向有向边WJ设置完成（S300）。此后，再次从（步骤1）的处理开始。

[0425] （步骤7）如果$\#JP(CP)+n^{1/k}-1 \leq DDT-D$，则有向图生成部分160计算满足$J = n^{j/k}$的自然数j(S292)。

[0426] （步骤8）有向图生成部分160在形成当前路径CP的具有长度J的有向边之中，提取距离当前路径CP的起点最远的有向边（S294）。

[0427] （步骤9）有向图生成部分160紧接在从（步骤8）中提取的有向边的尾部延伸的、具有长度$n^{(j-1)/k}$的数量为$n^{1/k}-1$的有向边之后，添加具有长度$n^{(j-1)/k}$的一条有向边，并移除在（步骤8）中提取的有向边（S296）。此后，进行到（步骤3）并重复以上步骤。

[0428] 如果执行有向边的进一步替换，则当从WJS到WJE-1的有向路径由全部具有长度1的有向边组成时，或者当形成从WJS到WJE-1的有向路径的有向边的数量超过DDT时，在上述（步骤3）到（步骤9）中出现的处理的循环结束。另一方面，当没有对组成有向图I'的任意有向边设置完成，并且不存在具有长度2或更长的有向边时，在上述（步骤1）到（步骤5）或（步骤6）中出现的处理的循环结束。通过以上处理，可以生成期望的有向图I。

[0429] 最后，示出了使用上述有向图生成方法而生成的有向图I的示例。图26示出了基于具有图3所示的叶节点的数量n＝64的完全二叉树，在设置参数k＝6的情况下的有向图I。

[0430] 首先，将基于基本方案生成的有向图H（图4）与根据本实施例的有向图I（图26）进行比较，如下两点是显而易见的。(1) 与有向图H相比，在有向图I中，具有长度2或更长的有向边的数量减少，并且从一个坐标点延伸的有向边的数量减少。(2) 对于有向图I上的许多有向路径，有向边的数量减少。由此，确认生成了能够减少生成集合密钥所需的计算量的最差值并减少要由用户保存的中间密钥的数量的有向图I。

[0431] 为了更加量化地理解根据本实施例减少密钥数量的效果，在图27中的表格中示出了在基本方案与本实施例之间的比较结果。参照图27，减少要由用户保存的密钥的总和（密钥的总数）以及要由用户保存的密钥的平均数。尽管由于在用户数量n只有n＝64那么小的执行中获得以上结果，因此要减少的密钥数量的绝对值似乎不大，但是由于用户数量相差悬殊，因此期望在执行环境中减小的效果作为非常明显的差别出现。进一步，由形成最长有向路径的有向边的数量表示生成集合密钥所需的计算量的最差值，并且当在基于基本方案生成的有向图H中所述值为 $(2k-1)*(n^{1/k}-1)$ 时，在根据本实施例的有向 图I中减少了一半至 $k*(n^{1/k}-1)$。

[0432] 在上文中描述了生成能够减少生成集合密钥所需的计算量的最差值并减少要由用户保存的中间密钥的数量的有向图的逻辑。上述密钥生成逻辑（有向图）的构造主要由组成密钥分发服务器152的密钥生成逻辑构建块来执行。然而，为了基于以上密钥生成逻辑执行加密密钥分发，其他元件是必需的。由此，重新参照图19，在下文中描述其他元件。

[0433] 重新参照图19，除了上述密钥生成逻辑构建块之外，密钥分发服务器152包括初始中间密钥设置部分162、密钥生成部分164、加密部分166、传送部分168和子集确定部分170。

[0434] （初始中间密钥设置部分162）

[0435] 初始中间密钥设置部分162对于与树的每个中间节点对应的每个有向图I，生成与有向图I的初始坐标点对应的中间密钥。例如，初始中间密钥设置部分162可以使用伪随机数发生器来生成随机数，并将随机数设置为与以上初始坐标点（根）对应的每个中间密钥，或者可以将给定数值设置为每个中间密钥。

[0436] （密钥生成部分164）

[0437] 对于组成有向图I的某个有向边，当输入分配给由有向边的尾部表示的坐标点的给定中间密钥时，密钥生成部分164输出与由有向边的尾部表示的坐标点对应的集合密钥以及与从有向边的尾部延伸的所有有向边的头部对应的中间密钥。由此，密钥生成部分164与基本方案的PRSG对应。然而，密钥生成部分164与基本方案的PRSG的不同在于：它基于由有向图生成部分160生成的有向图I输出中间密钥。如果将密钥生成部分164表示为与

PRSG 相同，则当输入与有向图 I 的某个坐标点 S0 对应的中间密钥 t(S0) 时，输出与其尾部位于所述坐标点的有向边的头部对应的中间密钥 t(S1)、t(S2)、.....、t(Sm)（与子集 S0 对应）以及集合密钥 k(S0)。注意，m 表示其尾部位于某个坐标点 S0 的有向边的数量。

[0438] （加密部分 166）

[0439] 加密部分 166 通过使用集合密钥加密内容密钥。尽管内容密钥的数量是 1，但是存在与组成集合系统 Φ 的子集数量相同的集合密钥的数量。因此，在组成集合系统 Φ 的所有子集之中，加密部分 116 通过使用与由子集确定部分 170 选择的子集对应的每个集合密钥来加密内容密钥（将在后面描述）。 由此，加密部分 166 生成与各个集合密钥对应的经加密的内容密钥。因此，如果所选择的子集的数量是 m，则生成 m 个经加密的内容密钥。可替代地，加密部分 166 可以加密内容。例如，加密部分 166 可以使用内容密钥来加密内容或者可以使用上述各个集合密钥来加密内容。然而，使用集合密钥来加密内容的配置是本实施例的可替代的示例。

[0440] （传送部分 168）

[0441] 传送部分 168 将由加密部分 166 加密的内容密钥传送到与叶节点对应的所有用户。进一步，传送部分 168 通过参照上述有向图 I 可以向每个用户分发中间密钥。此时，传送部分 168 可以以每个用户均可以导出与其所属的子集对应所有中间密钥的方式分发最小所需数量的中间密钥。具体地说，传送部分 168 可以从组成集合系统 Φ（参照以上表达式 (1)）的子集中提取中间密钥的分发目的地用户所属的子集，从与所提取的子集对应的有向图 I 的坐标点中选择一个坐标点，以便在与达到所述坐标点的有向边的尾部对应的子集中不包括分发目的地用户，并仅将与所选择的坐标点对应的中间密钥分发至分发目的地用户。然而，如果中间密钥的分发目的地用户所属的子集与有向图 I 的初始坐标点对应，则传送部分 168 可以仅将与初始坐标点对应的中间密钥分发至分发目的地用户。进一步，传送部分 168 可以用作向每个用户分发有向图 I 的信息的有向图信息分发部分。具体地说，当输入每个中间密钥时，传送部分 168 可以分发与基于有向图 I 输出给定中间密钥和集合密钥的 PRSG 的密钥生成算法（如密钥生成程序）有关的信息。

[0442] 通过使用不同于用于内容分发的信道的通信信道，可以在内容的分发之前执行中间密钥的分发。例如，在终端单元的制造工厂中制造终端时，可以从密钥分发服务器 152 输出每个终端的中间密钥，并将其记录在记录媒体上，并且可以将从记录媒体中读取的每个终端单元的中间密钥存储到对应的终端单元中。

[0443] （子集确定部分 170）

[0444] 子集确定部分 170 确定应该对其禁止内容或内容密钥的解密的排除用户的集合 (R)，并通过使用从与有向图 I 的坐标点对应的子集中选择的给定子集的并集，从所有用户的集合 (N) 中消除排除用户的集合 (R)，来定义许可用户的集合 (N\R)，然后以组成许可用户的集合 (N\R) 的子集数量最小的方式确定组成许可用户的集合 (N\R) 的一组子集。子集确定部分 170 可以由如下部分组成：许可用户集合确定部分，用于确定许可用户的集合 (N\R)；以及许可用户子集确定部分，用于确定组成许可用户的集合 (N\R) 的一组子集。

[0445] 在以上述方式由子集确定部分 170 确定组成许可用户的集合 (N\R = S1 ∪ S2 ∪ ... ∪ Sm；m 是自然数）的子集 (S1、S2、.....、Sm) 之后，传送部分 168 向每个用户分发许可用户的集合 (N\R) 或组成许可用户的集合 (N\R) 的子集 (S1、S2、.....、

Sm)。进一步，加密部分 166 使用与由子集确定部分 170 确定的子集 (S1、S2、.....、Sm) 对应的集合密钥，来加密内容或内容密钥，并且传送部分 168 将经加密的内容或内容密钥分发至每个用户。

[0446] 在上文中描述了根据本发明的优选实施例的密钥分发服务器 152 的配置。如上所述，本实施例的特征主要在于密钥生成逻辑构建块的配置。特别地，本实施例具有在用于生成确定密钥生成逻辑的有向图的有向图生成部分 160 的配置方面的特征。根据本实施例的有向图生成部分 160 可以生成能够在不增加对于每个用户来说用以生成集合密钥所需的计算量的情况下减少要由每个用户保存的中间密钥的数量的密钥生成逻辑（有向图）。结果，可以节省每个用户用以保存中间密钥所需的存储器容量以及用于密钥生成的计算量，并且还可以降低用于向每个用户分发中间密钥的分发成本。

[0447] [加密密钥分发系统 100 的应用]

[0448] 最后，在下文中描述上述加密密钥分发系统 100 的应用。

[0449] (应用 1)

[0450] 首先，作为应用 1，在图 28 中示出了广播加密系统 300 的配置。

[0451] 图 28 是示出了使用广播卫星的广播加密系统的配置的框图。在广播加密系统 300 中，将经加密的数据（即所谓的密文）经由广播信道传送到接收器 310。广播加密系统 300 中的广播信道是卫星广播分发信道。例如，作为密文传送的数据是包含加密密钥、音频数据、视频数据、文本数据等的内容。卫星电视广播设备 302 的广播信托中心 (broadcast trusted center)304 向广播卫星 306 传送数据。例如，广播信托中心 304 选择用于加密的密钥，或者控制数据的加密和数据的分发。广播卫星 306 广播数据。在住宅中安装的接收器 310 包括例如卫星广播接收器，并接收所广播的数据。多个其他接收器 310 也可以接收所广播的数据。以这种方式，广播信托中心 304 可以向由接收器 310 组成的接收器组中的每个接收器 310 传送数据。如后面所述，广播信托中心 304 以仅授权接收器 310 可以解密所广播的数据的方式加密广播数据。尽管图 28 示出了使用广播卫星 306 的广播系统，但是也可以使用其他广播信道，如有线电视和计算机网络。

[0452] 在上文中描述了作为加密密钥分发系统 100 的广播加密系统 300 的配置。简要地总结与加密密钥分发系统 100 的关系，就是广播信托中心 304 与密钥分发服务器 102 对应，而接收器 310 与接收器 122 对应。广播卫星 306 作为连接它们的网络的媒介。

[0453] (应用 2)

[0454] 接着，作为应用 2，在图 29 中示出了广播加密系统 400 的配置。

[0455] 图 29 是示出了使用数据媒体的广播加密系统 400 的配置的框图。在广播加密系统 400 中，广播信道是数据媒体的分发。媒体制造商 402 中的广播信托中心 404 在诸如只读媒体（如 CD-ROM、DVD-ROM 等）和可重写媒体（如 CD-RW、DVD-RW 等）之类的媒体 406 的每一件数据媒体中存储数据。在只读媒体中，广播信托中心 404 记录经加密的内容密钥和经加密的内容，以便仅授权用户可以解密内容并访问经加密的内容（如声音、视频、文本等）。另一方面，在可重写媒体中，广播信托中心 404 记录经加密的内容密钥，以便仅授权的记录单元可以将对应数据记录到记录媒体中。例如，媒体制造商 402 将媒体 406 发送到诸如零售商店之类的分发中间商。分发中间商 408 向住宅 412 中的接收器 414 提供媒体 410。例如，分发中间商 408 向一人销售媒体 410，并且该人将媒体 410 带入住宅 412 中，并将媒体

410 插入接收器 414。例如，接收器 414 可以是读取并回放媒体 410 中存储的数据的单元，如 CD 播放器、DVD 播放器和计算机。作为另一具体示例，接收器 414 可以是能够将数据记录到媒体 410 中并从媒体 410 读取数据的盘单元，如 DVD-RW 驱动器。广播信托中心 404 以仅授权接收器 414 可以解密经加密的数据的方式加密数据。

[0456] 在上文中描述了作为加密密钥分发系统 100 的一个应用的广播加密系统 400 的配置。简单地总结与加密密钥分发系统 100 的关系，就是广播信托中心 404 与密钥分发服务器 102 对应，而接收器 414 与接收器 122 对应。进一步，代替连接它们的网络，分发媒体 406 和 410 的分发中间商 408 作为媒介存在。

[0457] 尽管参照附图描述本发明的优选实施例，但是本发明当然不限于此。对于本领域的技术人员来说显而易见，在不脱离权利要求的范围的情况下可以进行各种改变和修改，并且旨在本发明的技术范围内的包含。

[0458] 例如，假设上述树结构设置部分 104 形成分支从上到下变得更宽的树结构，不限于此，并且树结构可以是这样的：分支从下到上变得更宽，从左到右变得更宽，或从右到左变得更宽。在这种情况下，必须改变与各个中间节点相关的子集的定义以便适合它。然而，改变是简单地旋转由上述树结构设置部分 104 配置的树结构，并且其意义与任意情况下完全相同。进一步，尽管临时有向图生成部分 108 和有向图生成部分 110 通过从左至右或从右至左设置坐标轴来构建有向图 I’和 I，但是对于颠倒了左和右的改变来说是相同的。具体地说，尽管在以上描述中为了方便起见，基于垂直方向或水平方向来定义参数，但是基于普通人或本领域技术人员的常识，即使旋转或颠倒树结构或有向图以改变垂直和水平关系，这也旨在包含于完全相同的技术范围。

[0459] 例如，根据本发明的实施例的临时有向图生成部分 108 不仅可以基于上述基本方案生成临时有向图，还可以基于另一方案生成临时有向图。例如，临时有向图可以是通过简单地组合具有长度 1 的有向边和具有长度 2 的有向边而形成的有向图，或者可以是将更长的有向边朝向更接近或更远离有向路径的起点的位置放置的有向图。当然，它可以是基于比上述基本方案更复杂的逻辑而生成的临时有向图。以这种方式，本发明的基本构思可应用的范围不限于上述基本方案，而是覆盖了通过各种方案生成的有向图。当然，根据本实施例的信息处理单元可以进一步包括获取或接收由另一信息处理单元生成的有向图的获取部分并可以基于给定条件重建有向图。

[0460] 例如，假设上述树结构设置部分 154 形成分支从上到下变得更宽的树结构，不限于此，并且树结构可以是这样的：分支从下到上变得更宽，从左到右变得更宽，或从右到左变得更宽。在这种情况下，必须改变与各个中间节点相关的子集的定义以便适合它。然而，改变是简单地旋转由上述树结构设置部分 104 配置的树结构，并且其意义与任意情况下完全相同。进一步，尽管临时有向图生成部分 158 和有向图生成部分 160 通过从左至右或从右至左设置坐标轴来构建有向图 I’和 I，但是对于颠倒了左和右的改变来说是相同的。具体地说，尽管在以上描述中为了方便起见，基于垂直方向或水平方向来定义参数，但是基于普通人或本领域技术人员的常识，即使旋转或颠倒树 结构或有向图以改变垂直和水平关系，这也旨在包含于完全相同的技术范围。

[0461] 例如，根据本发明的实施例的临时有向图生成部分 158 不仅可以基于上述基本方案生成临时有向图，还可以基于另一方案生成临时有向图。例如，临时有向图可以是将更长

的有向边朝向更接近或更远离有向路径的起点的位置放置的有向图。当然，它可以是基于比上述基本方案更复杂的逻辑而生成的临时有向图。以这种方式，本发明的基本构思可应用的范围不限于上述基本方案，而是覆盖了通过各种方案生成的有向图。进一步，根据本实施例的信息处理单元可以进一步包括获取给定有向图的获取部分。在这种情况下，信息处理单元基于所获取的有向图可以生成集合密钥。

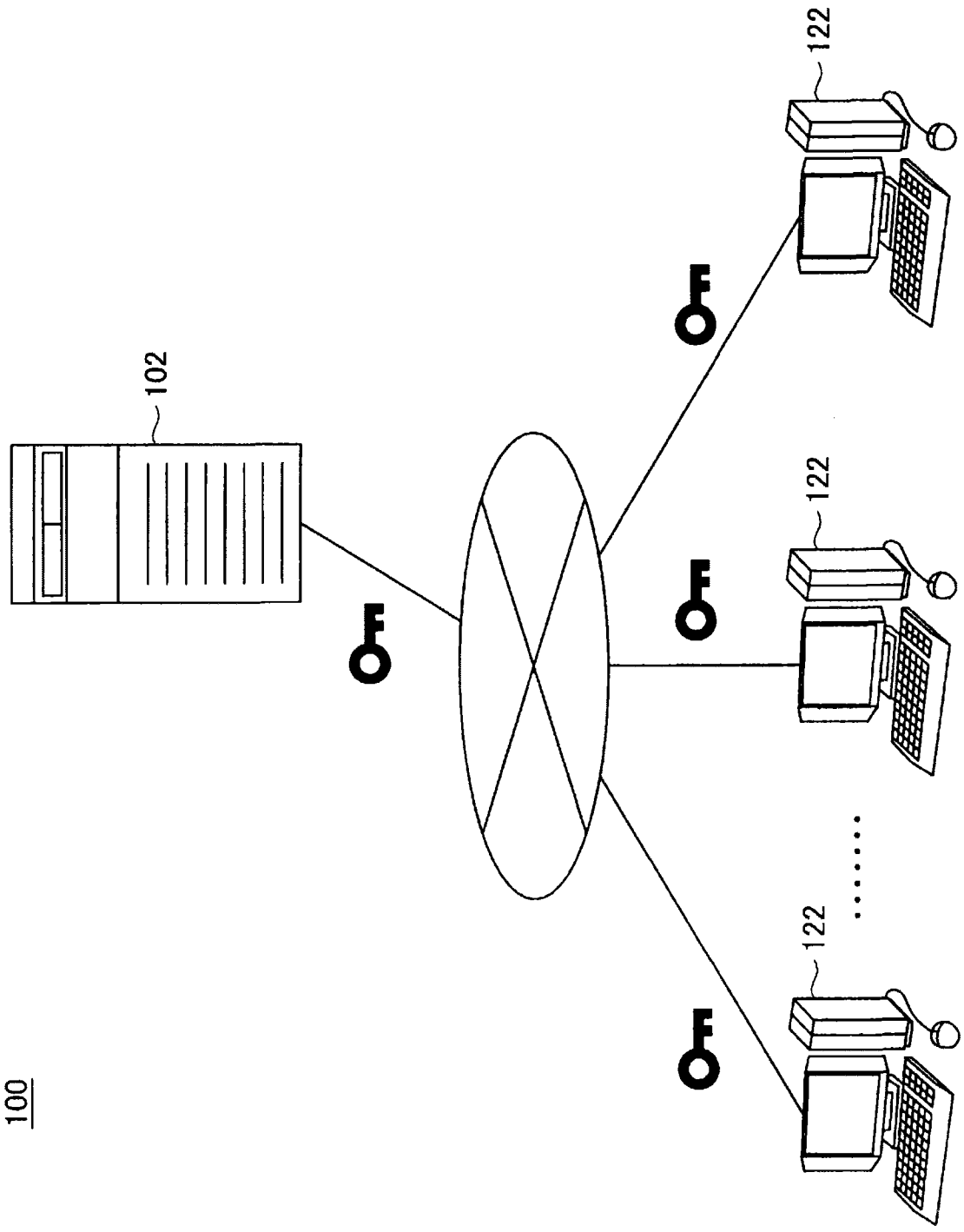


图 1

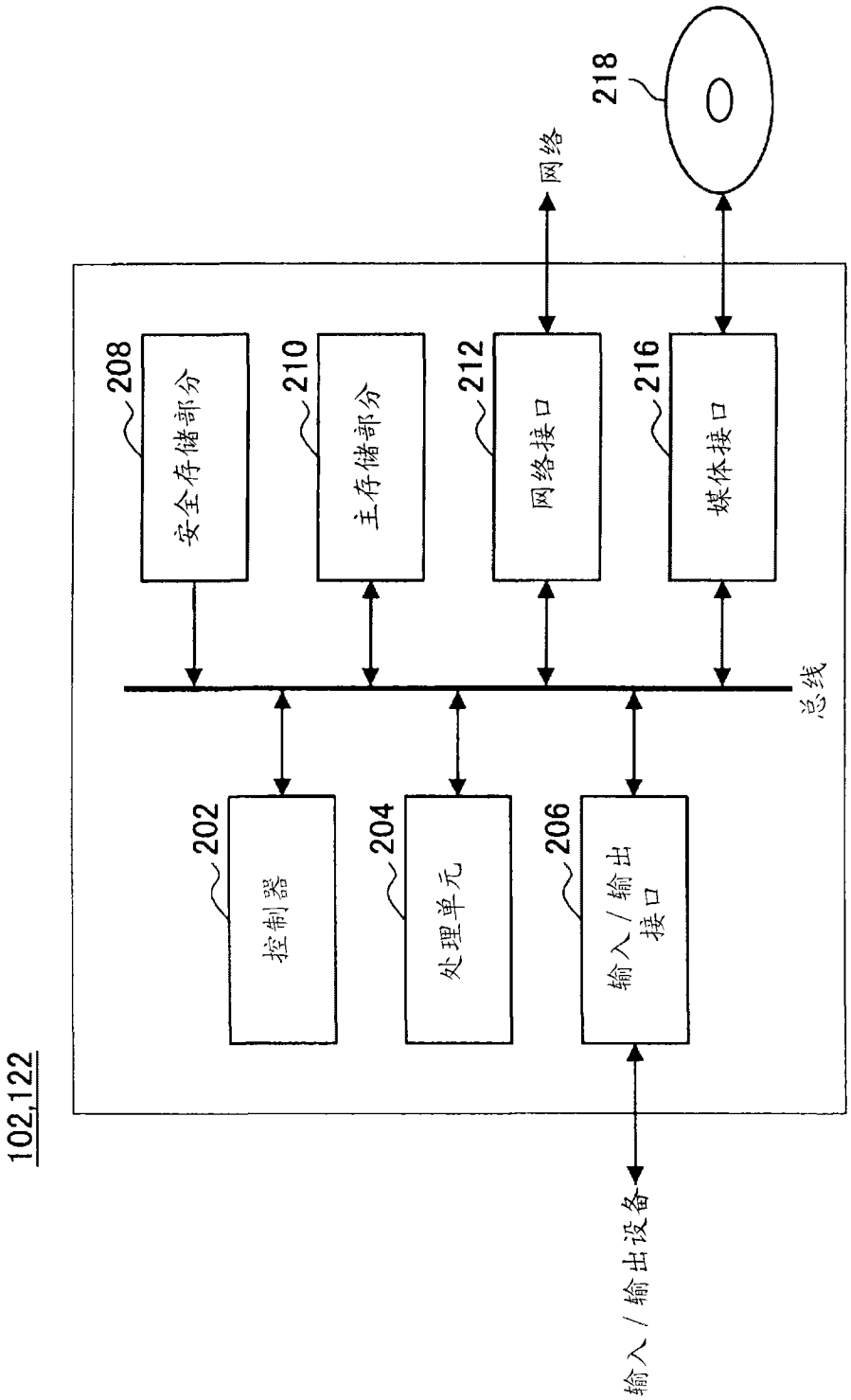

102,122
208
安全存储部分
210
主存储部分
212
网络接口
216
媒体接口
218
网络
总线
202
控制器
204
处理单元
206
输入/输出接口
输入/输出设备

图 2

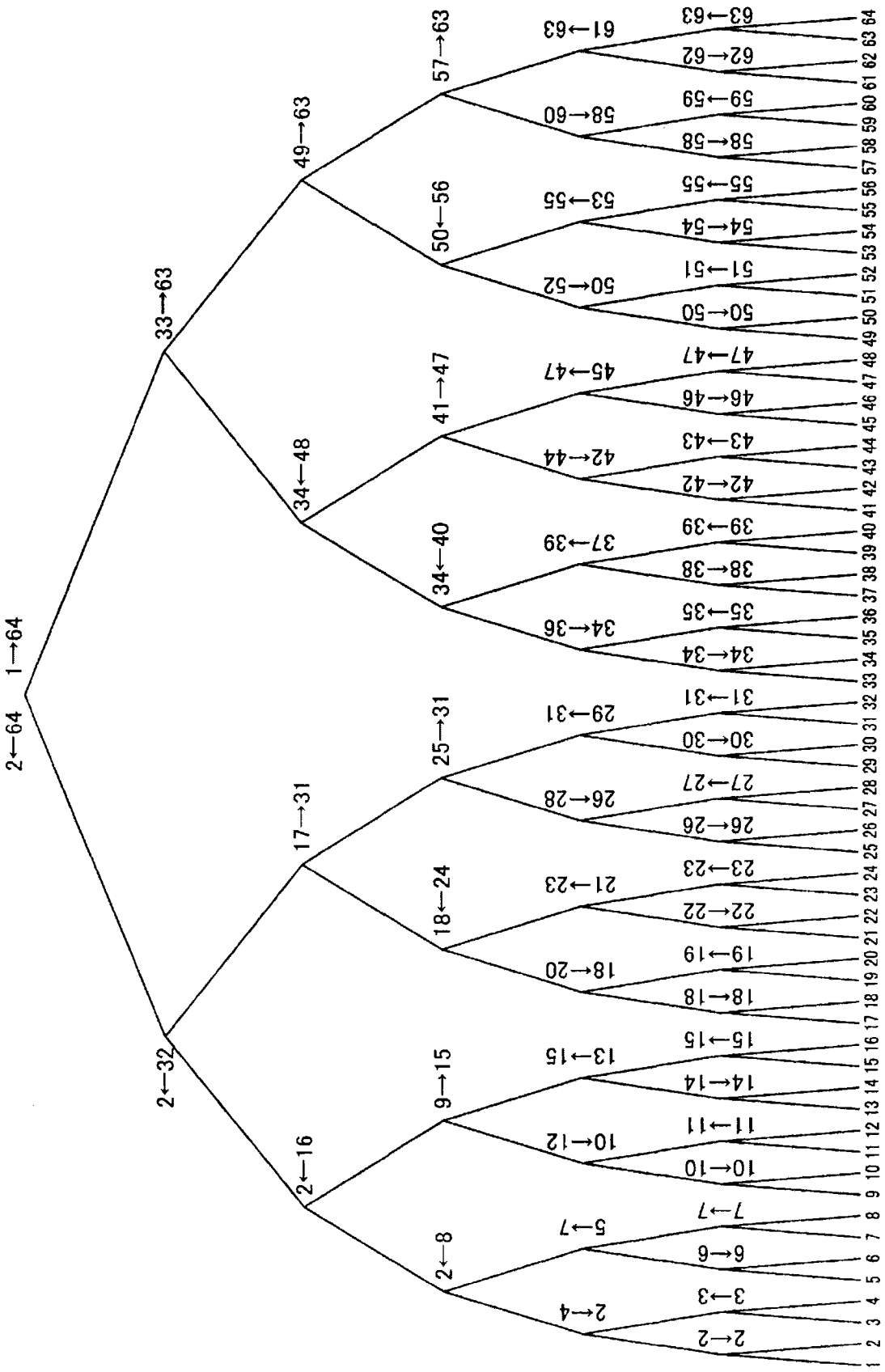

1→64
2←64
33→63
2←32
49→63
17→31
34←48
2←16
57→63
50←56
41→47
25→31
34←40
18←24
9→15
2←8
61←63
58←60
53←55
50←52
45←47
42←44
37←39
34←36
29←31
26←28
21←23
18←20
13←15
10←12
5←7
2←4
63←63
62←62
59←59
58←58
55←55
54←54
51←51
50←50
47←47
46←46
43←43
42←42
39←39
38←38
35←35
34←34
31←31
30←30
27←27
26←26
23←23
22←22
19←19
18←18
15←15
14←14
11←11
10←10
7←7
6←6
3←3
2←2
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 3

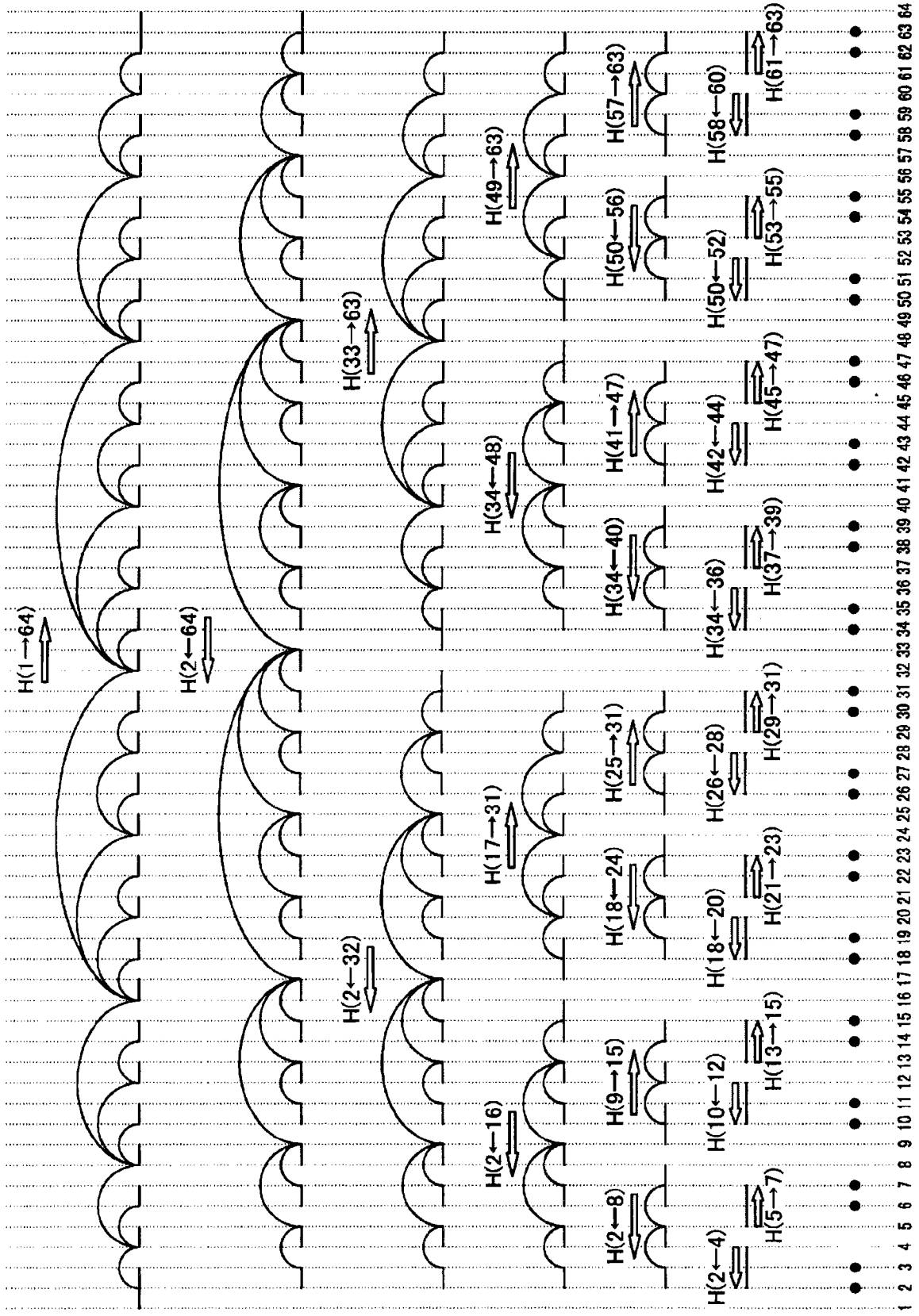

H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(49→63)
H(17→31)
H(34←48)
H(57→63)
H(25→31)
H(50←56)
H(41→47)
H(9→15)
H(18←24)
H(29→31)
H(26←28)
H(37→39)
H(2←16)
H(34←40)
H(53→55)
H(45→47)
H(61→63)
H(58←60)
H(42←44)
H(5→7)
H(13→15)
H(21→23)
H(50←52)
H(34←36)
H(10←12)
H(2←8)
H(2←4)
H(18←20)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 4

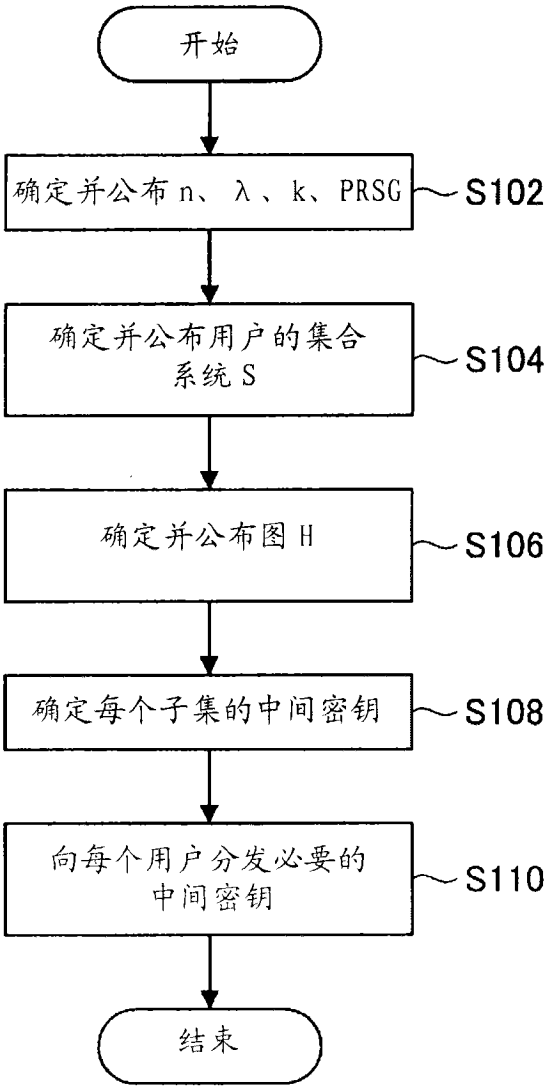

开始
确定并公布 n、λ、k、PRSG
S102
确定并公布用户的集合系统 S
S104
确定并公布图 H
S106
确定每个子集的中间密钥
S108
向每个用户分发必要的中间密钥
S110
结束

图 5

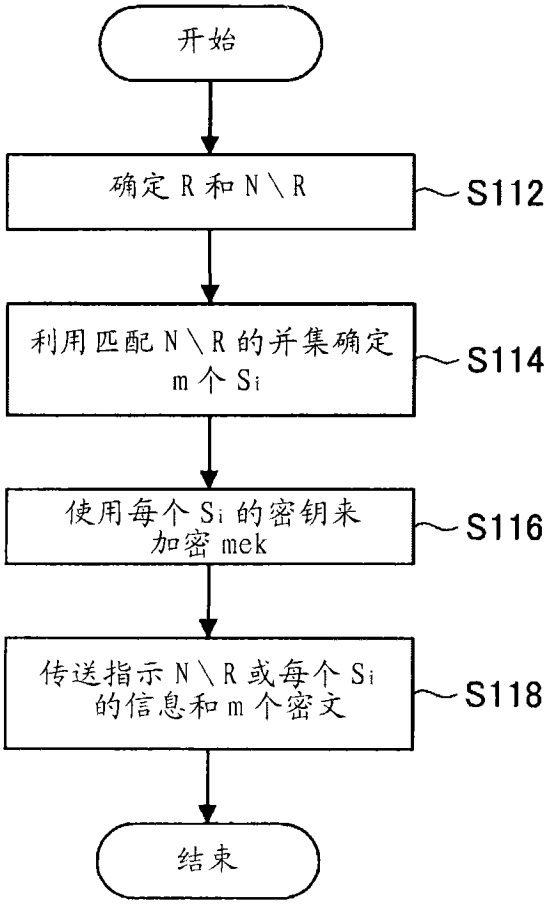

开始
确定 R 和 N \ R
S112
利用匹配 N \ R 的并集确定 m 个 Si
S114
使用每个 Si 的密钥来加密 mek
S116
传送指示 N \ R 或每个 Si 的信息和 m 个密文
S118
结束

图 6

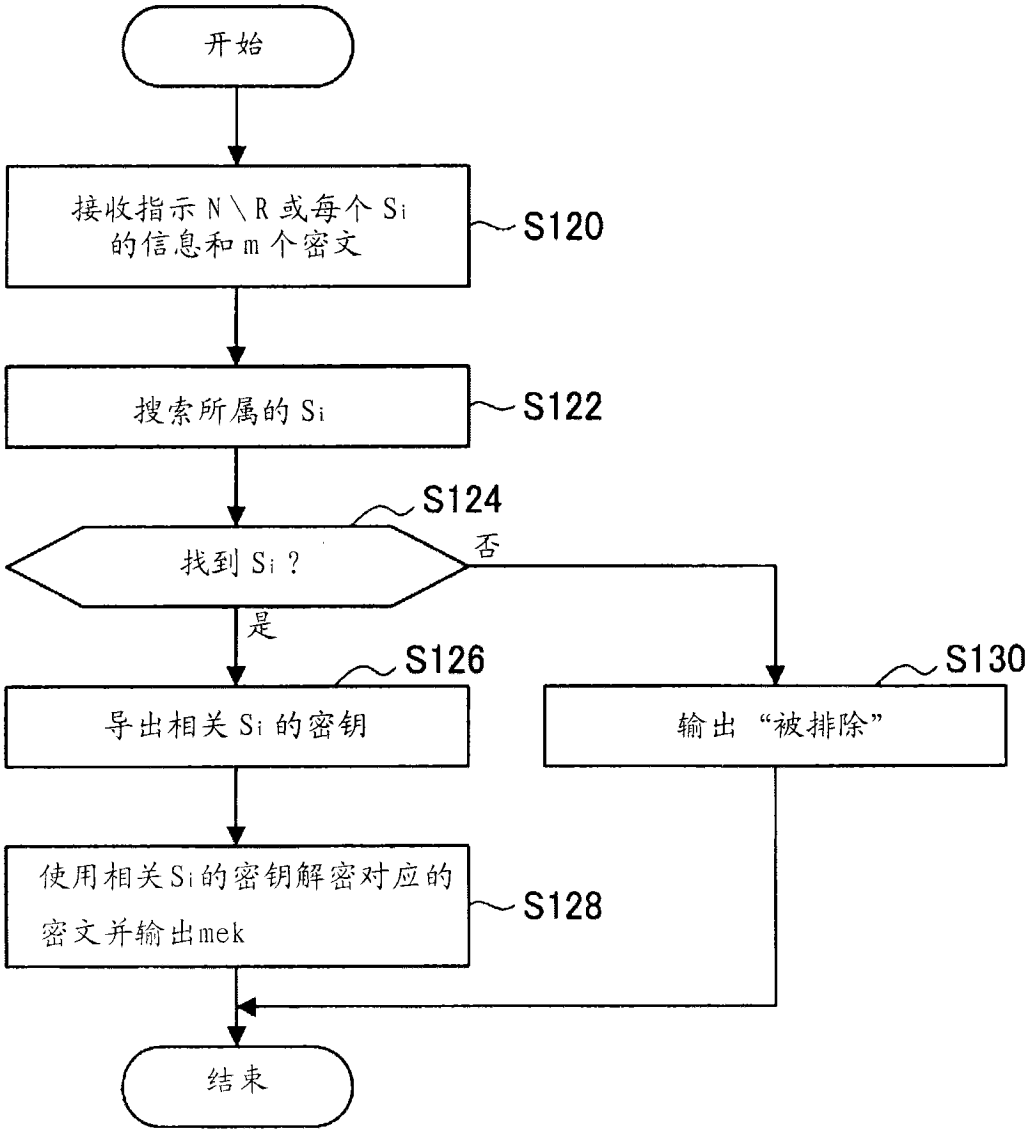

开始
接收指示 N \ R 或每个 Si 的信息和 m 个密文
S120
搜索所属的 Si
S122
S124
找到 Si ?
否
是
S126
导出相关 Si 的密钥
S130
输出 “被排除”
使用相关Si的密钥解密对应的密文并输出mek
S128
结束

图 7

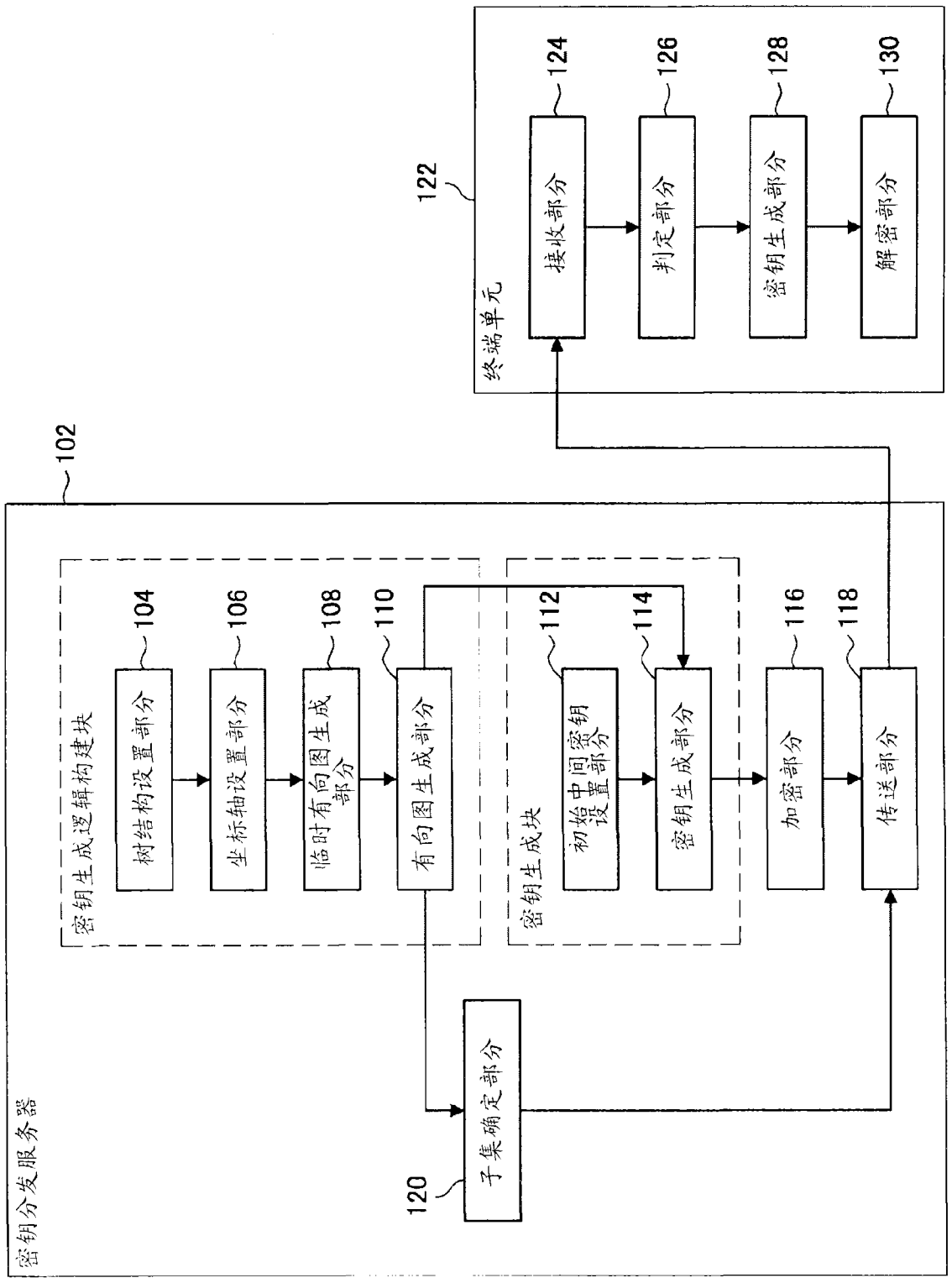

密钥分发服务器
102
密钥生成逻辑构建块
树结构设置部分
104
坐标轴设置部分
106
临时有向图生成部分
108
有向图生成部分
110
密钥生成块
初始中间密钥设置部分
112
密钥生成部分
114
加密部分
116
传送部分
118
子集确定部分
120
终端单元
122
接收部分
124
判定部分
126
密钥生成部分
128
解密部分
130

图 8

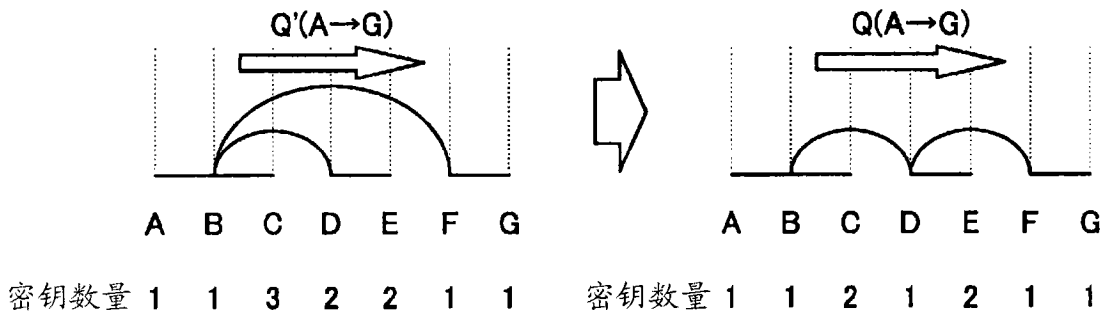

Q'(A→G)
Q(A→G)
A B C D E F G
密钥数量 1 1 3 2 2 1 1
A B C D E F G
密钥数量 1 1 2 1 2 1 1

图 9

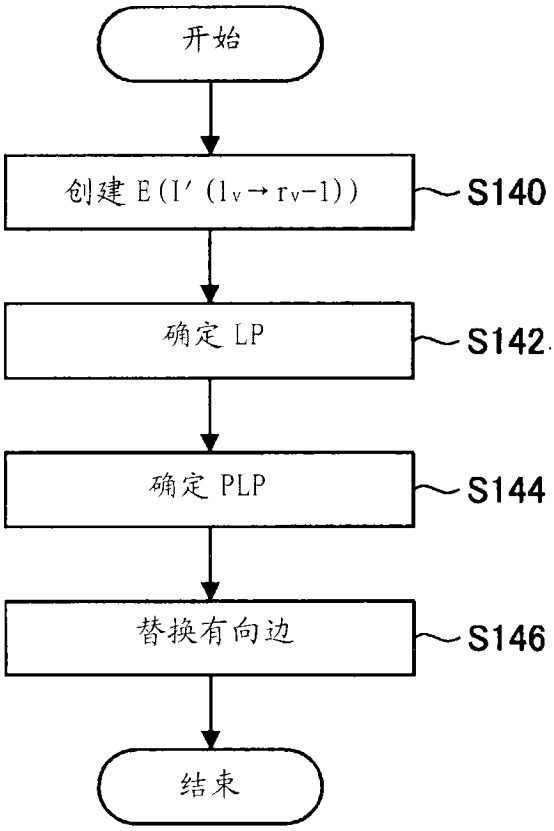

开始
创建 E(I'(lv→rv-1))
S140
确定 LP
S142
确定 PLP
S144
替换有向边
S146
结束

图 10

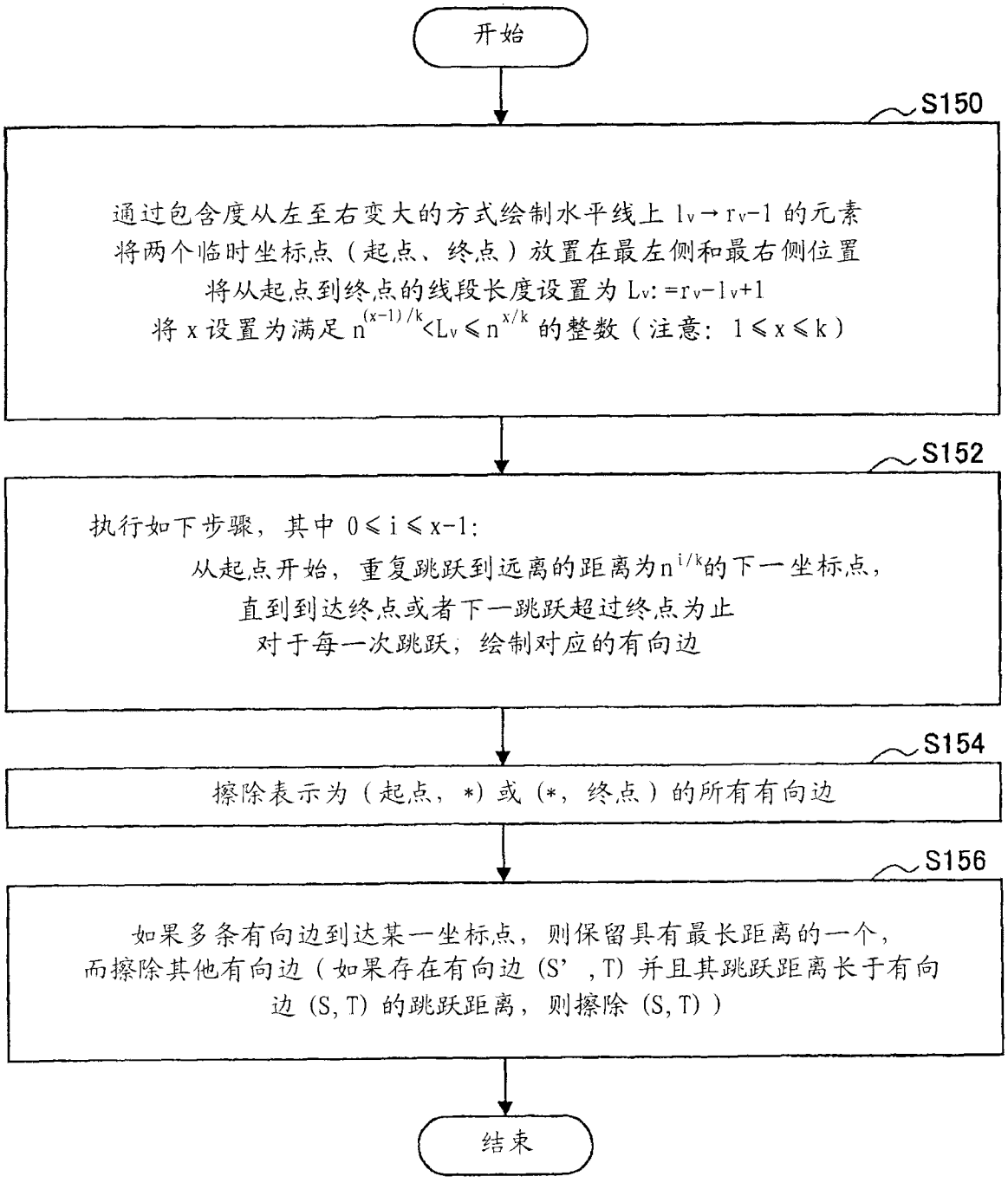

开始
S150
通过包含度从左至右变大的方式绘制水平线上 $l_v \rightarrow r_v-1$ 的元素
将两个临时坐标点（起点、终点）放置在最左侧和最右侧位置
将从起点到终点的线段长度设置为 $L_v:=r_v-l_v+1$
将 x 设置为满足 $n^{(x-1)/k}<L_v \leqslant n^{x/k}$ 的整数（注意：$1 \leqslant x \leqslant k$）
S152
执行如下步骤，其中 $0 \leqslant i \leqslant x-1$:
从起点开始，重复跳跃到远离的距离为 $n^{i/k}$ 的下一坐标点，
直到到达终点或者下一跳跃超过终点为止
对于每一次跳跃，绘制对应的有向边
S154
擦除表示为（起点，*）或（*，终点）的所有有向边
S156
如果多条有向边到达某一坐标点，则保留具有最长距离的一个，
而擦除其他有向边（如果存在有向边 (S', T) 并且其跳跃距离长于有向
边 (S, T) 的跳跃距离，则擦除 (S, T)）
结束

图 11

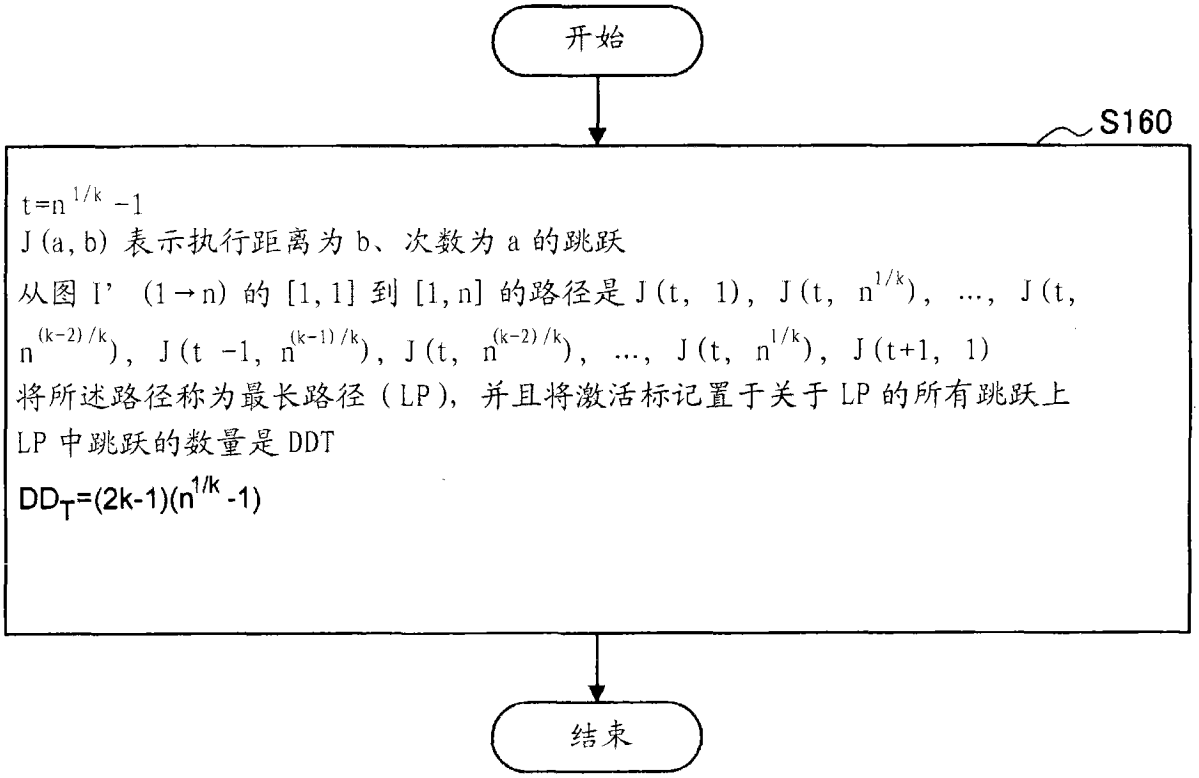

开始
S160
$t=n^{1/k}-1$
J(a, b) 表示执行距离为 b、次数为 a 的跳跃
从图 I' (1→n) 的 [1, 1] 到 [1, n] 的路径是 J(t, 1), J(t, $n^{1/k}$), ..., J(t, $n^{(k-2)/k}$), J(t -1, $n^{(k-1)/k}$), J(t, $n^{(k-2)/k}$), ..., J(t, $n^{1/k}$), J(t+1, 1)
将所述路径称为最长路径 (LP), 并且将激活标记置于关于 LP 的所有跳跃上
LP 中跳跃的数量是 DDT
$DD_T=(2k-1)(n^{1/k}-1)$
结束

图 12

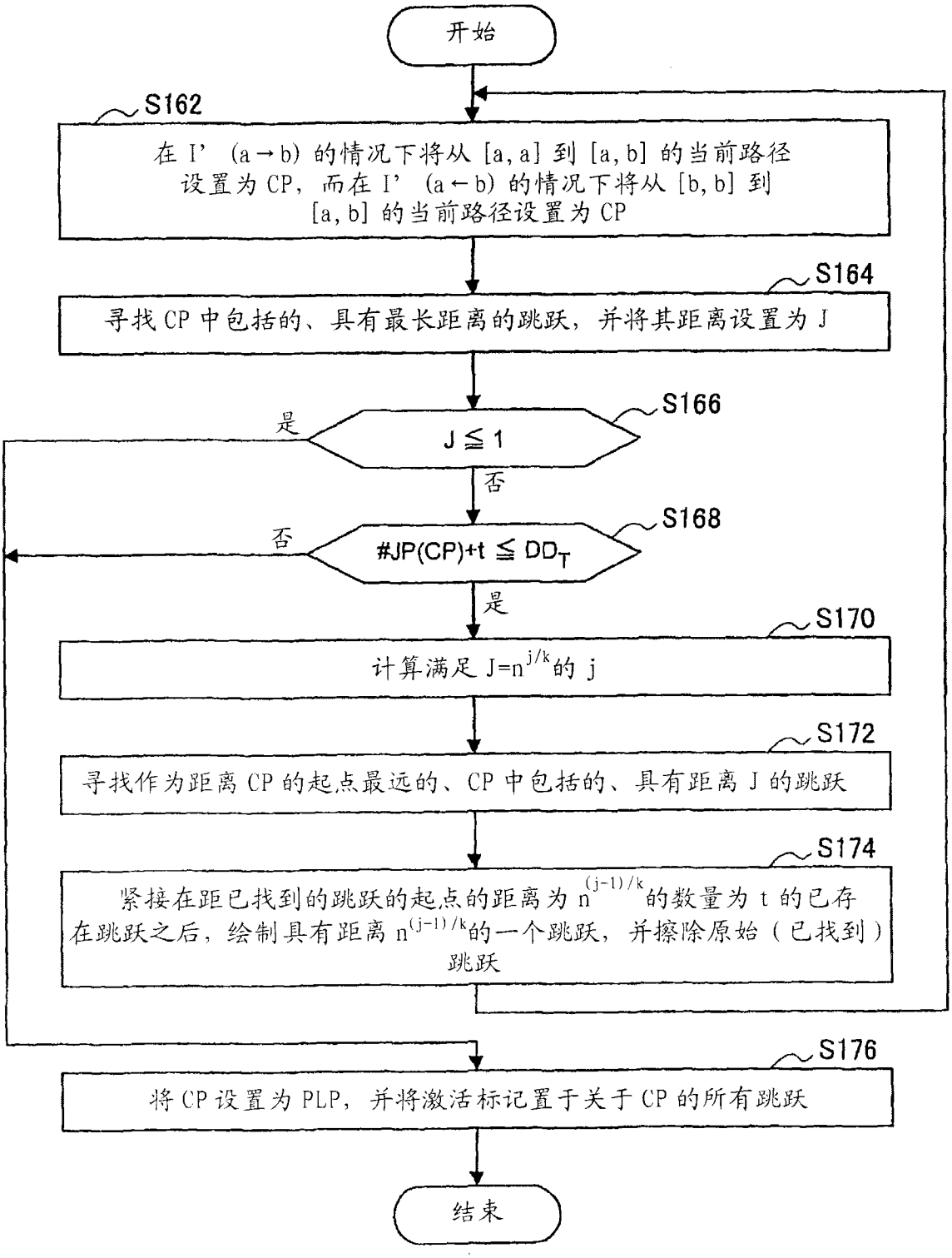

开始
S162
在 I' (a→b) 的情况下将从 [a,a] 到 [a,b] 的当前路径设置为 CP，而在 I' (a←b) 的情况下将从 [b,b] 到 [a,b] 的当前路径设置为 CP
S164
寻找 CP 中包括的、具有最长距离的跳跃，并将其距离设置为 J
S166
是
J ≦ 1
否
S168
否
#JP(CP)+t ≦ DD_T
是
S170
计算满足 J=n^(j/k) 的 j
S172
寻找作为距离 CP 的起点最远的、CP 中包括的、具有距离 J 的跳跃
S174
紧接在距已找到的跳跃的起点的距离为 n^((j-1)/k) 的数量为 t 的已存在跳跃之后，绘制具有距离 n^((j-1)/k) 的一个跳跃，并擦除原始（已找到）跳跃
S176
将 CP 设置为 PLP，并将激活标记置于关于 CP 的所有跳跃
结束

图 13

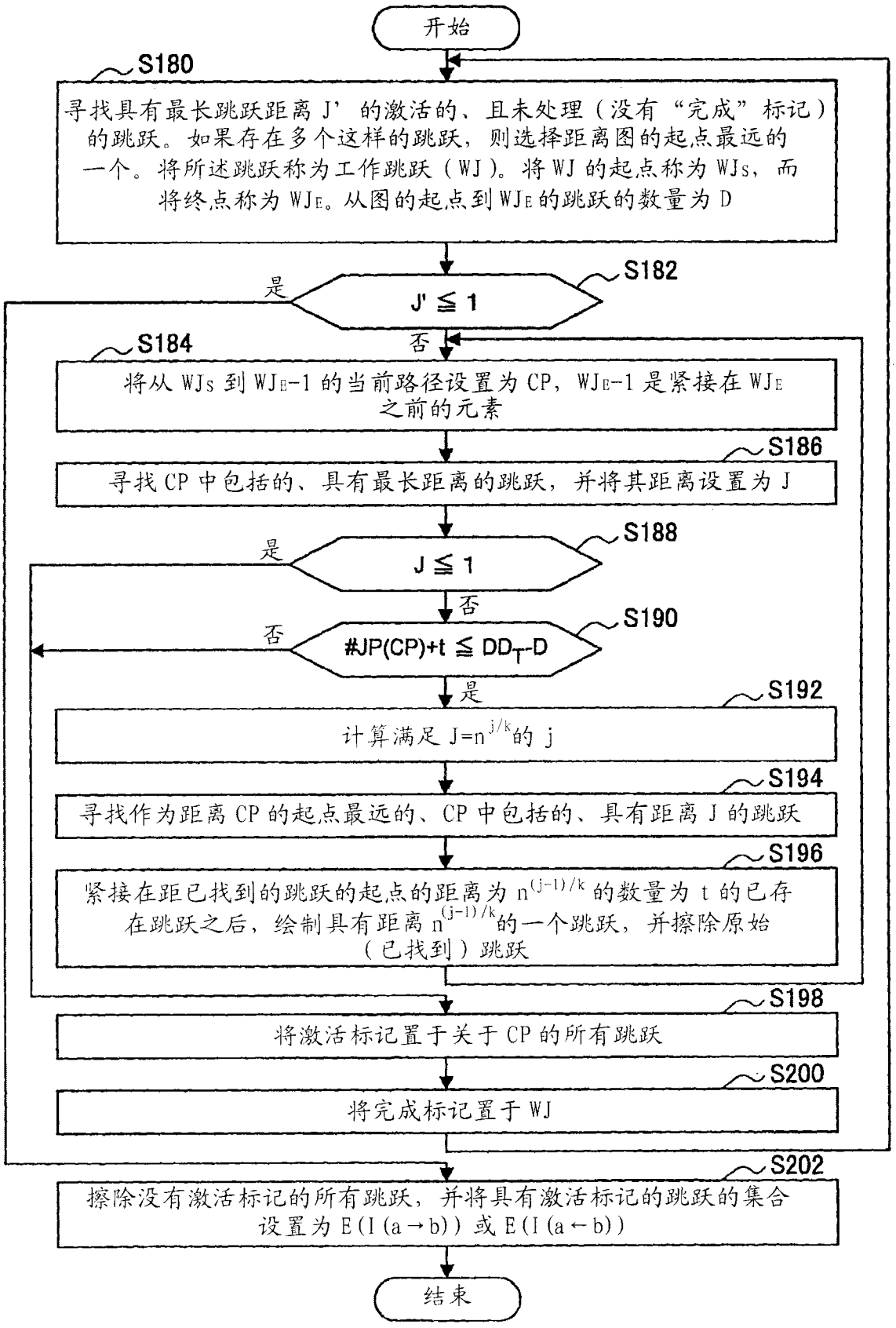

开始
S180
寻找具有最长跳跃距离 J' 的激活的、且未处理（没有“完成”标记）的跳跃。如果存在多个这样的跳跃，则选择距离图的起点最远的一个。将所述跳跃称为工作跳跃（WJ）。将 WJ 的起点称为 WJS，而将终点称为 WJE。从图的起点到 WJE 的跳跃的数量为 D
S182
是
J' ≦ 1
否
S184
将从 WJS 到 WJE-1 的当前路径设置为 CP，WJE-1 是紧接在 WJE 之前的元素
S186
寻找 CP 中包括的、具有最长距离的跳跃，并将其距离设置为 J
S188
是
J ≦ 1
否
S190
否
#JP(CP)+t ≦ DDT-D
是
S192
计算满足 J=n^(j/k) 的 j
S194
寻找作为距离 CP 的起点最远的、CP 中包括的、具有距离 J 的跳跃
S196
紧接在距已找到的跳跃的起点的距离为 n^((j-1)/k) 的数量为 t 的已存在跳跃之后，绘制具有距离 n^((j-1)/k) 的一个跳跃，并擦除原始（已找到）跳跃
S198
将激活标记置于关于 CP 的所有跳跃
S200
将完成标记置于 WJ
S202
擦除没有激活标记的所有跳跃，并将具有激活标记的跳跃的集合设置为 E(I(a→b)) 或 E(I(a←b))
结束

图 14

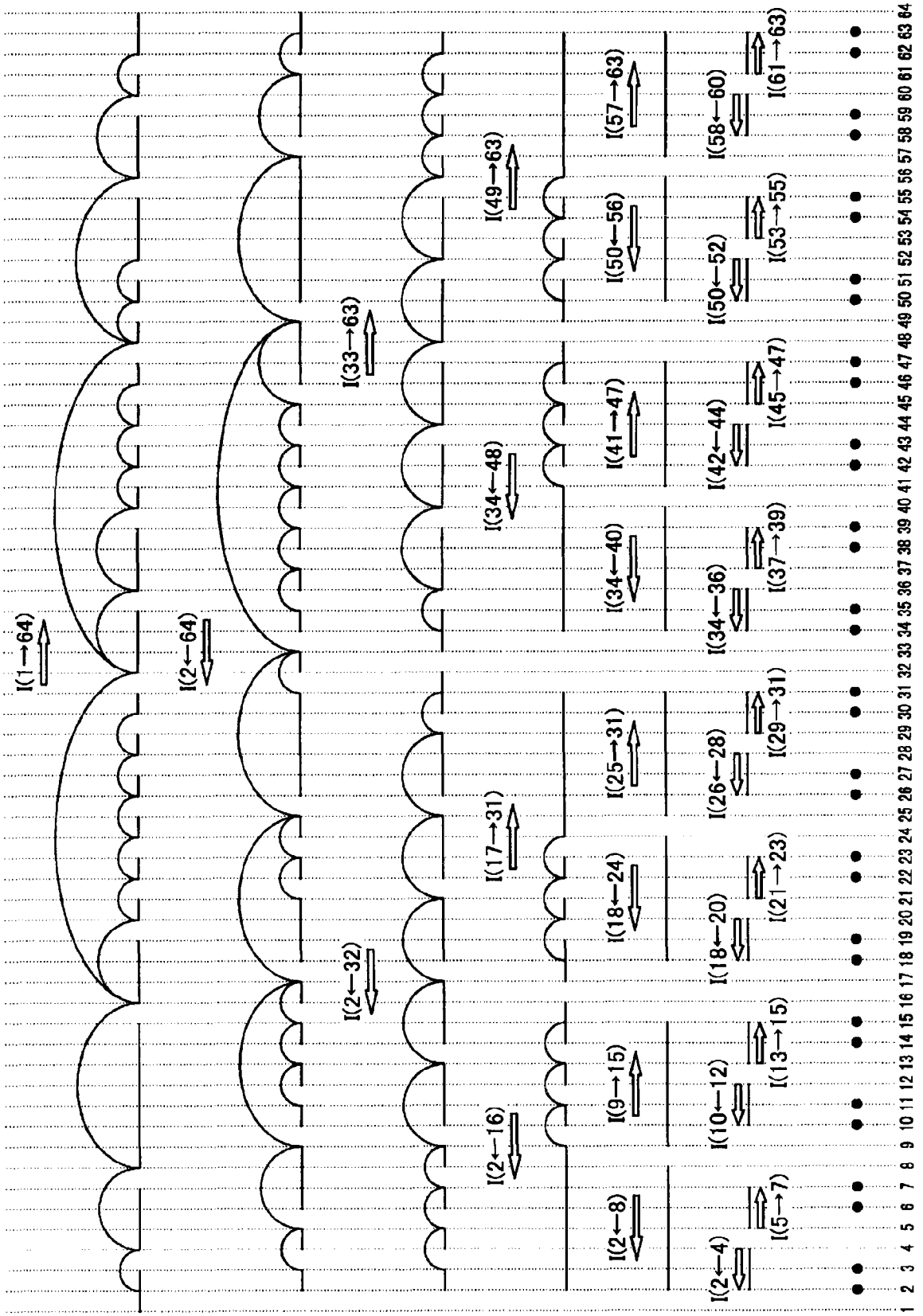

I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(17→31)
I(49→63)
I(34←48)
I(2←16)
I(9→15)
I(25→31)
I(41→47)
I(57→63)
I(2←8)
I(18←24)
I(34←40)
I(50←56)
I(5→7)
I(13→15)
I(29→31)
I(45→47)
I(61→63)
I(10←12)
I(26←28)
I(42←44)
I(58←60)
I(2←4)
I(21→23)
I(37→39)
I(53→55)
I(18←20)
I(34←36)
I(50←52)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 15

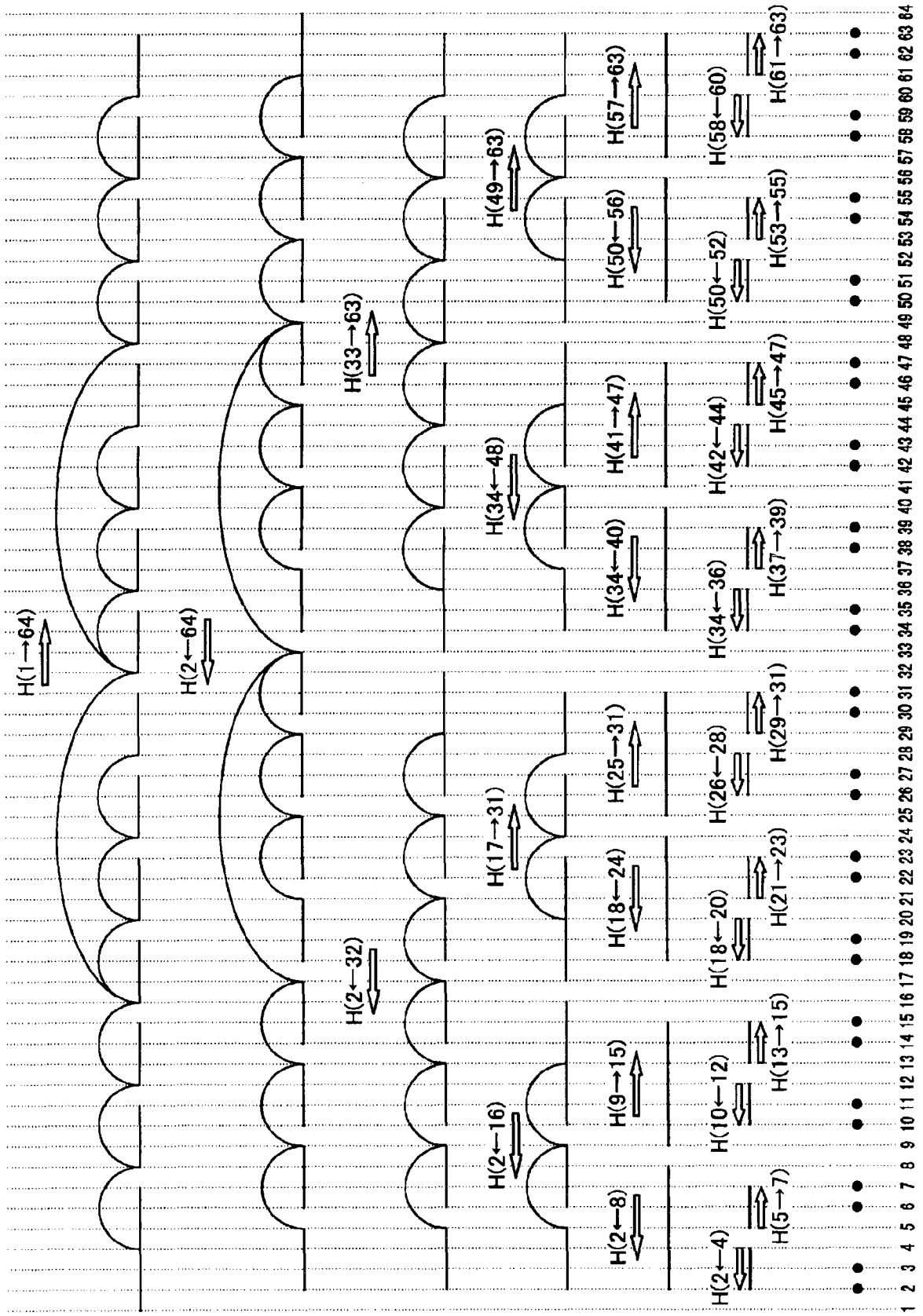

H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(49→63)
H(57→63)
H(50←56)
H(17→31)
H(34←48)
H(41→47)
H(25→31)
H(34←40)
H(2←16)
H(9→15)
H(18←24)
H(26←28)
H(29→31)
H(42←44)
H(45→47)
H(50←52)
H(53→55)
H(58←60)
H(61→63)
H(34←36)
H(37→39)
H(10←12)
H(13→15)
H(18←20)
H(21→23)
H(2←4)
H(5→7)
H(2←8)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 16

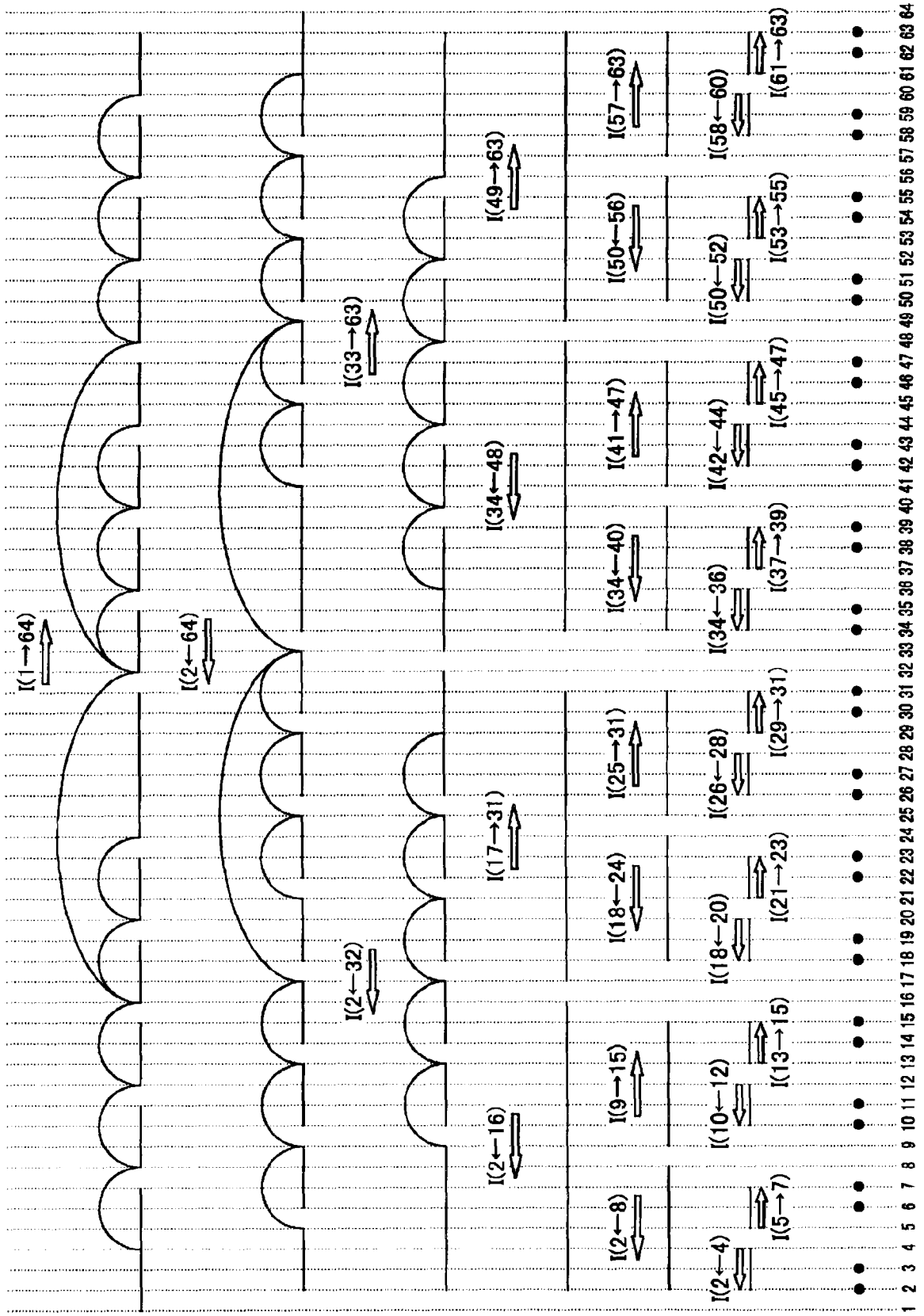

I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(17→31)
I(2←16)
I(9→15)
I(2←8)
I(5→7)
I(2←4)
I(10←12)
I(13→15)
I(18←20)
I(21→23)
I(25→31)
I(18←24)
I(26←28)
I(29→31)
I(34←40)
I(41→47)
I(34←48)
I(49→63)
I(34←36)
I(37→39)
I(42←44)
I(45→47)
I(50←52)
I(53→55)
I(50←56)
I(57→63)
I(58←60)
I(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 17

	(A)	(B)	(C)	(D)	(E)
用户	基本方案 (k=6)	基本方案 (k=3)	本发明 (k=6)	基本方案（k=6）与本发明（k=6）之间的差别	基本方案（k=3）与本发明（k=6）之间的差别
1	1	1	1	0	0
2	7	7	7	0	0
3	8	7	8	0	-1
4	10	6	8	2	-2
5	8	7	7	1	0
6	12	11	10	2	1
7	11	11	9	2	2
8	11	8	7	4	1
9	8	6	6	2	0
10	12	11	11	1	0
11	13	11	10	3	1
12	13	9	11	2	-2
13	11	7	8	3	-1
14	13	10	12	1	-2
15	12	10	10	2	0
16	10	6	7	3	-1
17	8	6	6	2	0
18	12	11	11	1	0
19	13	11	12	1	-1
20	13	9	9	4	0
21	13	10	10	3	0
22	15	13	11	4	2
23	14	13	12	2	1
24	12	9	9	3	0
25	11	9	7	4	2
26	13	13	10	3	3
27	14	13	11	3	2
28	12	10	9	3	1
29	12	8	9	3	-1
30	12	10	10	2	0
31	11	10	9	2	1
32	7	5	5	2	0
33	7	5	5	2	0
34	11	10	10	1	0
35	12	10	11	1	-1
36	12	8	9	3	-1
37	12	10	10	2	0
38	14	13	12	2	1
39	13	13	11	2	2
40	11	9	8	3	1
41	12	9	9	3	0
42	14	13	12	2	1
43	15	13	11	4	2
44	13	10	10	3	0
45	13	9	10	3	-1
46	13	11	12	1	-1
47	12	11	11	1	0
48	8	6	6	2	0
49	10	6	7	3	-1
50	12	10	10	2	0
51	13	10	12	1	-2
52	11	7	8	3	-1
53	13	9	10	3	-1
54	13	11	10	3	1
55	12	11	11	1	0
56	8	6	6	2	0
57	11	8	7	4	1
58	11	11	9	2	2
59	12	11	10	2	1
60	8	7	7	1	0
61	10	6	8	2	-2
62	8	7	8	0	-1
63	7	7	7	0	0
64	2	2	2	0	0
密钥总数	705	577	571	134	6
密钥平均数	11.02	9.02	8.92	2.09	0.09
密钥最大数	15	13	12	3	1

图 18

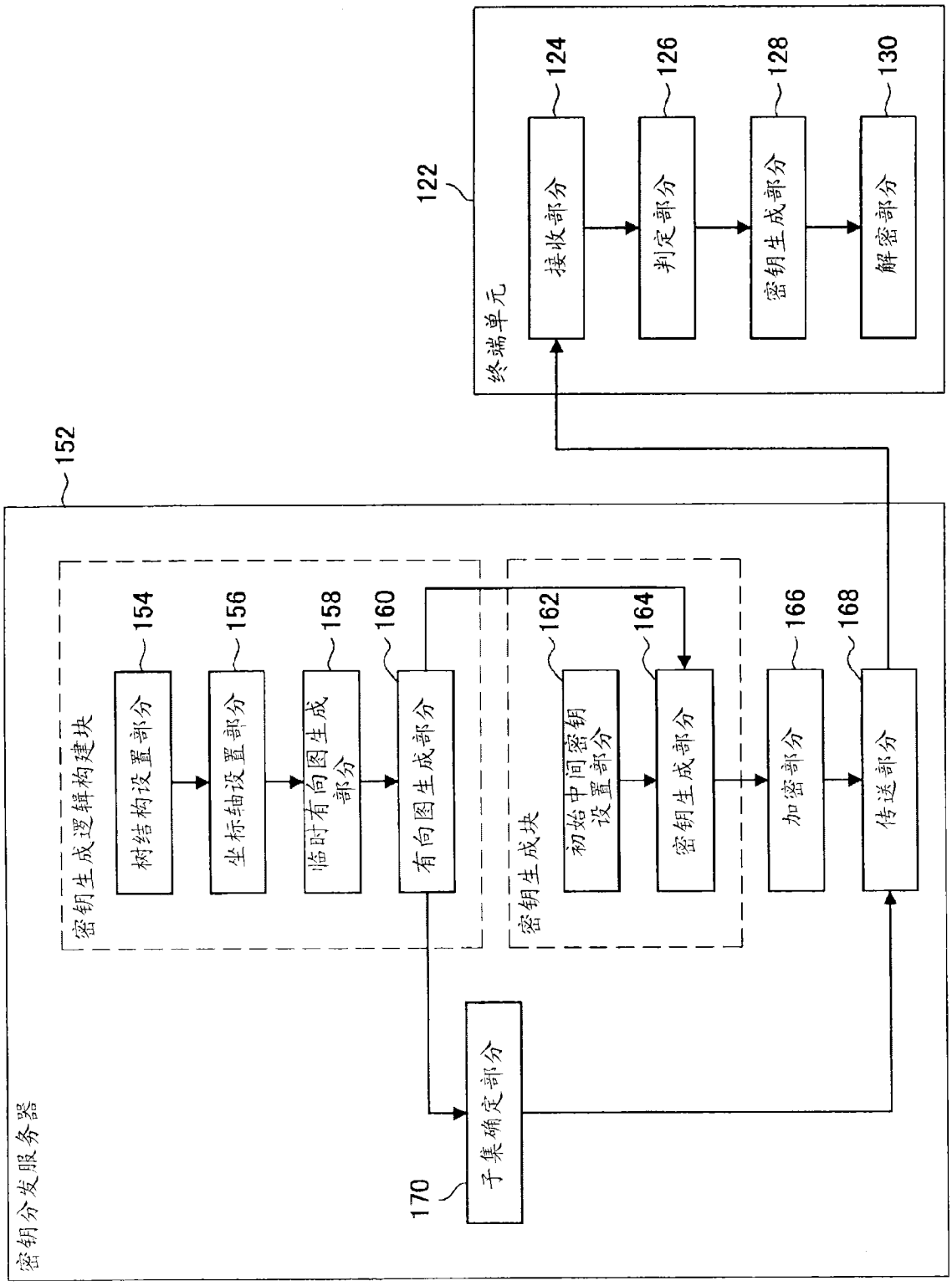

密钥分发服务器
152
密钥生成逻辑构建块
树结构设置部分
154
坐标轴设置部分
156
临时有向图生成部分
158
有向图生成部分
160
密钥生成块
初始中间密钥设置部分
162
密钥生成部分
164
加密部分
166
传送部分
168
子集确定部分
170
终端单元
122
接收部分
124
判定部分
126
密钥生成部分
128
解密部分
130

图 19

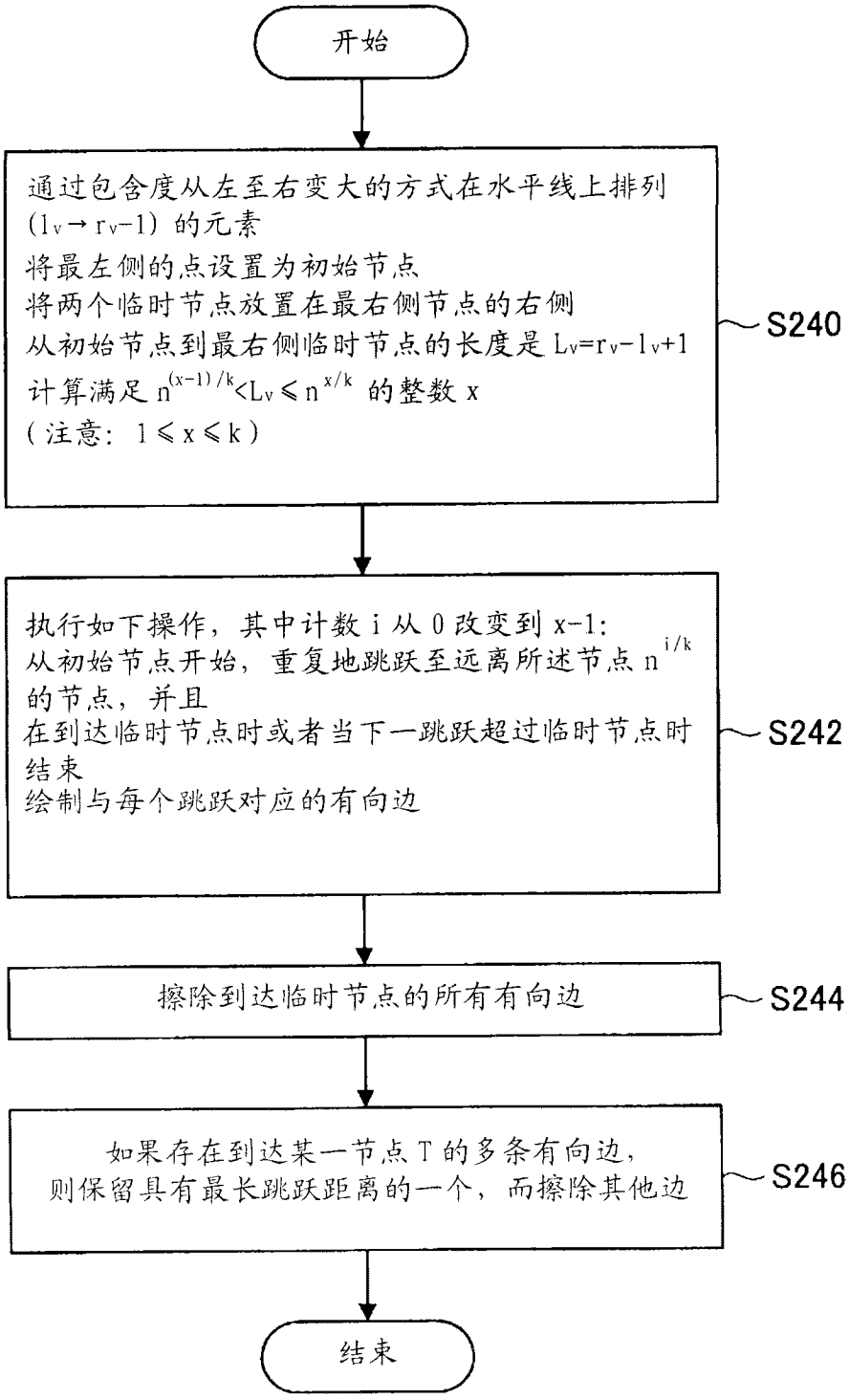

开始
通过包含度从左至右变大的方式在水平线上排列 ($l_v \rightarrow r_v-1$) 的元素
将最左侧的点设置为初始节点
将两个临时节点放置在最右侧节点的右侧
从初始节点到最右侧临时节点的长度是 $L_v=r_v-l_v+1$
计算满足 $n^{(x-1)/k}<L_v \leqslant n^{x/k}$ 的整数 x
(注意: $1 \leqslant x \leqslant k$)
S240
执行如下操作，其中计数 i 从 0 改变到 x-1:
从初始节点开始，重复地跳跃至远离所述节点 $n^{i/k}$ 的节点，并且
在到达临时节点时或者当下一跳跃超过临时节点时结束
绘制与每个跳跃对应的有向边
S242
擦除到达临时节点的所有有向边
S244
如果存在到达某一节点 T 的多条有向边，
则保留具有最长跳跃距离的一个，而擦除其他边
S246
结束

图 20

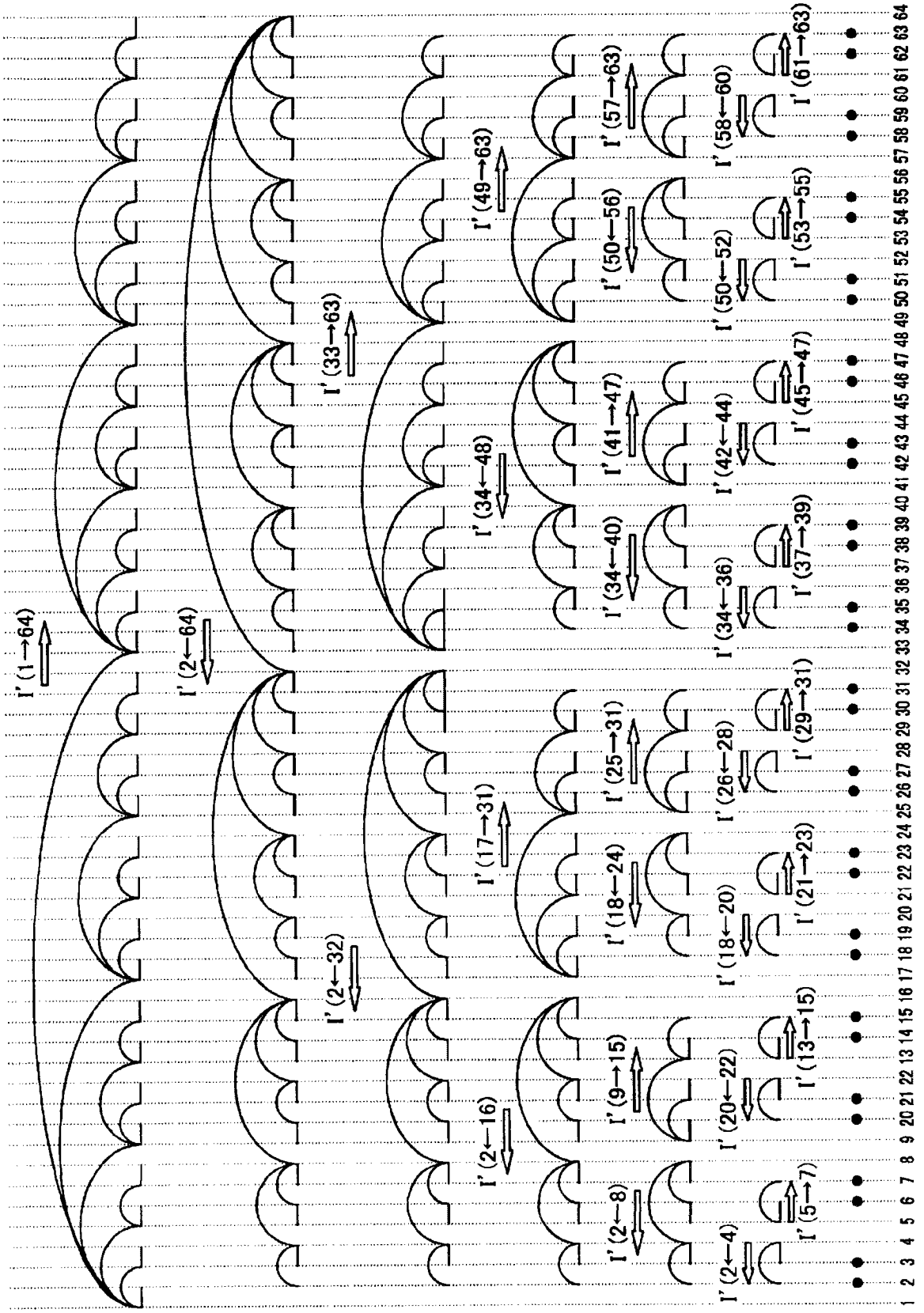

I'(1→64)
I'(2←64)
I'(33→63)
I'(2←32)
I'(49→63)
I'(34←48)
I'(17→31)
I'(2←16)
I'(57→63)
I'(50←56)
I'(41→47)
I'(34←40)
I'(25→31)
I'(18←24)
I'(9→15)
I'(2←8)
I'(61→63)
I'(58←60)
I'(53→55)
I'(50←52)
I'(45→47)
I'(42←44)
I'(37→39)
I'(34←36)
I'(29→31)
I'(26←28)
I'(21→23)
I'(18←20)
I'(13→15)
I'(20←22)
I'(5→7)
I'(2←4)
1 2 3 4 5 6 7 8 9 20 21 22 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 21

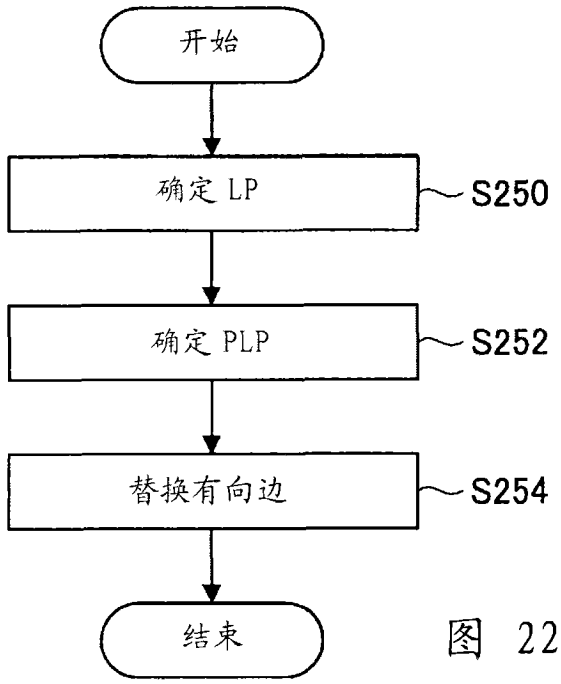

开始
确定 LP
S250
确定 PLP
S252
替换有向边
S254
结束

图 22

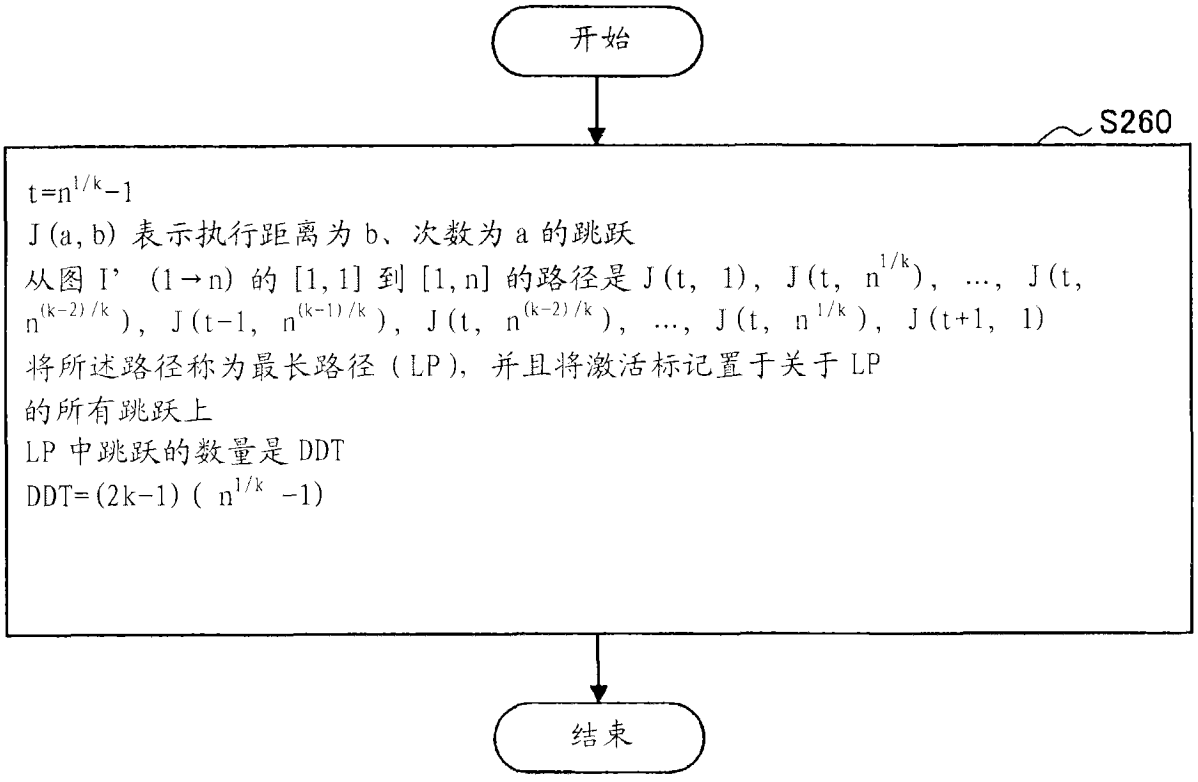

开始
S260
$t=n^{1/k}-1$
J(a, b) 表示执行距离为 b、次数为 a 的跳跃
从图 I' (1→n) 的 [1, 1] 到 [1, n] 的路径是 J(t, 1), J(t, $n^{1/k}$), ..., J(t, $n^{(k-2)/k}$), J(t-1, $n^{(k-1)/k}$), J(t, $n^{(k-2)/k}$), ..., J(t, $n^{1/k}$), J(t+1, 1)
将所述路径称为最长路径 (LP), 并且将激活标记置于关于 LP 的所有跳跃上
LP 中跳跃的数量是 DDT
$DDT=(2k-1)(n^{1/k}-1)$
结束

图 23

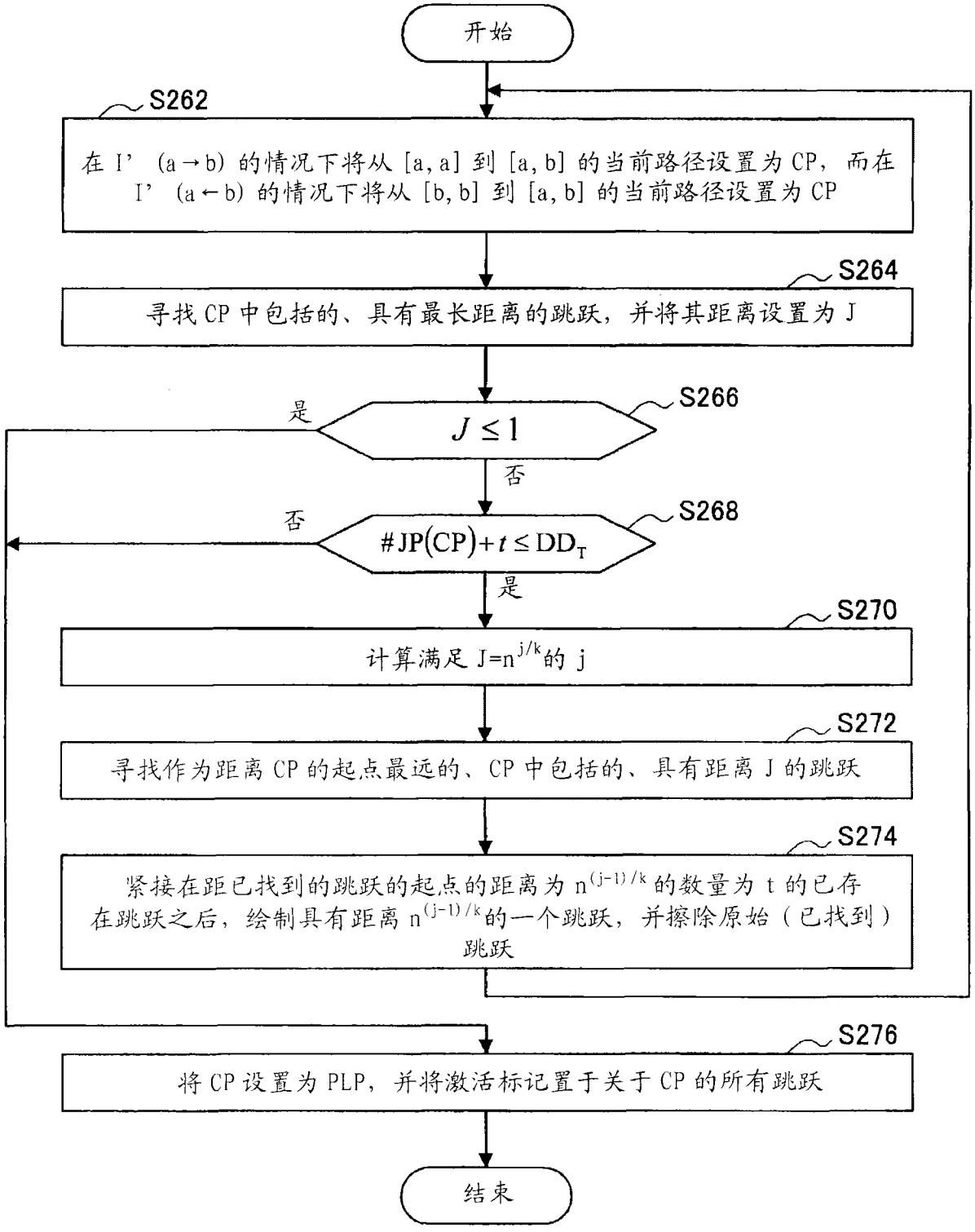

开始
S262
在 I' (a→b) 的情况下将从 [a,a] 到 [a,b] 的当前路径设置为 CP，而在 I' (a←b) 的情况下将从 [b,b] 到 [a,b] 的当前路径设置为 CP
S264
寻找 CP 中包括的、具有最长距离的跳跃，并将其距离设置为 J
S266
是
$J \leq 1$
否
S268
否
$\#JP(CP)+t \leq DD_T$
是
S270
计算满足 $J=n^{j/k}$ 的 j
S272
寻找作为距离 CP 的起点最远的、CP 中包括的、具有距离 J 的跳跃
S274
紧接在距已找到的跳跃的起点的距离为 $n^{(j-1)/k}$ 的数量为 t 的已存在跳跃之后，绘制具有距离 $n^{(j-1)/k}$ 的一个跳跃，并擦除原始（已找到）跳跃
S276
将 CP 设置为 PLP，并将激活标记置于关于 CP 的所有跳跃
结束

图 24

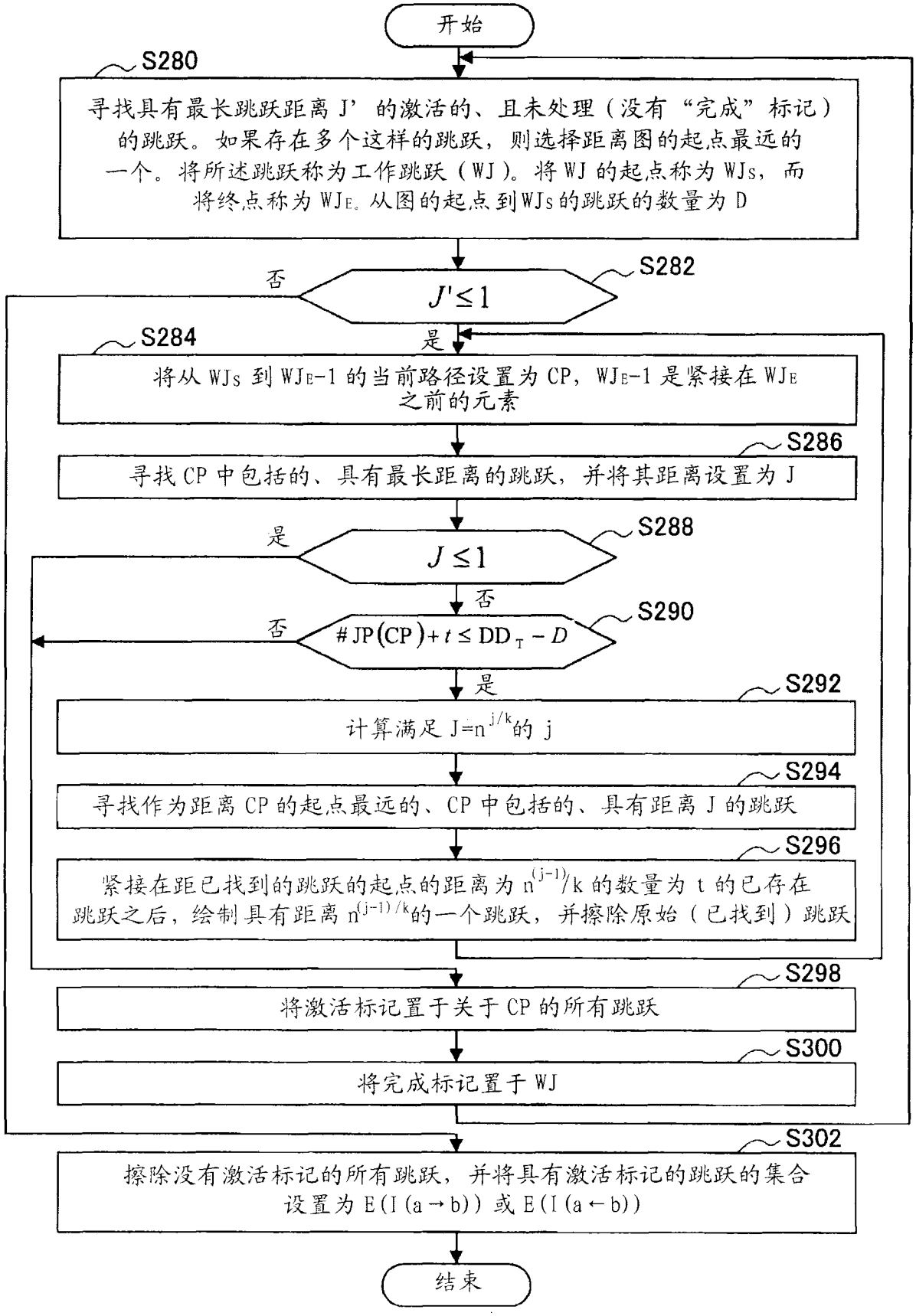

开始
S280
寻找具有最长跳跃距离 J' 的激活的、且未处理（没有“完成”标记）的跳跃。如果存在多个这样的跳跃，则选择距离图的起点最远的一个。将所述跳跃称为工作跳跃（WJ）。将 WJ 的起点称为 WJS，而将终点称为 WJE。从图的起点到WJS的跳跃的数量为 D
S282
否
$J' \leq 1$
是
S284
将从 WJS 到 WJE-1 的当前路径设置为 CP，WJE-1 是紧接在 WJE 之前的元素
S286
寻找 CP 中包括的、具有最长距离的跳跃，并将其距离设置为 J
S288
是
$J \leq 1$
否
S290
否
$\#JP(CP)+t \leq DD_T - D$
是
S292
计算满足 $J=n^{j/k}$ 的 j
S294
寻找作为距离 CP 的起点最远的、CP 中包括的、具有距离 J 的跳跃
S296
紧接在距已找到的跳跃的起点的距离为 $n^{(j-1)}/k$ 的数量为 t 的已存在跳跃之后，绘制具有距离 $n^{(j-1)/k}$ 的一个跳跃，并擦除原始（已找到）跳跃
S298
将激活标记置于关于 CP 的所有跳跃
S300
将完成标记置于 WJ
S302
擦除没有激活标记的所有跳跃，并将具有激活标记的跳跃的集合设置为 E(I(a→b)) 或 E(I(a←b))
结束

图 25

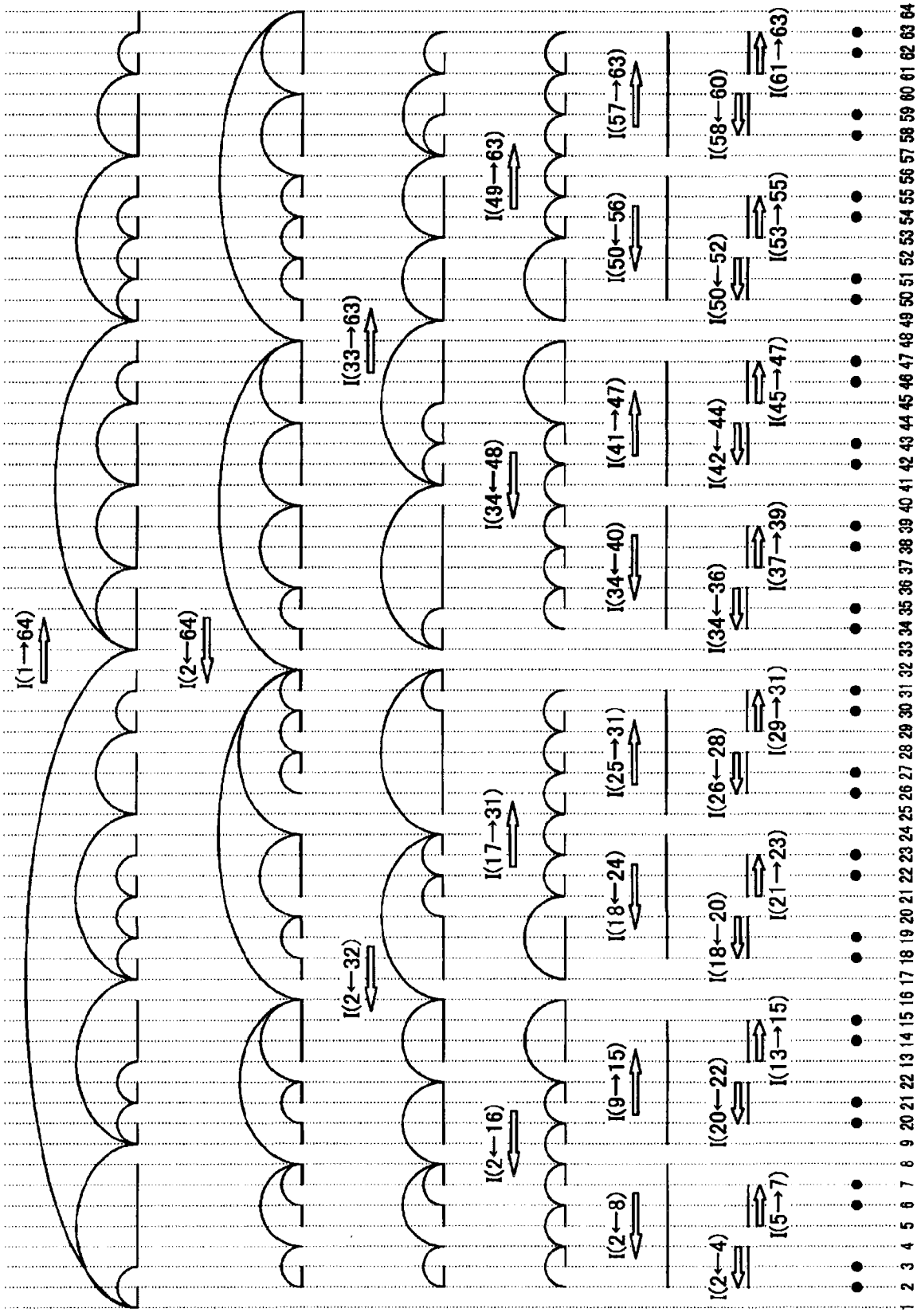

I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(49→63)
I(34←48)
I(17→31)
I(2←16)
I(57→63)
I(50←56)
I(41→47)
I(34←40)
I(25→31)
I(18←24)
I(9→15)
I(2←8)
I(61→63)
I(58←60)
I(53→55)
I(50←52)
I(45→47)
I(42←44)
I(37→39)
I(34←36)
I(29→31)
I(26←28)
I(21→23)
I(18←20)
I(13→15)
I(20←22)
I(5→7)
I(2←4)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

图 26

	(A)	(B)	(C)
用户	基本方案	本发明	基本方案与本发明之间的差别
1	1	1	0
2	7	20	-3
3	8	22	-4
4	20	8	2
5	8	21	-3
6	22	21	1
7	21	14	-3
8	21	7	4
9	8	9	-1
20	22	22	0
21	13	13	0
22	13	20	3
13	21	22	-1
14	13	13	0
15	22	13	-1
16	20	6	4
17	8	7	1
18	22	13	-1
19	13	13	0
20	13	22	1
21	13	22	1
22	15	14	1
23	14	13	1
24	22	9	3
25	21	9	2
26	13	13	0
27	14	13	1
28	22	22	0
29	22	21	1
30	22	13	-1
31	21	13	-2
32	7	4	3
33	7	4	3
34	21	22	-1
35	22	13	-1
36	22	20	2
37	22	21	1
38	14	22	2
39	13	13	0
40	21	9	2
41	22	9	3
42	14	13	1
43	15	13	2
44	13	21	2
45	13	21	2
46	13	13	0
47	22	22	0
48	8	6	2
49	20	5	5
50	22	22	0
51	13	22	1
52	21	21	0
53	13	9	4
54	13	22	1
55	22	21	1
56	8	9	-1
57	21	7	4
58	21	13	-2
59	22	21	1
60	8	20	-2
61	20	8	2
62	8	22	-4
63	7	9	-2
64	2	2	0
密钥总数	705	668	37
密钥平均数	21.02	20.44	0.58
密钥最大数	15	14	1

图 27

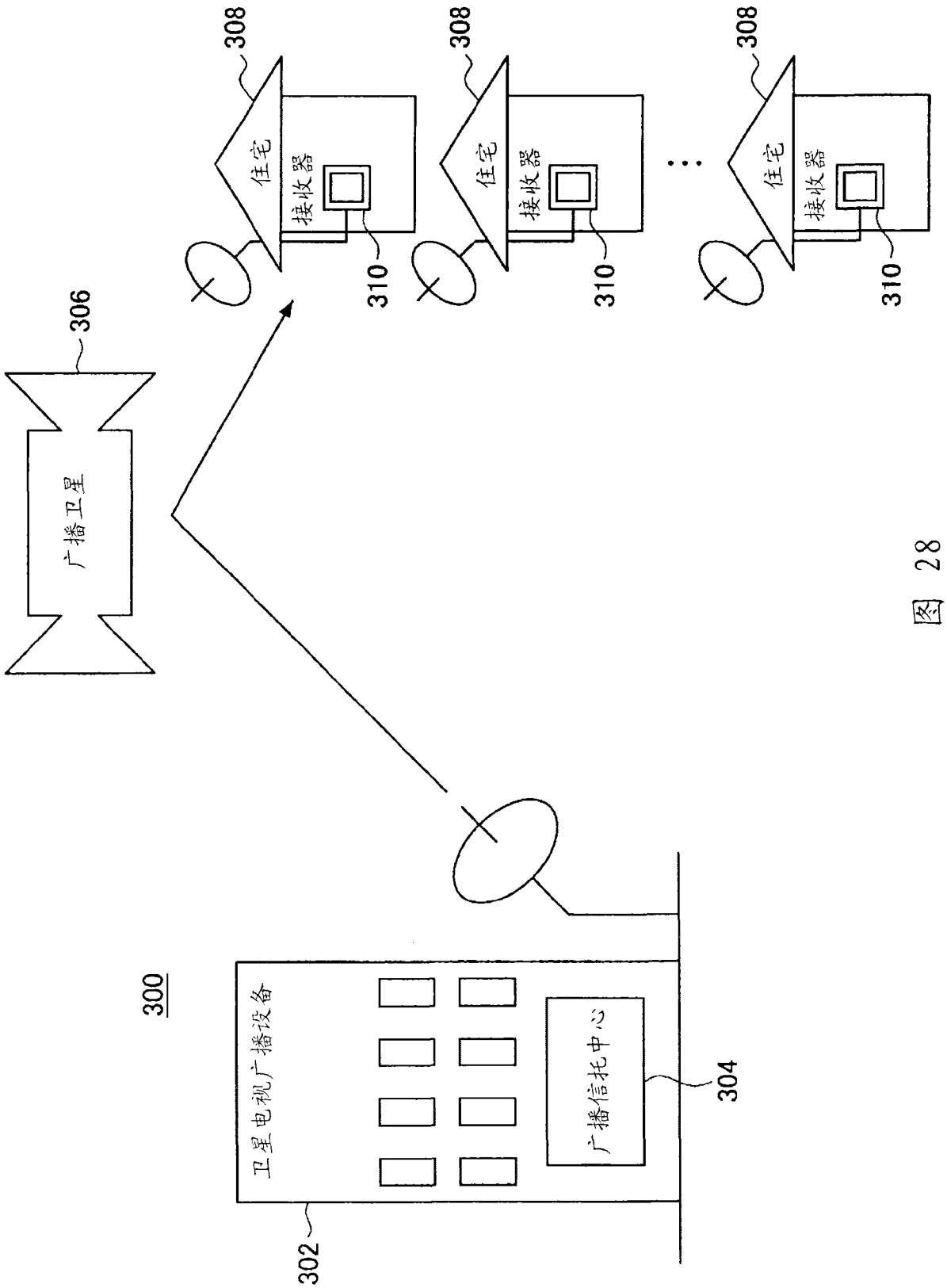

300
卫星电视广播设备
302
广播信托中心
304
306
广播卫星
308
住宅
接收器
310
308
住宅
接收器
310
308
住宅
接收器
310

图 28

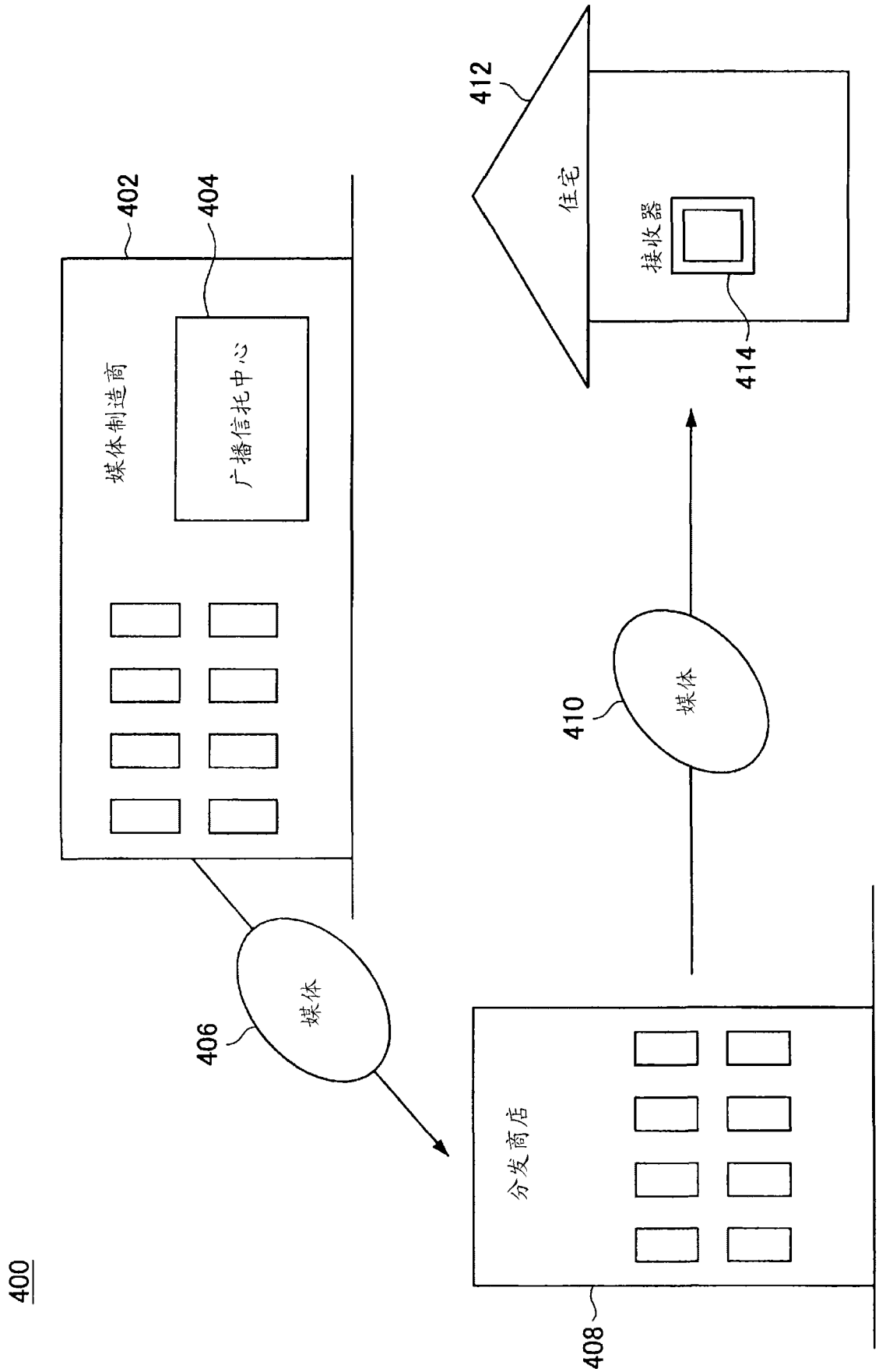


图 29