(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 101542966 B
(45)授权公告日 2013.03.27

(21)申请号 200780042754.1

(22)申请日 2007.10.03

(30)优先权数据
310213/2006 2006.11.16 JP
310208/2006 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/JP2007/069388 2007.10.03

(87)PCT申请的公布数据
WO2008/059673 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
CN 1846396 A,2006.10.11,
WO 2004/028073 A1,2004.04.01,
WO 2006/025589 A1,2006.03.09,

审查员 文娟

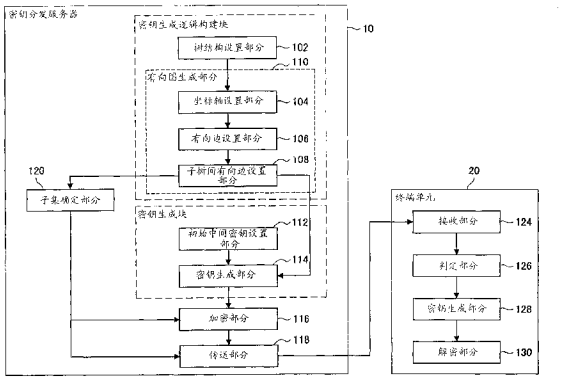
权利要求书 14 页 说明书 49 页 附图 19 页

(54)发明名称

信息处理装置

(57)摘要

本发明提供可以减少终端设备保存的密钥的数量和解码加密数据所需的计算量的信息处理设备。该信息处理设备建立由n个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个树结构，将整个树结构划分成具有$n^{1/y}$个叶节点的多个基本子树，并将它分类成y层(y是log(n)的约数)，以便下层的基本子树的根节点被配置成上层的基本子树的叶节点。进一步，该信息处理设备将终端设备的子集指定给每个基本子树的每个节点，并且生成建立相互连接坐标轴上的坐标点的有向枝的有向图。



CN 101542966 B

1. 一种信息处理单元，包含：

树结构设置部分，用于

配置由 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的数个基本子树，形成 y 层分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，其中 y 是 log(n) 的约数，

将比整个树的节点 w 低的叶节点的集合定义成 Aw，

在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 上的叶节点定义成 $v^{(-i)}$ 和将位于右侧第 i 上的叶节点定义成 $v^{(+i)}$，

关于基本子树的两个叶节点 u 和 v，将集合 (u → v) 定义成 {Au，Au ∪ $Au^{(+1)}$，...，Au ∪ ... ∪ Av}，而将集合 (u ← v) 定义成 {Av，Av ∪ $Av^{(-1)}$，...，Av ∪ ... ∪ Au}，其中 v 在 u 的右侧，

当在比基本子树的节点 v 低的数个叶节点中，位于左端的叶节点被定义成 lv′ 和位于右端的叶节点被定义成 rv′ 时，

将集合 (l_{root}' → r_{root}') 和集合 (l_{root}' $^{(+1)}$ ← r_{oot}') 与顶层上的基本子树的根节点 root 相关联，

将集合 (lv′ → $rv'^{(-1)}$) 和集合 (lv′ $^{(+1)}$ ← rv′) 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，

如果每个子树的中间节点位于它的母节点左侧，将集合 (lv′ $^{(+1)}$ ← rv′) 与中间节点 v 相关联，和

如果每个子树的中间节点位于它的母节点右侧，将集合 (lv′ → $rv'^{(-1)}$) 与中间节点 v 相关联；和

有向图生成部分，用于针对各自基本子树的根节点 root 和根节点 v 以及中间节点 v 的每一个，生成包含度从左到右增大地在水平坐标轴上排列与包括在集合 (l_{root}' → r_{root}') 或集合 (lv′ → $rv'^{(-1)}$) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图、和 / 或包含度从右到左增大地在水平坐标轴上排列与包括在集合 (l_{root}' $^{(+1)}$ ← r_{root}') 或集合 (lv′ $^{(+1)}$ ← rv′) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图；

密钥生成部分，用于根据有向图生成加密内容或内容密钥的设置密钥，其中，当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，所述密钥生成部分输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

2. 按照权利要求 1 所述的信息处理单元，其中，

有向图生成部分进一步包括子树间有向枝设置部分，用于设置从与下层的基本子树相对应的有向图到与上层的基本子树相对应的有向图的有向枝。

3. 按照权利要求 2 所述的信息处理单元，其中，

子树间有向枝设置部分设置从与下层的基本子树相对应的有向图中的第一坐标点到与上层的基本子树相对应的有向图中的第二坐标点的有向枝，和

与第二坐标点相对应的子集包括与第一坐标点相对应的子集。

4. 按照权利要求 1 所述的信息处理单元，其中，

有向图生成部分包括坐标轴设置部分和有向枝设置部分，

坐标轴设置部分针对各自基本子树的根节点 root 和根节点 v 以及中间节点 v 的每一个，设置包含度从左到右增大地排列与包括在集合 ($l_{root}' \rightarrow r_{root}'$) 或集合 ($lv' \rightarrow rv'^{(-1)}$) 中的子集相对应的坐标点的第一水平坐标轴、和 / 或包含度从右到左增大地排列与包括在集合 ($l_{root}'^{(+1)} \leftarrow r_{root}'$) 或集合 ($lv'^{(+1)} \leftarrow rv'$) 中的子集相对应的坐标点的第二水平坐标轴，另外还在第一和第二水平坐标轴每一根的左端和 / 或右端上总共设置至少两个临时坐标点，和

有向枝设置部分在设置了给定整数 k 和计算出满足 $n^{(x-1)/k*y} < (rv' - lv' + 1) \leqslant n^{x/k*y}$ 的整数 x 之后，其中 k 是 $\log(n^{1/y})$ 的约数，

重复地设置从每根第一水平坐标轴上的左端坐标点开始延伸到相隔 $n^{i/(k*y)}$ 的坐标点的向右有向枝，其中 i ＝ 0 ～ x-1，

重复地设置从每根第二水平坐标轴上的右端坐标点开始延伸到相隔 $n^{i/(k*y)}$ 的坐标点的向左有向枝，其中 i ＝ 0 ～ x-1，

排除在第一和第二水平坐标轴的每一根上的临时坐标点上有头或有尾的所有有向枝，和

从到达第一和第二水平坐标轴上的每个坐标点的有向枝中排除除了最长有向枝之外的其它有向枝。

5. 按照权利要求 1 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，密钥生成部分输出与对应于该坐标点的子集 Si 相对应的设置密钥 k(Si)、和在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

6. 按照权利要求 1 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的设置密钥 k(S) 的输入，密钥生成部分输出在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的设置密钥 k(S1)、k(S2)、...、k(Sk)。

7. 按照权利要求 1 所述的信息处理单元，进一步包含：

加密部分，用于使用设置密钥加密内容或内容密钥。

8. 按照权利要求 7 所述的信息处理单元，进一步包含：

发送部分，用于将加密部分加密的内容或内容密钥发送到分别与整个树的叶节点 1 ～ n 的一些或全部相关联的终端单元。

9. 按照权利要求 1 所述的信息处理单元，进一步包含：

子集确定部分，用于当整个树的叶节点 1 ～ n 的子集被定义成 Si 时，确定允许解密使用设置密钥加密的内容或内容密钥的终端单元的集合 (N\R)，和确定满足集合 (N\R) ＝ {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm。

10. 按照权利要求 9 所述的信息处理单元，其中，

子集确定部分确定使 m 的值最小的子集 S1 ～ Sm。

11. 按照权利要求 9 所述的信息处理单元，其中，

发送部分将指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息发送到终端单元。

12. 按照权利要求 8 所述的信息处理单元，其中，

发送部分将加密部分使用分别与子集 S1 ～ Sm 相对应的设置密钥加密的内容或内容密钥发送到终端单元。

13. 一种终端单元，包含：

密钥生成部分，用于根据有向图生成解密加密内容或加密内容密钥的设置密钥，其中，有向图是通过如下步骤生成的：

配置由 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的数个基本子树，形成 y 层分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点 一致，其中 y 是 log(n) 的约数，

将比整个树的节点 w 低的叶节点的集合定义成 Aw，

在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 上的叶节点定义成 $v^{(-i)}$ 和将位于右侧第 i 上的叶节点定义成 $v^{(+i)}$，

关于基本子树的两个叶节点 u 和 v，将集合 (u → v) 定义成 $\{Au, Au \cup Au^{(+1)}, Au \cup Au^{(+1)} \cup Au^{(+2)}, \ldots, Au \cup Au^{(+1)} \ldots Av^{(-1)}, Au \cup Au^{(+1)} \ldots Av^{(-1)} \cup Av\}$，而将集合 (u ← v) 定义成 $\{Av, Av \cup Av^{(-1)}, Av \cup Av^{(-1)} \cup Av^{(-2)}, \ldots, A \cup Av^{(-1)} \ldots Au^{(+1)}, Av \cup Av^{(-1)} \ldots Au^{(+1)} \cup Au\}$，其中 v 在 u 的右侧，

当在比基本子树的节点 v 低的数个叶节点中，位于左端的叶节点被定义成 lv′ 和位于右端的叶节点被定义成 rv′ 时，

将集合 (l_{root}' → r_{root}') 和集合 ($l_{root}'^{(+1)}$ ← r_{root}') 与顶层上的基本子树的根节点相关联，

将集合 (lv′ → $rv'^{(-1)}$) 和集合 ($lv'^{(+1)}$ ← rv′) 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，

如果每个子树的中间节点 v 位于它的母节点左侧，将集合 ($lv'^{(+1)}$ ← rv′) 与中间节点 v 相关联，

如果每个子树的中间节点 v 位于它的母节点右侧，将集合 ($l\ v'$ → $rv'^{(-1)}$) 与中间节点 v 相关联，和

针对各自基本子树的根节点 root 和根节点 v 以及中间节点 v 的每一个，生成包含度从左到右增大地在水平坐标轴上排列与包括在集合 (l_{root}' → r_{root}') 或集合 (lv′ → $rv'^{(-1)}$) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图、和 / 或包含度从右到左增大地在水平坐标轴上排列与包括在集合 ($l_{root}'^{(+1)}$ ← r_{root}') 或集合 ($lv'^{(+1)}$ ← rv′) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图；以及

当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，所述密钥生成部分输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

14. 按照权利要求 13 所述的终端单元，其中，

设置从与下层的基本子树相对应的有向图到与上层的基本子树相对应的有向图的有向枝。

15. 按照权利要求 14 所述的终端单元，其中，

设置从与下层的基本子树相对应的有向图中的第一坐标点到与上层的基本子树相对应的有向图中的第二坐标点的有向枝，和

与第二坐标点相对应的子集包括与第一坐标点相对应的子集。

16. 按照权利要求 13 所述的终端单元，进一步包含：

解密部分，用于使用密钥生成部分生成的设置密钥解密加密内容或加密内容密钥。

17. 按照权利要求 13 所述的终端单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，密钥生成部分输出与对应于该坐标点的子集 Si 相对应的设置密钥 k(Si)、和与在坐标点 S 上有尾的有向枝的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

18. 按照权利要求 13 所述的终端单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的设置密钥 k(S) 的输入，密钥生成部分输出在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的设置密钥 k(S1)、k(S2)、...、k(Sk)。

19. 按照权利要求 16 所述的终端单元，其中，

解密部分使用设置密钥解密加密内容密钥，和使用解密内容密钥解密加密内容。

20. 按照权利要求 13 所述的终端单元，包含：

接收部分，用于当确定了允许解密使用设置密钥加密的内容或内容密钥的终端单元的集合 (N\R)，和确定了满足集合 (N\R) = {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm 时，接收指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息，其中，整个树的叶节点 1 ～ n 的子集被定义成 Si ；和

判定部分，用于根据接收信息判定终端单元是否属于子集 S1 ～ Sm 的某一个，并且根据判定结果判定是否允许解密加密内容。

21. 按照权利要求 20 所述的终端单元，进一步包含：

解密部分，用于使用密钥生成部分生成的设置密钥解密加密内容或加密内容密钥，

其中，当判定部分判定终端单元属于子集 S1 ～ Sm 的某一个时，解密部分使用设置密钥解密加密内容或加密内容密钥。

22. 一种信息处理方法，包含：

配置由 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的数个基本子树，形成 y 层分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致的步骤，其中 y 是 log(n) 的约数；

将比整个树的节点 w 低的叶节点的集合定义成 Aw 的步骤，

在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 上的叶节点定义成 $v^{(-i)}$ 和将位于右侧第 i 上的叶节点定义成 $v^{(+i)}$，

关于基本子树的两个叶节点 u 和 v，将集合 (u → v) 定义成 $\{Au, Au \cup Au^{(+1)}, Au \cup Au^{(+1)} \cup Au^{(+2)}, \ldots, Au \cup Au^{(+1)} \ldots Av^{(-1)}, Au \cup Au^{(+1)} \ldots Av^{(-1)} \cup Av\}$，而将集合 (u ← v) 定义成 $\{Av, Av \cup Av^{(-1)}, Av \cup Av^{(-1)} \cup Av^{(-2)}, \ldots, A \cup Av^{(-1)} \ldots Au^{(+1)}, Av \cup Av^{(-1)} \ldots Au^{(+1)} \cup Au\}$，其中 v 在 u 的右侧，

当在比基本子树的节点 v 低的数个叶节点中，位于左端的叶节点被定义成 lv′ 和位于右端的叶节点被定义成 rv′ 时，

将集合 ($l_{root}' \rightarrow r_{root}'$) 和集合 ($l_{root}' {}^{(+1)} \leftarrow r_{root}'$) 与顶层上的基本子树的根节点 root 相关联，

将集合 (lv′ → rv′ $^{(-1)}$) 和集合 (lv′ $^{(+1)}$ ← rv′) 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，

如果每个子树的中间节点位于它的母节点左侧，将集合 (lv′ $^{(+1)}$ ← rv′) 与中间节点 v 相关联，和

如果每个子树的中间节点位于它的母节点右侧，将集合 (lv′ → rv′ $^{(-1)}$) 与中间节点 v 相关联；

针对各自基本子树的根节点 root 和根节点 v 以及中间节点 v 的每一个，生成包含度从左到右增大地在水平坐标轴上排列与包括在集合 (l_{root}′ → r_{root}′) 或集合 (lv′ → rv′ $^{(-1)}$) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图、和 / 或包含度从右到左增大地在水平坐标轴上排列与包括在集合 (l_{root}′ $^{(+1)}$ ← r_{root}′) 或集合 (lv′ $^{(+1)}$ ← rv′) 中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图的步骤；和

用于根据有向图生成加密内容或内容密钥的设置密钥的步骤，其中，当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的 有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

23. 一种根据有向图生成解密加密内容或加密内容密钥的设置密钥的密钥生成方法，其中，有向图是通过如下步骤获得的：

配置由 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的数个基本子树，形成 y 层分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，其中 y 是 log(n) 的约数，

将比整个树的节点 w 低的叶节点的集合定义成 Aw，

在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 上的叶节点定义成 $v^{(-i)}$ 和将位于右侧第 i 上的叶节点定义成 $v^{(+i)}$，

关于基本子树的两个叶节点 u 和 v，将集合 (u → v) 定义成 {Au，Au ∪ $Au^{(+1)}$，Au ∪ $Au^{(+1)}$ ∪ $Au^{(+2)}$，...，Au ∪ $Au^{(+1)}$...$Av^{(-1)}$，Au ∪ $Au^{(+1)}$...$Av^{(-1)}$ ∪ Av}，而将集合 (u ← v) 定义成 {Av，Av ∪ $Av^{(-1)}$，Av ∪ $Av^{(-1)}$ ∪ $Av^{(-2)}$，...，A ∪ $Av^{(-1)}$...$Au^{(+1)}$，Av ∪ $Av^{(-1)}$...$Au^{(+1)}$ ∪ Au}，其中 v 在 u 的右侧，

当在比基本子树的节点 v 低的数个叶节点中，位于左端的叶节点被定义成 lv′ 和位于右端的叶节点被定义成 rv′ 时，

将集合 (l_{root}′ → r_{root}′) 和集合 (l_{root}′ $^{(+1)}$ ← r_{oot}′) 与顶层上的基本子树的根节点相关联，

将集合 (lv′ → rv′ $^{(-1)}$) 和集合 (lv′ $^{(+1)}$ ← rv′) 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，

如果每个子树的中间节点 v 位于它的母节点左侧，将集合 (lv′ $^{(+1)}$ ← rv′) 与中间节点 v 相关联，

如果每个子树的中间节点 v 位于它的母节点右侧，将集合 (lv′ → rv′ $^{(-1)}$) 与中间节点 v 相关联，和

针对各自基本子树的根节点 root 和根节点 v 以及中间节点 v 的每一个，生成包

含度从左到右增大地在水平坐标轴上排列与包括在集合（l_{root}' → r_{root}'）或集合（lv' → $rv'^{(-1)}$）中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图、和 / 或包含度从右到左增大地在水平坐标轴上排列与包括在集合（$l_{root}'^{(+1)}$ ← r_{root}'）或集合（$lv'^{(+1)}$ ← rv'）中的子集相对应的坐标点和设置连接坐标点的有向枝的有向图；以及

当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

24. 一种信息处理单元，包含：

有向图获取部分，用于获取如权利要求 1 所述的由数条有向枝组成的有向图，以便构成有向图的最长有向枝的一个尾部与有向图的尾部一致；和

密钥生成部分，用于根据有向图获取部分获取的有向图生成加密或解密内容或内容密钥的设置密钥；

其中，当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，所述密钥生成部分输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

25. 按照权利要求 24 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，密钥生成部分输出与对应于该坐标点的子集 S 相对应的设置密钥 k(S)、和在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

26. 按照权利要求 24 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的设置密钥 k(S) 的输入，密钥生成部分输出在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的设置密钥 k(S1)、k(S2)、...、k(Sk)。

27. 按照权利要求 24 所述的信息处理单元，进一步包含：

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

28. 按照权利要求 24 所述的信息处理单元，进一步包含：

加密部分，用于使用设置密钥加密内容或内容密钥。

29. 按照权利要求 28 所述的信息处理单元，进一步包含：

发送部分，用于将加密部分加密的内容或内容密钥发送到分别与构成给定二叉树的叶节点 1 ～ n 的一些或全部相关联的终端单元，其中 n 是自然数。

30. 按照权利要求 29 所述的信息处理单元，进一步包含：

子集确定部分，用于将叶节点 1 ～ n 的子集被定义成 Si，确定允许解密使用设置密钥加密的内容或内容密钥的终端单元的集合 (N\R)，和确定满足集合 (N\R) = {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm。

31. 按照权利要求 30 所述的信息处理单元，其中，

子集确定部分确定使 m 的值最小的子集 S1 ～ Sm。

32. 按照权利要求 29 所述的信息处理单元，其中，

发送部分将指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息发送到终端单元。

33. 按照权利要求 24 所述的信息处理单元，进一步包含 ：

解密部分，用于使用设置密钥解密内容或内容密钥。

34. 按照权利要求 33 所述的信息处理单元，进一步包含 ：

与构成给定二叉树的一个或多个叶节点 1 ～ n 相关联的接收部分，用于接收使用设置密钥加密的内容或内容密钥，其中 n 是自然数。

35. 按照权利要求 34 所述的信息处理单元，其中，

接收部分接收的加密内容或加密内容密钥可以通过与定义成叶节点 1 ～ n 的子集的集合 Si 中作为包括与自身相关联的叶节点的集合 S 的元素的叶节点相关联的一个或多个信息处理单元解密。

36. 一种处理临时有向图的信息处理单元，临时有向图是对于给定整数 k，按照满足 $n^{(x-1)/k}(rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，在第一到第四水平坐标轴上排列长度为 $n^{i/k}$ 的数条有向枝形成的，其中 i ＝ 0、1、...、x-1，

在由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树中，其中，在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左端的叶节点的号码定义成 lv，而将指定给位于右端的叶节点的号码定义成 rv，其中 n 是自然数，

对于自然数 i 和 j，其中 i ≤ j，假设将集合 (i → j) 表示成 {{i}，{i，i+1}，{i，i+1，i+2}，...，{i，i+1，...，j-1}，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 表示成 {{j}，{j，j-1}，{j，j-1，j-2}，...，{j，j-1，...，i+1}，{j，j-1，...，i+1，i}}，

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

设置与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联 和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

设置与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

设置与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

该信息处理单元包含 ：

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，用于通过留下构成临时有向图获取部分获取的临时有向图的数条有向枝当中的较长有向枝，生成有向图 ；和

密钥生成部分，用于根据有向图生成加密内容或内容密钥的设置密钥 ；

其中，当输入与有向图的某个坐标点 Si 相对应的中间密钥 t(Si) 时，所述密钥生成部分输出与尾部在与子集 Si 对应的坐标点上的有向边的头部相对应的中间密钥 t(S1)，t(S2)，...，t(Sm)。

37. 一种信息处理单元，包含 ：

有向图获取部分，用于获取通过在由数条有向枝组成的临时有向图中，留下构成临时有向图的数条有向枝当中的的较长有向枝生成的有向图，其中，所述临时有向图是如权利要求 36 所述的临时有向图，且所述较长有向枝是比如权利要求 1 所述的有向图中的有向枝更长的有向枝；和

密钥生成部分，用于根据有向图获取部分获取的有向图生成加密或解密内容或内容密钥的设置密钥；

其中，当输入与有向图的某个坐标点 Si 相对应的中间密钥 t(Si) 时，所述密钥生成部分输出与尾部在与子集 Si 对应的坐标点上的有向边的头部相对应的中间密钥 t(S1)，t(S2)，...，t(Sm)。

38. 一种信息处理单元，包含：

树结构设置部分，用于配置由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树，其中 n 是自然数，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，...，{j， j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv；

坐标轴设置部分，用于

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，并且

将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边；和

有向图生成部分，用于

通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leq n^{x/k}$ 的自然数，和

对于整数 i ＝ 0 ～ x-1 的每一个，

通过耦合长度为 $n^{i/k}$ 的一条或数条向右有向枝，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，

通过耦合长度为 $n^{i/k}$ 的一条或数条向左有向枝，形成在第二和第四水平坐标轴上的最

右坐标点上有尾的有向路径，

排除在第一到第四水平坐标轴的每一根上的临时坐标轴上有尾或有头的所有有向枝，并且

从到达第一到第四水平坐标轴上的每个坐标点的有向枝中排除除了最长有向枝之外的其它有向枝，和

通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向枝加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图；和

密钥生成部分，用于根据有向图生成加密内容或内容密钥的设置密钥；

其中，当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，所述密钥生成部分输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S 1)，t(S2)，...，t(Sk)。

39. 按照权利要求 38 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，密钥生成部分输出与对应于该坐标点的子集 S 相对应的设置密钥 k(S)、和在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

40. 按照权利要求 38 所述的信息处理单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的设置密钥 k(S) 的输入，密钥生成部分输出在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的设置密钥 k(S1)、k(S2)、...、k(Sk)。

41. 一种终端单元，包含：

密钥生成部分，用于根据有向图生成解密内容或内容密钥的设置密钥，其中，有向图是通过如下步骤生成的：

配置由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树，其中 n 是自然数，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，{i，i+1，i+2}，...，{i，i+1，...，j-1}，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，{j，j-1，j-2}，...，{j，j-1，...，i+1}，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左端的叶节点的号码设置成 l v，而将指定给位于右端的叶节点的号码设置成 rv，

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联 和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

与某个中间节点 v 相关联和含有分别与包括在集合 (l v+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐

标轴左端的坐标点的左侧上的两个临时坐标点，

将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边，

通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数，和

对于整数 i ＝ 0 ～ x-1 的每一个，

通过耦合长度为 $n^{i/k}$ 的一条或数条向右有向枝，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，

通过耦合长度为 $n^{i/k}$ 的一条或数条向左有向枝，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，

排除在第一到第四水平坐标轴的每一根上的临时坐标轴上有尾或有头的所有有向枝，并且

从到达第一到第四水平坐标轴上的每个坐标点的有向枝中排除除了最长有向枝之外的其它有向枝，和

通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向枝加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图；

其中，当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，所述密钥生成部分输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

42. 按照权利要求 41 所述的终端单元，进一步包含：

解密部分，用于使用设置密钥解密加密内容或加密内容密钥。

43. 按照权利要求 41 所述的终端单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，密钥生成部分输出与对应于该坐标点的子集 S 相对应的设置密钥 k(S)、和与在坐标点 S 上有尾的有向枝的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

44. 按照权利要求 41 所述的终端单元，其中，

响应与有向图中的某个坐标点相对应的子集 S 的设置密钥 k(S) 的输入，密钥生成部分输出在坐标点 S 上有尾的有向枝的头上的坐标点 S1、S2、...、Sk 的设置密钥 k(S1)、k(S2)、...、k(Sk)。

45. 按照权利要求 42 所述的终端单元，其中，

解密部分使用设置密钥解密加密内容密钥，和使用解密内容密钥解密加密内容。

46. 按照权利要求 41 所述的终端单元，其中，

在树的叶节点 1 ～ n 的子集被定义成 S i 的情况下，和

当确定了允许解密使用设置密钥加密的内容或内容密钥的终端单元的集合 (N\R) 时，确定满足集合 (N\R) ＝ {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm，并且接收指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息，和

终端单元包括判定部分，用于根据接收信息判定终端单元是否属于子集 S1 ～ Sm 的某一个，并且根据判定结果判定是否允许解密加密内容。

47. 按照权利要求 45 所述的终端单元，其中，

当判定终端单元属于子集 S1 ～ Sm 的某一个时，解密部分使用与终端单元所属的子集相对应的设置密钥解密内容或内容密钥。

48. 一种处理临时有向图的信息处理方法，临时有向图是对于给定整数 k，按照满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，在第一到第四水平坐标轴上排列长度为 $n^{i/k}$ 的数条有向枝形成的，其中 i ＝ 0、1、...、x-1，

在由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树中，其中，在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左端的叶节点的号码定义成 lv，而将指定给位于右端的叶节点的号码定义成 rv，其中 n 是自然数，

对于自然数 i 和 j(i ⩽ j)，假设将集合 (i → j) 表示成 {{i}，{i，i+1}，{i，i+1，i+2}，...，{i，i+1，...，j-1}，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 表示成 {{j}，{j，j-1}，{j，j-1，j-2}，...，{j，j-1，...，i+1}，{j，j-1，...，i+1，i}}，

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

设置与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

设置与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

设置与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

该信息处理方法包含 ：

临时有向图获取步骤，用于获取临时有向图 ；

有向图生成步骤，用于通过留下构成临时有向图获取部分获取的临时有向图的数条有向枝当中的较长有向枝，生成有向图 ；和

密钥生成步骤，用于根据有向图生成加密内容或内容密钥的设置密钥 ；

其中，当输入与有向图的某个坐标点 Si 相对应的中间密钥 t(Si) 时，输出与尾部在与子集 Si 对应的坐标点上的有向边的头部相对应的中间密钥 t(S1)，t(S2)，...，t(Sm)。

49. 一种信息处理方法，包含 ：

有向图获取步骤，用于获取通过在由数条有向枝组成的有向图中，留下构成临时有向图的数条有向枝当中的较长有向枝生成的有向图，其中，所述有向图是如权利要求 48 所述的有向图，且所述较长有向枝是比如权利要求 1 所述的有向图中的有向枝更长的有向枝 ；和

密钥生成步骤，用于根据有向图获取部分获取的有向图生成加密或解密内容或内容密钥的设置密钥 ；

其中，当输入与有向图的某个坐标点 Si 相对应的中间密钥 t(Si) 时，输出与尾部在与

子集 Si 对应的坐标点上的有向边的头部相对应的中间密钥 t(S1)，t(S2)，...，t(Sm)。

50. 一种信息处理方法，包含：

树结构设置步骤，用于

配置由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树，其中 n 是自然数，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，{i，i+1，i+2}，...，{i，i+1，...，j-1}，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，{j，j-1，j-2}，...，{j，j-1，...，i+1}，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv；

坐标轴设置步骤，用于

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，并且

将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临 时坐标点放置在第一临时坐标点的右边；和

有向图生成步骤，用于

通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数，和

对于整数 i ＝ 0 ～ x-1 的每一个，

通过耦合长度为 $n^{i/k}$ 的一条或数条向右有向枝，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，

通过耦合长度为 $n^{i/k}$ 的一条或数条向左有向枝，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，

排除在第一到第四水平坐标轴的每一根上的临时坐标轴上有尾或有头的所有有向枝，并且

从到达第一到第四水平坐标轴上的每个坐标点的有向枝中排除除了最长有向枝之外的其它有向枝，和

通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向枝加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图；以及

当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

51. 一种密钥生成方法，包含：

密钥生成步骤，用于根据有向图生成解密内容或内容密钥的设置密钥，其中，有向图是通过如下步骤生成的：

配置由指定号码 1 ～ n 的 n 个叶节点、根节点和与根节点和叶节点不同的数个中间节点组成的二叉树，其中 n 是自然数，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，{i，i+1，i+2}，...，{i，i+1，...，j-1}，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，{j，j-1，j-2}，...，{j，j-1，...，i+1}，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的数个叶节点中，将指定给位于左 端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv，

设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第一水平坐标轴，

与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第二水平坐标轴，

对于每个中间节点，

与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和包含度从左到右增大地排列在水平坐标轴上的坐标点的第三水平坐标轴，和

与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和包含度从右到左增大地排列在水平坐标轴上的坐标点的第四水平坐标轴，

放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，

将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边，

通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：

设置给定整数 k，

计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数，和

对于整数 i ＝ 0 ～ x-1 的每一个，

通过耦合长度为 $n^{i/k}$ 的一条或数条向右有向枝，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，

通过耦合长度为 $n^{i/k}$ 的一条或数条向左有向枝，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，

排除在第一到第四水平坐标轴的每一根上的临时坐标轴上有尾或有头的所有有向枝，并且

从到达第一到第四水平坐标轴上的每个坐标点的有向枝中排除除了最长有向枝之外的其它有向枝，和

通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向 枝加入与集

合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图；以及

当输入与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 时，输出与对应于坐标点的子集 Si 相对应的集合密钥 k(Si)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1，S2，...，Sk 的中间密钥 t(S1)，t(S2)，...，t(Sk)。

信息处理装置

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、密钥生成方法及其程序。

背景技术

[0002] 当今，与网络等上的内容分发有关的加密技术的发展引起人们越来越大的兴趣。尤其，安全地和有效地分发解密加密内容的加密密钥的方法引起人们特别的关注。一般说来，针对分发加密内容的一个分发者存在具有有效接收权的 n 个（n 是 2 或以上的自然数）接收者，并且只有存在于网络上的无多个截取者当中的 n 个接收者才能解密加密内容的机制是必不可少的。进一步，因为具有有效接收权的接收者的数量 n 随时间而变，所以需要能够灵活应付接收者的集合的变化的机制。

[0003] 更进一步，在这样机制的实现中，必然地，在分发者方面会产生与加密密钥的生成、保存和分发、内容的加密等有关的处理负担，而在接收者方面会产生与解密密钥的保存和接收、内容的解密等有关的处理负担。的确，加密分发成本的负担随着诸如信息处理设备的吞吐量、存储容量等的提高、和信息传输路径的通信速度的提高之类的各种各样最近技术发展而相应减轻。但是，由于内容分发服务的客户的数量的显著增加、和对安全得足以提防熟练的恶意截取者的加密技术的要求，由加密分发引起的处理负担随之增大。

[0004] 在这样的环境下，作为使用广播信道安全地将信息传送给分发者任意选择的一组接收者的技术，人们已经提出了诸如撤销方案和广播加密方案之类的方案。广播加密方案的一个例子是公开在如下非专利文献 1 中的加密密钥分发方案，该方案的特征是使用现有分层树结构对密钥分发方案作出密钥导出路径方面的改进。具体地说，这种接收者的集合被认为划分成多个子集的方案通过将未包括在某个子集中的接收者加入该子集中创建一个新子集，作为重复这种方法的结果，创建一条子集链，然后导出与沿着该链的每个子集相对应的加密密钥。从而，可以减少接收者保存的密钥的数量、生成解密密钥的计算量和密钥分发的通信量。

[0005] 非专利文献 1：Nattapong Attrapadung and Hideki Imai, ″ Subset Incre-mental Chain Based Broadcast Encryption with Shorter Ciphertext″，The 28thSymposium on Information Theory and Its Application(SITA2005).

发明内容

[0006] 本发明要解决的问题

[0007] 按照上述非专利文献 1 的加密密钥分发方案与诸如按照现有技术的 CD 方案（完整子树方案）和 SD 方案（子集差分方案）之类的密钥分发方案相比具有明显的优点。但是，从打算实现的实际观点来看，存在着在接收者的数量很大的情况下，接收端上的终端单元要保存的密钥的数量和在使用解密密钥解密时所需的终端单元中的计算量仍然很大的问题。

[0008] 本发明就是为了解决上面的问题而作出的，因此，本发明的目的是提供能够减少

终端单元要保存的密钥的数量和解密加密数据所需的计算量的新颖和改进信息处理单元、终端单元、信息处理方法、密钥生成方法及其程序。

[0009] 解决问题的手段

[0010] 为了解决上面的问题，按照本发明的一个方面，提供了包括如下的信息处理单元：树结构设置部分，用于配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层（y 是 log(n) 的约数）分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v（v 在 u 的右侧），将集合 (u → v) 定义成 $\{Au, Au \cup Au^{(+1)}, \ldots, Au \cup \ldots \cup Av\}$，而将集合 (u ← v) 定义成 $\{Av, Av \cup Av^{(-1)}, \ldots, Av \cup \ldots \cup Au\}$，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv′，而位于右端的叶节点被定义成 rv′ 时，将集合 $(l_{root}' \rightarrow r_{root}')$ 和集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 与顶层上的基本子树的根节点 root 相关联，将集合 $(lv' \rightarrow rv'^{(-1)})$ 和集合 $(lv'^{(+1)} \leftarrow rv')$ 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合 $(lv'^{(+1)} \leftarrow rv')$ 与中间节点 v 相关联，而如果每个子树的中间节点 v 位于它的父节点右侧，则将集合 $(lv' \rightarrow rv'^{(-1)})$ 与中间节点 v 相关联；和有向图生成部分，用于针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}' \rightarrow r_{root}')$ 或集合 $(lv' \rightarrow rv'^{(-1)})$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 或集合 $(lv'^{(+1)} \leftarrow rv')$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0011] 进一步，有向图生成部分可以进一步包括子树间有向边设置部分，用于设置从与下层的基本子树相对应的有向图到与上层的基本子树相对应的有向图的有向边。

[0012] 进一步，子树间有向边设置部分可以设置从与下层的基本子树相对应的有向图中的第一坐标点到与上层的基本子树相对应的有向图中的第二坐标点的有向边。

[0013] 与第二坐标点相对应的子集可以包括与第一坐标点相对应的子集。

[0014] 进一步，有向图生成部分可以包括坐标轴设置部分和有向边设置部分，坐标轴设置部分可以针对各个基本子树的根节点和中间节点 v 中的每一个，设置以从左到右增大的包含度排列与包括在集合 $(l_{root}' \rightarrow r_{root}')$ 或集合 $(lv' \rightarrow rv'^{(-1)})$ 中的子集相对应的坐标点的第一水平坐标轴、和 / 或包含度从右到左增大地排列与包括在集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 或集合 $(lv'^{(+1)} \leftarrow rv')$ 中的子集相对应的坐标点的第二水平坐标轴，另外还在第一和第二水平坐标轴每一根的左端和 / 或右端上总共设置至少两个临时坐标点，和有向边设置部分可以在设置了给定整数 k（k 是 $\log(n^{1/y})$ 的约数）和计算出满足 $n^{(x-1)/k*y} < (rv' - lv' + 1) \leqslant n^{x/k*y}$ 的整数 x 之后，重复地设置从每根第一水平坐标轴上的左端坐标点开始延伸到相隔 $n^{i/(k*y)}$ (i = 0 ～ x-1) 的坐标点的向右有向边，重复地设置从每根第二水平坐标轴上的右端坐标点开始延伸到相隔 $n^{i/(k*y)}$ (i = 0 ～ x-1) 的坐标点的向左有向边，排除在第一和第二水平坐标轴的每一根上的临时坐标点上有头或有尾的所有有向边，和从到达第一和第二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

的其它有向边。

[0015] 信息处理单元可以进一步包括密钥生成部分，用于根据有向图生成加密内容或内容密钥的集合密钥 (set key)。

[0016] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，输出与对应于该坐标点的子集 Si 相对应的集合密钥 k(Si)、和在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

[0017] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的集合密钥 k(S) 的输入，输出在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的集合密钥 k(S1)、k(S2)、...、k(Sk)。

[0018] 信息处理单元可以进一步包括加密部分，用于使用集合密钥加密内容或内容密钥。

[0019] 信息处理单元可以进一步包括传送部分，用于将加密部分加密的内容或内容密钥传送到分别与整个树的叶节点 1 ～ n 的一些或全部相关联的终端单元。

[0020] 信息处理单元可以进一步包括子集确定部分，用于当整个树的叶节点 1 ～ n 的子集被定义成 Si 时，确定允许解密使用集合密钥或内容密钥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 ～ Sm。

[0021] 进一步，子集确定部分可以确定使 m 的值最小的子集 S1 ～ Sm。

[0022] 进一步，传送部分可以将指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息传送到终端单元。

[0023] 进一步，传送部分可以将加密部分使用分别与子集 S1 ～ Sm 相对应的集合密钥加密的内容或内容密钥传送到终端单元。

[0024] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了包括如下的终端单元：密钥生成部分，用于根据有向图生成解密加密内容或加密内容密钥的集合密钥，其中，有向图是通过如下步骤生成的：配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层 (y 是 log(n) 的约数）分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v(v 在 u 的右侧)，将集合 (u → v) 定义成 {Au，Au ∪ $Au^{(+1)}$，...，Au ∪ ... ∪ Av}，而将集合 (u ← v) 定义成 {Av，Av ∪ $Av^{(-1)}$，...，Av ∪ ... ∪ Au}，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv′，而位于右端的叶节点被定义成 rv′ 时，将集合 (l_{root}' → r_{root}') 和集合 ($l_{root}'^{(+1)}$ ← r_{root}') 与顶层上的基本子树的根节点相关联，将集合 (lv′ → $rv'^{(-1)}$) 和集合 ($lv'^{(+1)}$ ← rv′) 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合 ($lv'^{(+1)}$ ← rv′) 与中间节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点右侧，则将集合 (lv′ → $rv'^{(-1)}$) 与中间节点 v 相关联，和针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合 (l_{root}' → r_{root}') 或集合 (lv′ → $rv'^{(-1)}$)

中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合 ($l_{root}'^{(+1)} \leftarrow r_{root}'$) 或集合 ($lv'^{(+1)} \leftarrow rv'$) 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0025] 进一步，可以设置从与下层的基本子树相对应的有向图到与上层的基本子树相对应的有向图的有向边。

[0026] 进一步，可以设置从与下层的基本子树相对应的有向图中的第一坐标点到与上层的基本子树相对应的有向图中的第二坐标点的有向边，和与第二坐标点相对应的子集可以包括与第一坐标点相对应的子集。

[0027] 终端单元可以进一步包括解密部分，用于使用密钥生成部分生成的集合密钥解密加密内容或加密内容密钥。

[0028] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，输出与对应于该坐标点的子集 S 相对应的集合密钥 k(Si)、和与在坐标点 S 上有尾的有向边的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

[0029] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的集合密钥 k(S) 的输入，输出在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的集合密钥 k(S1)、k(S2)、...、k(Sk)。

[0030] 进一步，解密部分可以使用集合密钥解密加密内容密钥，并使用解密内容密钥解密加密内容。

[0031] 进一步，终端单元可以包括接收部分，用于当确定了允许解密使用集合密钥或内容密钥加密的内容的终端单元的集合 (N\R)，并确定了满足集合 (N\R) = {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm 时，接收指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息，其中，整个树的叶节点 1 ～ n 的子集被定义成 Si ；和判定部分，用于根据接收信息判定终端单元是否属于子集 S1 ～ Sm 的某一个，并且根据判定结果判定是否允许解密加密内容。

[0032] 终端单元可以进一步包括解密部分，用于使用密钥生成部分生成的集合密钥解密加密内容或加密内容密钥，和当判定部分判定终端单元属于子集 S1 ～ Sm 的某一个时，解密部分可以使用集合密钥解密加密内容或加密内容密钥。

[0033] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了包括如下步骤的信息处理方法 ：配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层 (y 是 log(n) 的约数) 分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致 ；将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v(v 在 u 的右侧)，将集合 (u → v) 定义成 {Au，Au ∪ $Au^{(+1)}$，...，Au ∪ ... ∪ Av}，而将集合 (u ← v) 定义成 {Av，Av ∪ $Av^{(-1)}$，...，Av ∪ ... ∪ Au}，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv′ ，而位于右端的叶节点被定义成 rv′ 时，将集合 ($l_{root}' \rightarrow r_{root}'$) 和集合 ($l_{root}'^{(+1)} \leftarrow r_{root}'$) 与顶层上的基本子树的根节点 root 相关联，将集合 ($lv' \rightarrow rv'^{(-1)}$)

和集合 $(lv'^{(+1)} \leftarrow rv')$ 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合 $(lv'^{(+1)} \leftarrow rv')$ 与中间节点 v 相关联，而如果每个子树的中间节点 v 位于它的父节点右侧，则将集合 $(lv' \rightarrow rv'^{(-1)})$ 与中间节点 v 相关联；和针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}' \rightarrow r_{root}')$ 或集合 $(lv' \rightarrow rv'^{(-1)})$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 或集合 $(lv'^{(+1)} \leftarrow rv')$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0034] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了根据有向图生成解密加密内容或加密内容密钥的集合密钥的密钥生成方法，其中，有向图是通过如下步骤获得的：配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层 (y 是 log(n) 的约数）分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v(v 在 u 的右侧），将集合 $(u \rightarrow v)$ 定义成 $\{Au, Au \cup Au^{(+1)}, \ldots, Au \cup \ldots \cup Av\}$，而将集合 $(u \leftarrow v)$ 定义成 $\{Av, Av \cup Av^{(-1)}, \ldots, Av \cup \ldots \cup Au\}$，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv'，而位于右端的叶节点被定义成 rv' 时，将集合 $(l_{root}' \rightarrow r_{root}')$ 和集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 与顶层上的基本子树的根节 root 点相关联，将集合 $(lv' \rightarrow rv'^{(-1)})$ 和集合 $(lv'^{(+1)} \leftarrow rv')$ 与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合 $(lv'^{(+1)} \leftarrow rv')$ 与中间节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点右侧，则将集合 $(lv' \rightarrow rv'^{(-1)})$ 与中间节点 v 相关联，和针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}' \rightarrow r_{root}')$ 或集合 $(lv' \rightarrow rv'^{(-1)})$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 或集合 $(lv'^{(+1)} \leftarrow rv')$ 中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0035] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了使计算机执行包括如下步骤的处理的程序：配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层 (y 是 log(n) 的约数）分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致；将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v(v 在 u 的右侧），将集合 $(u \rightarrow v)$ 定义成 $\{Au, Au \cup Au^{(+1)}, \ldots, Au \cup \ldots \cup Av\}$，而将集合 $(u \leftarrow v)$ 定义成 $\{Av, Av \cup Av^{(-1)}, \ldots, Av \cup \ldots \cup Au\}$，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv'，而位于右端的叶节点被定义成 rv' 时，将集合 $(l_{root}' \rightarrow r_{root}')$ 和集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 与顶层上的基本子树的根节点 root 相关联，将集合 $(lv' \rightarrow rv'^{(-1)})$

和集合（$lv'^{(+1)} \leftarrow rv'$）与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合（$lv'^{(+1)} \leftarrow rv'$）与中间节点 v 相关联，而如果每个子树的中间节点 v 位于它的父节点右侧，则将集合（$lv' \rightarrow rv'^{(-1)}$）与中间节点 v 相关联；和针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合（$l_{root}' \rightarrow r_{root}'$）或集合（$lv' \rightarrow rv'^{(-1)}$）中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合（$l_{root}'^{(+1)} \leftarrow r_{root}'$）或集合（$lv'^{(+1)} \leftarrow rv'$）中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0036] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了使计算机执行根据有向图生成解密加密内容或加密内容密钥的集合密钥的步骤的程序，其中，有向图是通过如下步骤获得的：配置由 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的整个二叉树，并且将整个树划分成包括 $n^{1/y}$ 个叶节点的多个基本子树，以形成 y 层（y 是 log(n) 的约数）分层结构，以便下层的基本子树的根节点与上层的基本子树的叶节点一致，将比整个树的节点 w 低的叶节点的集合定义成 Aw，在基本子树的叶节点中，将位于某个叶节点 v 左侧第 i 位置上的叶节点定义成 $v^{(-i)}$，而将位于右侧第 i 位置上的叶节点定义成 $v^{(+i)}$，关于基本子树的两个叶节点 u 和 v（v 在 u 的右侧），将集合（u → v）定义成 $\{Au, Au \cup Au^{(+1)}, \ldots, Au \cup \ldots \cup Av\}$，而将集合（u ← v）定义成 $\{Av, Av \cup Av^{(-1)}, \ldots, Av \cup \ldots \cup Au\}$，当在比基本子树的节点 v 低的多个叶节点中，位于左端的叶节点被定义成 lv'，而位于右端的叶节点被定义成 rv' 时，将集合（$l_{root}' \rightarrow r_{root}'$）和集合（$l_{root}'^{(+1)} \leftarrow r_{root}'$）与顶层上的基本子树的根节 root 点相关联，将集合（$lv' \rightarrow rv'^{(-1)}$）和集合（$lv'^{(+1)} \leftarrow rv'$）与除了顶层之外的其它层上的基本子树的根节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点左侧，则将集合（$lv'^{(+1)} \leftarrow rv'$）与中间节点 v 相关联，如果每个子树的中间节点 v 位于它的父节点右侧，则将集合（$lv' \rightarrow rv'^{(-1)}$）与中间节点 v 相关联，和针对各个基本子树的根节点和中间节点 v 中的每一个，生成以从左到右增大的包含度在水平坐标轴上排列与包括在集合（$l_{root}' \rightarrow r_{root}'$）或集合（$lv' \rightarrow rv'^{(-1)}$）中的子集相对应的坐标点并设置连接坐标点的有向边的有向图、和 / 或以从右到左增大的包含度在水平坐标轴上排列与包括在集合（$l_{root}'^{(+1)} \leftarrow r_{root}'$）或集合（$lv'^{(+1)} \leftarrow rv'$）中的子集相对应的坐标点并设置连接坐标点的有向边的有向图。

[0037] 为了解决上面的问题，按照本发明的一个方面，提供了包括如下的信息处理单元：有向图获取部分，用于获取由多条有向边组成的有向图，以便构成有向图的最长有向边的一个尾部与有向图的尾部一致；和密钥生成部分，用于根据有向图获取部分获取的有向图生成加密或解密内容或内容密钥的集合密钥。

[0038] 进一步，为了解决上面的问题，按照本发明的一个方面，提供了处理临时有向图的信息处理单元，临时有向图是对于给定整数 k，按照满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，在第一到第四水平坐标轴上排列长度为 $n^{i/k}$（i ＝ 0、1、...、x-1）的多条有向边形成的，在由指定号码 1 ～ n（n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树中，其中，在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码定义成 lv，而将指定给位于右端的叶节点的号码定义成 rv，对于自然数 i 和 j（i ⩽ j），假设将集合（i → j）表示成 {{i}，{i，i+1}，...，{i，

i+1，...，j-1，j}}，而将集合（i ← j）表示成{{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，设置与根节点相关联和含有分别与包括在集合（1 → n）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，设置与根节点相关联和含有分别与包括在集合（2 ← n）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，设置与某个中间节点 v 相关联和含有分别与包括在集合（lv → rv-1）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，并设置与某个中间节点 v 相关联和含有分别与包括在集合（lv+1 ← rv）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，和该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，用于通过留下构成临时有向图获取部分获取的临时有向图的多条有向边当中的较长有向边，生成有向图；和密钥生成部分，用于根据有向图生成加密内容或内容密钥的集合密钥。

[0039] 进一步，为了解决上面的问题，按照本发明的一个方面，提供了包括如下的信息处理单元：树结构设置部分，用于配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j(i ≤ j)，将集合（i → j）定义成{{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合（i ← j）定义成{{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv；坐标轴设置部分，用于设置与根节点相关联和含有分别与包括在集合（1 → n）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合（2 ← n）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合（lv → rv-1）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合（lv+1 ← rv）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，并且将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边；和有向图生成部分，用于通过如下步骤生成分别与集合（1 → n-1）、集合（2 ← n）、集合（lv+1 → rv）和集合（lv ← rv-1）有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加入与集合（1 → n-1）有关的有向图中，生成与集合（1 → n）有关的有向图。

[0040] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案能够根据上述有向图分

发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0041] 进一步，信息处理单元可以包括密钥生成部分，用于根据有向图生成加密内容或内容密钥的集合密钥。

[0042] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(Si) 的输入，输出与对应于该坐标点的子集 S 相对应的集合密钥 k(Si)、和在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

[0043] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的集合密钥 k(S) 的输入，输出在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的集合密钥 k(S1)、k(S2)、...、k(Sk)。

[0044] 进一步，密钥生成部分可以包括初始中间密钥设置部分，用于将给定随机数设置成与每个有向图的尾部相对应的中间密钥。

[0045] 进一步，信息处理单元可以包括加密部分，用于使用集合密钥加密内容或内容密钥。

[0046] 进一步，信息处理单元可以包括传送部分，用于将加密部分加密的内容或内容密钥传送到分别与构成给定二叉树的叶节点 1 ～ n(n 是自然数）的一些或全部相关联的终端单元。

[0047] 进一步，信息处理单元可以包括子集确定部分，用于将叶节点 1 ～ n 的子集被定义成 Si，确定允许解密使用集合密钥或内容密钥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 ～ Sm。

[0048] 进一步，子集确定部分可以确定使 m 的值最小的子集 S1 ～ Sm。

[0049] 进一步，信息处理单元可以包括传送部分，用于将指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息传送到终端单元。

[0050] 信息处理单元可以进一步包括解密部分，用于使用集合密钥解密内容或内容密钥。

[0051] 信息处理单元可以进一步包括与构成给定二叉树的一个或多个叶节点 1 ～ n(n 是自然数）相关联的接收部分，用于接收使用集合密钥加密的内容或内容密钥。

[0052] 接收部分接收到的加密内容或加密内容密钥可以通过与定义成叶节点 1 ～ n 的子集的集合 Si 中作为包括与自身相关联的叶节点的集合 S 的元素的叶节点相关联的一个或多个信息处理单元解密。

[0053] 进一步，为了解决上面的问题，按照本发明的另一个方面，提供了包括如下的终端单元 :密钥生成部分，用于根据有向图生成解密内容或内容密钥的集合密钥。有向图是通过如下步骤生成的 :配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义成 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，和在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv，设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和以从左

到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边，通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图。

[0054] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案能够根据上述有向图分发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0055] 进一步，终端单元可以包括解密部分，用于使用集合密钥解密加密内容或加密内容密钥。

[0056] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的中间密钥 t(S) 的输入，输出与对应于该坐标点的子集 S 相对应的集合密钥 k(S)、和与在坐标点 S 上有尾的有向边的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。

[0057] 进一步，密钥生成部分可以响应于关于与有向图中的某个坐标点相对应的子集 S 的集合密钥 k(S) 的输入，输出在坐标点 S 上有尾的有向边的头上的坐标点 S1、S2、...、Sk 的集合密钥 k(S1)、k(S2)、...、k(Sk)。

[0058] 进一步，解密部分可以使用集合密钥解密加密内容密钥，并使用解密内容密钥解密加密内容。

[0059] 进一步，当树的叶节点 1 ～ n 的子集被定义成 Si 时，并且在确定了允许解密使用集合密钥或内容密钥加密的内容的终端单元的集合 (N\R)，确定了满足集合 (N\R) ＝ {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个子集 S1 ～ Sm，和接收到指示集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息的情况下，终端单元可以包括判定部分，用于根据接收信息判定终端单元是否属于子集 S1 ～ Sm 的某一个，并且根据判定结果判定是否允许解密加密内容。

[0060] 进一步，当判定终端单元属于子集 S1 ～ Sm 的某一个时，解密部分可以使用与终端

单元所属的子集相对应的集合密钥解密内容或内容密钥。

[0061] 进一步，为了解决上面的问题，按照本发明的又一个方面，提供了包括如下步骤的信息处理方法：有向图获取步骤，用于获取通过在由多条有向边组成的有向图中，留下构成临时有向图的多条有向边当中的较长有向边而生成的有向图；和密钥生成步骤，用于根据通过有向图获取步骤获取的有向图生成加密或解密内容或内容密钥的集合密钥。

[0062] 进一步，为了解决上面的问题，按照本发明的又一个方面，提供了处理临时有向图的信息处理方法，临时有向图是对于给定整数 k，按照满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的自然数 x，在第一到第四水平坐标轴上排列长度为 $n^{i/k}$（i ＝ 0、1、...、x-1）的多条有向边形成的，在由指定号码 1 ～ n（n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树中，其中，在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码定义成 lv，而将指定给位于右端的叶节点的号码定义成 rv，对于自然数 i 和 j（i ≤ j），假设将集合（i → j）表示成 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合（i ← j）表示成 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，设置与根节点相关联和含有分别与包括在集合（1 → n）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，设置与根节点相关联和含有分别与包括在集合（2 ← n）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，设置与某个中间节点 v 相关联和含有分别与包括在集合（lv → rv-1）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，并设置与某个中间节点 v 相关联和含有分别与包括在集合（lv+1 ← rv）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，和该信息处理方法包括临时有向图获取步骤，用于获取临时有向图；有向图生成步骤，用于通过留下构成临时有向图获取部分获取的临时有向图的多条有向边当中的较长有向边，生成有向图；和密钥生成步骤，用于根据有向图生成加密内容或内容密钥的集合密钥。

[0063] 进一步，为了解决上面的问题，按照本发明的又一个方面，提供了包括如下步骤的信息处理方法：树结构设置步骤，用于配置由指定号码 1 ～ n（n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j（i ≤ j），将集合（i → j）定义成 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合（i ← j）定义成 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv；坐标轴设置步骤，用于设置与根节点相关联和含有分别与包括在集合（1 → n）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合（2 ← n）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合（lv → rv-1）中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合（lv+1 ← rv）中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的

两个临时坐标点，并且将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边；和有向图生成步骤，用于通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图。

[0064] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案能够根据上述有向图分发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0065] 进一步，为了解决上面的问题，按照本发明的再一个方面，提供了包括如下步骤的密钥生成方法：密钥生成步骤，用于根据有向图生成解密内容或内容密钥的集合密钥。有向图是通过如下步骤生成的：配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j(i ⩽ j)，将集合 (i → j) 定义成 {{i}, {i, i+1}, ..., {i, i+1, ..., j-1, j}}，而将集合 (i ← j) 定义成 {{j}, {j, j-1}, ..., {j, j-1, ..., i+1, i}}，和在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv，设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边，通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加

入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图。

[0066] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案能够根据上述有向图分发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0067] 进一步，为了解决上面的问题，按照本发明的又一个方面，提供了使计算机实现如下功能的程序：树结构设置功能，用于配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv；坐标轴设置功能，用于设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，并且将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边；和有向图生成功能，用于通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图。

[0068] 如上所述，使用中间密钥和集合密钥的加密密钥分发方案能够根据上述有向图分发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0069] 进一步，为了解决上面的问题，按照本发明的再一个方面，提供了使计算机实现如下功能的程序：密钥生成功能，用于根据有向图生成解密内容或内容密钥的集合密钥。有向图是通过如下步骤生成的：配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、一个根节点和与根节点和叶节点不同的多个中间节点组成的二叉树，对于自然数 i 和 j(i ≤ j)，将集合 (i → j) 定义成 {{i}，{i，i+1}，...，{i，i+1，...，j-1，j}}，而将集合 (i ← j) 定义成 {{j}，{j，j-1}，...，{j，j-1，...，i+1，i}}，和在比某个中间节点 v 或某个根节点 v 低

的多个叶节点中，将指定给位于左端的叶节点的号码设置成 lv，而将指定给位于右端的叶节点的号码设置成 rv，设置与根节点相关联和含有分别与包括在集合 (1 → n) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第一水平坐标轴，与根节点相关联和含有分别与包括在集合 (2 ← n) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第二水平坐标轴，对于每个中间节点，与某个中间节点 v 相关联和含有分别与包括在集合 (lv → rv-1) 中的子集相关联和以从左到右增大的包含度排列在水平坐标轴上的坐标点的第三水平坐标轴，和与某个中间节点 v 相关联和含有分别与包括在集合 (lv+1 ← rv) 中的子集相关联和以从右到左增大的包含度排列在水平坐标轴上的坐标点的第四水平坐标轴，放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两个临时坐标点，将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点和将第二临时坐标点放置在第一临时坐标点的右边，通过如下步骤生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图：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，和对于整数 i ＝ 0 ～ x-1 中的每一个，通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成在第一和第三水平坐标轴上的最左坐标点上有尾的有向路径，通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成在第二和第四水平坐标轴上的最右坐标点上有尾的有向路径，排除在第一到第四水平坐标轴的每一根上的临时坐标点上有尾或有头的所有有向边，并且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其它有向边，和通过将在第一水平坐标轴上的第一临时坐标点上有头的长度为 1 的有向边加入与集合 (1 → n-1) 有关的有向图中，生成与集合 (1 → n) 有关的有向图。

[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能够根据上述有向图分发中间密钥和生成集合密钥，从而不会使每个用户保存的密钥的数量增加地能够减小每个用户（终端单元）在解密分发的加密信息时生成解密密钥所需的计算量的最差值。

[0071] 本发明的优点

[0072] 如上所述，按照本发明，可以减少接收端上的终端单元要保存的密钥的数量、和解密加密数据所需的计算量。

附图说明

[0073] 图 1 是示出按照本发明一个实施例的加密密钥分发系统的说明图；

[0074] 图 2 是示出按照该实施例的密钥分发服务器和终端单元的硬件配置的方块图；

[0075] 图 3 是示出按照基本方案的二叉树结构的说明图；

[0076] 图 4 是示出按照基本方案的有向图的说明图；

[0077] 图 5 是示出按照基本方案的有向图计算方法的流程图；

[0078] 图 6 是示出按照基本方案的内容密钥分发方法的流程图；

[0079] 图 7 是示出按照基本方案的集合密钥生成方法的流程图；

[0080] 图 8 是示出按照本发明第一实施例的密钥分发服务器和终端单元的功能配置的方块图；

[0081] 图 9 是示出按照该实施例的二叉树的整个树结构的说明图；

[0082] 图 10 是示出按照该实施例的有向图的说明图；

[0083] 图 11 是示出按照该实施例设置子树之间的有向边的有向图的说明图；

[0084] 图 12 是示出按照该实施例的内容密钥分发方法的流程图；

[0085] 图 13 是示出基本方案与按照该实施例的密钥分发方案之间的比较的比较图；

[0086] 图 14 是示出按照该实施例的加密密钥分发系统的一种应用的说明图；

[0087] 图 15 是示出按照该实施例的加密密钥分发系统的一种应用的说明图；

[0088] 图 16 是示出按照本发明第二实施例的信息处理单元和终端单元的配置的方块图；

[0089] 图 17 是示出按照该实施例的有向图生成方法的流程图；

[0090] 图 18 是示出按照该实施例的有向图 (k = 6) 的一个例子的说明图；和

[0091] 图 19 是示出按照该实施例的有向图 (k = 3) 的一个例子的说明图。

[0092] 标号说明

[0093] 5 网络

[0094] 10 密钥分发服务器

[0095] 20 终端设备

[0096] 100 加密密钥分发系统

[0097] 102 树结构设置部分

[0098] 104 坐标轴设置部分

[0099] 106 有向边设置部分

[0100] 108 子树间有向边设置部分

[0101] 110 有向图生成部分

[0102] 112 初始中间密钥设置部分

[0103] 114 密钥生成部分

[0104] 116 加密部分

[0105] 118 传送部分

[0106] 120 子集确定部分

[0107] 124 接收部分

[0108] 126 判定部分

[0109] 128 密钥生成部分

[0110] 130 解密部分

[0111] 202 控制器

[0112] 204 处理单元

[0113] 206 输入 / 输出接口

[0114] 208 安全存储部分

[0115] 210 主存储部分

[0116] 212 网络接口

[0117] 216 媒体接口

[0118] 218 信息媒体

[0119] 154 树结构设置部分

[0120] 156 坐标轴设置部分

[0121] 160 有向图生成部分

[0122] 162 初始中间密钥设置部分

[0123] 164 密钥生成部分

[0124] 166 加密部分

[0125] 168 传送部分

[0126] 170 子集确定部分

[0127] 174 接收部分

[0128] 176 判定部分

[0129] 178 密钥生成部分

[0130] 180 解密部分

[0131] 优选实施方式

[0132] 在下文中，将参照附图详细描述本发明的实施例。注意，在本说明书和附图中，基本上具有相同功能和配置的元件用相同标号表示，并且省略重复的说明。

[0133] [加密密钥分发系统 100 的配置]

[0134] 下文描述按照本发明一个实施例的加密密钥分发系统 100 的配置。图 1 是示出按照该实施例的加密密钥分发系统 100 的配置的说明图。

[0135] 参照图 1，加密密钥分发系统 100 包括配置成按照该实施例的信息处理单元的一个例子的密钥分发服务器 10、多个用户分别拥有的多个终端单元 20、和连接密钥分发服务器 10 和终端单元 20 的网络 5。

[0136] 网络 5 是连接密钥分发服务器 10 和终端单元 20，以便允许双向通信或单向通信的通信网络。例如，网络 5 由有线或无线、诸如因特网、电话线网络、卫星通信网络和广播信道之类的公用网络、诸如 WAN(广域网)、LAN(局域网)、IP-VPN(因特网协议 - 虚拟专用网络) 和无线 LAN 之类的租用线网络等构成。

[0137] 密钥分发服务器 10 由具有服务器功能的计算机单元等构成，它可以通过网络 5 将各种类型的信息传送到外部单元。例如，密钥分发服务器 10 可以以广播加密方案生成加密密钥，并且将加密密钥分发给终端单元 20。进一步，按照该实施例的密钥分发服务器 10 配有作为提供诸如视频分发服务和电子音乐分发服务的内容分发服务的内容分发服务器的功能，它可以将内容分发给终端单元 20。当然，密钥分发服务器 10 和内容分发服务器可以配置成分立单元。

[0138] 例如，内容可以是诸如由诸如视频、电视节目、视频节目和图表之类的运动图像或静止图像组成的视频内容、诸如音乐、演讲和无线电节目之类的音频内容、游戏内容、文档内容、软件等的任何内容数据。视频内容不仅可以包含视频数据，而且可以包含音频数据。

[0139] 终端单元 20 是能够通过网络 5 与外部单元数据通信的信息处理单元，它由每个用户拥有。尽管终端单元 20 由诸如如图所示的个人计算机 (下文称为“PC”) 的计算机单元 (笔记本型或台式) 构成，但不局限于此，它可以由诸如 PDA(个人数字助理)、家用视频游戏机、DVD/HDD(数字多功能盘 / 硬盘驱动器) 记录器和电视机的家用信息电器、电视广播调谐器或解码器等构成，只要它具有通过网络 5 的通信功能即可。进一步，终端单元 20 可以是诸如便携式视频游戏播放器、蜂窝式电话、便携式视频 / 音频播放器、PDA 和 PHS(个人手持式电话系统，俗称小灵通) 等，用户可以携带的便携式设备。

[0140] 终端单元 20 可以从密钥分发服务器 10 接收各种类型的信息。例如，终端单元 20 可以接收从密钥分发服务器 10 分发的内容。在内容分发的时候，密钥分发服务器 10 可以加密各种类型的电子数据并分发它们。例如，密钥分发服务器 10 可以生成加密内容的内容密钥并分发它。内容密钥可以用，例如，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表示。当使用内容密钥时，密钥分发服务器 10 可以通过给定加密逻辑加密内容。进一步，密钥分发服务器 10 可以将内容密钥或与内容密钥相对应的解密密钥分发给任意终端单元 20。另一方面，终端单元 20 可以使用从密钥分发服务器 10 接收到的内容密钥或与内容密钥相对应的解密密钥解密加密内容。

[0141] 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种子值输出长间隔伪随机数序列的单元或程序，一般使用诸如线性同余方法或马其赛特旋转 (Mersenne Twister) 方法的逻辑实现。可应用于该实施例的伪随机数发生器当然不局限于此，并且可以使用其它逻辑生成伪随机数，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。

[0142] 进一步，按照该实施例的密钥分发服务器 10 不仅加密内容而且加密内容密钥，并且分发它们。的确，加密和分发内容保证了某种程度的安全水平。但是，为了灵活地应付大量用户当中许可拥有使用内容的权限的用户（下文称为“许可用户”）的加入或删除，加密内容密钥并分发它的方法是较有利的。在这样的情况下，在这个实施例中，密钥分发服务器 10 首先生成加密和解密内容密钥的多个集合密钥。正如后面详细描述的那样，将多个集合密钥分别与从大量用户中提取的许可用户的多个子集相关联。具体地说，密钥分发服务器 10 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加密内容密钥，并将加密内容密钥分发给所有用户的终端单元 20。在这种配置中，只有许可用户的终端单元 20 才可以解密加密内容密钥，然后使用内容密钥解密加密内容，从而使内容可看见。在许可用户的集合发生变化的情况下，密钥分发服务器 10 可以通过改变用于加密内容密钥的集合密钥应付这种变化。为了建立上面的加密密钥分发逻辑，有必要配置密钥分发服务器 10 等，以便实现与集合密钥的生成和分发有关的算法。

[0143] 在下文中，首先描述按照该实施例的密钥分发服务器 10 和终端单元 20 的示范性硬件配置。其次，描述与按照该实施例的加密密钥分发逻辑有关的基本技术。第三，详细描述按照该实施例的密钥分发服务器 10 和终端单元 20 的配置，和具体描述在配置和效果方面与基本技术的差异。最后，描述按照该实施例的加密密钥分发系统的应用。

[0144] [密钥分发服务器 10 和终端单元 20 的硬件配置]

[0145] 在下文中，首先参照图 2，描述按照该实施例的密钥分发服务器 10 和终端单元 20 的示范性硬件配置。图 2 示出了能够实现按照该实施例的密钥分发服务器 10 和终端单元 20 的功能的硬件配置的例子。

[0146] 密钥分发服务器 10 和终端单元 20 包括，例如，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。

[0147] （控制器 202）

[0148] 控制器 202 通过总线与其它元件连接，它主要用于根据存储在主存储部分 210 中的程序和数据控制单元的每个部分。控制器 202 可以由诸如 CPU（中央处理单元）的处理单元构成。

[0149] （处理单元 204（密钥分发服务器 10））

[0150] 包括在密钥分发服务器 10 中的处理单元 204 可以进行，例如，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。因此，处理单元 204 可以起根据给定数据（种子值等）生成伪随机数的伪随机数发生器的作用，并且还根据给定算法加密内容或内容密钥。可以将给定算法存储在主存储部分 210 中作为处理单元 204 可读的程序。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 可以将执行上面处理的输出结果记录在主存储部分 210 或安全存储部分 208 中。处理单元 204 可以由诸如 CPU 的处理单元构成，或与上述的控制器 202 合并在一起形成。

[0151] （处理单元 204（终端单元 20））

[0152] 另一方面，包括在终端单元 20 中的处理单元 204 可以进行，例如，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。因此，处理单元 204 可以起根据给定数据（种子值等）生成伪随机数的伪随机数发生器的作用，并且还根据给定算法解密内容或内容密钥。可以将给定算法存储在主存储部分 210 中作为处理单元 204 可读的程序。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 可以将执行上面处理的输出结果记录在主存储部分 210 或安全存储部分 208 中。处理单元 204 可以由诸如 CPU 的处理单元构成，或与上述的控制器 202 合并在一起形成。

[0153] （输入 / 输出接口 206）

[0154] 输入 / 输出接口 206 主要与用户输入信息的输入设备和输出内容的处理结果或描述的输出设备连接。例如，输入设备可以是键盘、鼠标、跟踪球、触控笔、键板、触摸板等，它可以经由无线或有线连接到输入 / 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诸如蜂窝式电话或 PDA（个人数字助理）的电子装备。另一方面，输出设备可以是，例如，诸如显示器的显示单元、诸如扬声器的音频输出设备等，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 10 或终端单元 20 中或与它们合并在一起。

[0155] 输入 / 输出接口 206 通过总线与其它元件连接，以便它可以将经由输入 / 输出接口 206 输入的信息传送到主存储部分 210 等。相反，输入 / 输出接口 206 可以将存储在主存储部分 210 等中的信息、经由网络接口 212 等输入的信息、或通过在处理单元 204 中处理那些信息获得的结果等输出到输出设备。

[0156] （安全存储部分 208）

[0157] 安全存储部分 208 主要安全地存储诸如内容密钥、集合密钥和中间密钥，有必要隐藏的信息。安全存储部分 208 可以由，例如，诸如硬盘的磁存储单元、诸如光盘的光存储单元、磁光存储单元、半导体存储单元等构成。进一步，安全存储部分 208 可以由，例如，防窜改存储单元构成。

[0158] （主存储部分 210）

[0159] 例如，主存储部分 210 可以存储控制其它元件的控制程序、加密内容、内容密钥等的加密程序、解密加密内容、内容密钥等的解密程序、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。主存储部分 210

可以由，例如，诸如硬盘的磁存储单元、诸如光盘的光存储单元、磁光存储单元、半导体存储单元等构成。进一步，安全存储部分 208 可以与安全存储部分 208 合并在一起形成。

[0160] （网络接口 212）

[0161] 网络接口 212 与，例如，网络 5 上的另一个通信单元等连接，它是传送和接收，例如，诸如加密内容或内容密钥、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 通过总线与其它元件连接，以便可以向其它元件传送从网络 5 上的外部单元接收到的信息，或向网络 5 上的外部单元传送其它元件保存的信息。

[0162] （媒体接口 216）

[0163] 媒体接口 216 是通过可换地附在信息媒体 218 上读取和写入信息的接口，它通过总线与其它元件连接。例如，媒体接口 216 可以从所附信息媒体 218 中读取信息，并且将它传送到其它元件，或者，将其它元件供应的信息写入信息媒体 218 中。例如，信息媒体 218 可以是诸如光盘、磁盘和半导体存储器的便携式存储媒体（可换存储媒体）、在相对短距离内经由有线或无线而不是通过网络 5 连接的信息终端的存储媒体等。

[0164] 上文描述了能够实现按照该实施例的密钥分发服务器 10 和终端单元 20 的功能的硬件配置的例子。上面元件中的每一个都可以使用通用硬件构成，或可以由专用于每个元件的功能的硬件构成。从而，在实现该实施例时，可以按照技术水平改变硬件配置以便得到适当使用。进一步，上述硬件配置仅仅是一个例子，当然不局限于此。例如，控制器 202 和处理单元 204 可以由相同处理单元构成，和安全存储部分 208 和主存储部分 210 可以由相同存储单元构成。进一步，视使用而定，去掉媒体接口 216、输入 / 输出接口 206 等的配置也是可行的。在下文中，将详细描述通过具有上述硬件配置的密钥分发服务器 10 和终端单元 20 实现的加密密钥分发方案。

[0165] [按照基本技术的加密密钥分发方案]

[0166] 在提供按照该实施例的加密密钥分发方案的详细描述之前，下文将描述形成实现该实施例的基础的技术问题。通过改进如下所述的基本技术，将该实施例配置成具有更重要的优点。因此，与改进有关的技术是该实施例的特征。因此，应该注意到，尽管该实施例遵循下文所述的技术问题的基本构思，但该实施例的精髓应当合并到改进部分中，配置明显不同，在优点方面也与基本技术存在明显差异。

[0167] 将按照下文所述的基本技术的加密密钥分发方案称为基本方案。该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成多个子集，然后通过指定给每个子集的集合密钥加密内容密钥并分发它。该基本方案提供了解决有关选择哪个子集、如何生成集合密钥和如何分发集合密钥的问题，以便减少加密密钥分发的通信量、每个用户要保存的解密密钥的数量、每个用户生成解密密钥所需的计算量等的一种手段。下文参照图 3 ～ 7 描述该基本方案。

[0168] （树结构的设置）

[0169] 在该基本方案中，作为内容分发目标的终端单元（用户）的集合被认为划分成多个子集。下文参照图 3 描述按照该基本方案划分成子集的方式。尽管划分成子集的方式当然不止一种，但在该基本方案中应用使用二叉树划分成子集的方式。示意性地说，该基本方案在考虑了节点之间的位置关系之后，将给定子集指定给形成二叉树的每个节点，从而，正

如后面详细描述的那样，以给定组合综合地选择用户的子集。这样选择方法的优点可以通过如图 3 所示的二叉树的特例得到更清楚理解。下文参照图 3 描述构建二叉树的方法。

[0170] 首先，将用在下面描述中的集合定义如下。

[0171] - 所有终端单元（用户）的集合 N = {1,2,...,n}(n 是 2 的乘方）

[0172] 对于自然数 i 和 j(i ≤ j)：

[0173] -[i,j] = {i,i+1,i+2,...,j},

[0174] -(i → i) = (i ← i) = {{i}},

[0175] -(i → j) = {{i},{i,i+1},...,{i,i+1,...,j}}

[0176] = {[i,i],[i,i+1],[i,i+2],...,[i,j]}

[0177] -(i ← j) = {{j},{j,j-1},...,{j,j-1,...,i}}

[0178] = {[j,j],[j-1,j],[j-2,j],...,[i,j]}。

[0179] 在下文中，将位于二叉树 (BT) 底部的节点称为叶节点，将位于顶部的节点称为根节点，并且将位于根节点和叶节点之间的节点称为中间节点。叶节点对应于各个终端单元。进一步，为了便于描述，在下文中假设终端单元和用户是一一对应的，并且在一些情况下，与叶节点相关联的“终端单元”用措词“用户”指示。图 3 示出了 BT 的叶节点的数量是 n = 64 的例子。

[0180] 首先，以叶节点的数量是 n(= 64) 的方式创建 BT。然后，从左端开始往右将号码 1,2,...,n 指定给各个叶节点。

[0181] 接着，定义调节要指定给某个中间节点 v 的子集的索引 lv 和 rv。在比某个中间节点 v 低的叶节点当中，将指定给最左叶节点的号码定义成 lv，而将指定给最右叶节点的号码定义成 rv。注意，v 可以是指定给各个中间节点的序号。因此，中间节点 v 指示索引为 v 的 BT 的中间节点。

[0182] 然后，BT 的中间节点通过将它们分类成两个集合来定义。在 BT 的中间节点当中，将位于父节点左侧的中间节点的集合定义成 BTL，而将位于父节点右侧的中间节点的集合定义成 BTR。本文所指的父子关系指示 BT 上连接的节点的分层关系，指的是父节点位于上层，而子节点位于下层的关系。

[0183] 进一步，将与各个叶节点相关联的用户集合的子集与 BT 的根节点相关联。首先，将集合 (1 → n) 和集合 (2 ← n) 与根节点相关联。因为在根节点的下层连接着所有叶节点，所以根节点通过综合地或有选择地包括那些叶节点的集合表示。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) 包括作为其元素的子集 [1,1]、[1,2]、...、[1,64]。例如，为了表示所有用户（叶节点），可以使用子集 [1,64]，它作为集合 (1 → 64) 的元素包括在其中。进一步，为了表示除了号码为 16 的用户之外的所有其它用户，可以使用子集 [1,15] 和 [17,64]，它们分别作为集合 (1 → 64) 和集合 (2 ← 64) 包括在其中。这样，可以通过相关联的集合的子集表示位于根节点下层的叶节点（用户）的组合。

[0184] 然后，将用户的子集与 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，那些集合与 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指示那些集合。例如，关于与集合 (2 ← 4) 相关联的中间节点，在中间节点的

下层存在分别与集合 (2 ← 2) 和集合 (3 → 3) 相关联的两个中间节点，并且，号码为 1 ～ 4 的叶节点进一步与它们连接。当表示除了号码为 3 的那个除外的那些叶节点的组合时，可以通过一组子集 {[1,1][2,2]，[4,4]} 或 {[1,2]，[4,4]} 表示。虽然子集 [1,1] 和 [1,2] 是与根节点相关联的集合 (1 → 64) 的元素，但子集 [2,2] 和 [4,4] 分别是集合 (2 ← 2) 和 (2 ← 4) 的元素。

[0185] 这样，该基本方案使用二叉树 BT 定义了用户集合的子集。这种方法能够以各种各样的组合表示用户的子集。由那些子集构成的全集被叫做集合系统 (set system) Φ，并且定义成下列表达式 (1)。因此，下列表达式 (1) 数学地表示了通过上面方法构建的二叉树。

[0186] [表达式 1]

[0187] $$\Phi = \bigcup_{v \in BTL} (lv+1 \leftarrow rv) \cup \bigcup_{v \in BTR} (lv \rightarrow rv-1) \cup (1 \rightarrow n) \cup (2 \leftarrow n) \quad \cdots \quad (1)$$

[0188] 上文描述了配置调节子集的二叉树的方法。该基本方案的基本构思是对各个子集设置加密内容密钥的集合密钥，使用各个集合密钥加密内容密钥，并且将它分发给所有用户。通过像上述那样定义子集，至少调节了分类用户组合的一种手段。在下文中，将描述使用那些子集生成集合密钥的算法。

[0189] (有向图的生成)

[0190] 下文参照图 4 描述生成代表生成集合密钥的算法的有向图的方法。但是，在此之前，下文首先描述加密内容密钥的集合密钥与生成集合密钥的中间密钥之间的关系。

[0191] 正如上面简述的那样，该基本方案将特定伪随机数发生器 PRSG(伪随机序列发生器) 用于生成集合密钥。当输入与某个子集 S0 相对应的中间密钥 t(S0) 时，PRSG 输出与子集 S0 相对应的集合密钥 k(S0)、和与关于子集 S0 的子集 S1、S2、...、Sk 相对应的中间密钥 t(S1)、t(S2)、...、t(Sk)。集合 S0 和 S1、S2、...、Sk 当然是构成集合系统 Φ 的子集的某一个。因此，PRSG 是密钥生成单元。该基本方案的特征是调节 PRSG 的输入和输出之间的关系的逻辑。下文描述调节集合 S0 和集合 S1、S2、...、Sk 之间的关系的有向图。

[0192] 将用于下列描述的符号定义如下：

[0193] - 与子集 Si 相对应的中间密钥 :t(Si)

[0194] - 与子集 Si 相对应的集合密钥 :k(Si)

[0195] - 内容密钥： mek

[0196] - 伪随机数发生器： PRSG

[0197] (注意，t(S0) 的输入表达成 PRSG(t(S0)))

[0198] 另一方面，将来自 PRSG 的输出表达成

[0199] t(S1)||...||t(Sk)||k(S0) ← PRSG(t(S0))

[0200] - 有向图： H

[0201] (注意，与集合 (i ← j) 相对应的有向图表达成 H(i ← j))

[0202] - 有向边： E

[0203] - 有向路径： V

[0204] 首先，确定参数 k(k 是自然数)。为了简化起见，在本例中假设是 k|log(n)(在下文中，log 的底数是 2)。因为参数 k 最终影响终端单元 20 保存的中间密钥的数量和生成集合密钥所需的计算量，所以应该按照状况适当设置。在图 4 中，例如，设置 k ＝ 6。

[0205] 接着，下文描述画出有向图的特定方式。首先，通过例示描述与属于 BTR 的中间节点 v 相对应的有向图 H(lv → rv-1)。

[0206] (S1) 设置构建有向图 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 指定成坐标点。形成坐标点的子集 Si 以包含度从左到右越来越大的方式排列。例如，将有向图 H(5 → 7) = H({[5,5], [5,6], [5,7]}) 取作一个例子，坐标轴含有从左侧开始依次指定了子集 [5,5]、[5,6]、[5,7] 的三个坐标点。

[0207] 如果第一水平坐标轴上向右有向图 H 的起点所在的垂线是 x，则有向图 H 和垂线 y 的交点代表 [x, y]，而如果第二水平坐标轴上向左有向图 H 的起点所在的垂线是 z，则有向图 H 和垂线 y 的交点代表 [y, z]。

[0208] 此后，将用作起点的临时坐标点放置在坐标轴上最左的坐标点的左侧，并且设置成起点，而将用作终点的临时坐标点放置在坐标轴上最右的坐标点的右侧，并且设置成终点。在这样设置的坐标轴中，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 是 Lv = rv-lv+1。

[0209] (S2) 设置构建有向图 H(lv → rv-1) 的有向边。

[0210] (S2-1) 计算满足 $n^{(x-1)/k} < Lv \leqslant n^{x/k}$ 的整数 x。整数 x 满足 $1 \leqslant x \leqslant k$。

[0211] (S2-2) 通过改变从 0 到 x-1 的计数 i 进行下列操作。从水平坐标轴左端的起点开始，重复设置延伸到与该坐标点相隔 $n^{i/k}$ (i = 0 ～ x-1) 的坐标点的向右有向边（跳跃到与该坐标点相隔 $n^{i/k}$ 的坐标点），直到有向边的头部到达水平坐标轴右端的终点，或下一个设置的有向边的头部超过终点。

[0212] (S3) 删除尾部或头部在临时坐标点上的所有有向边。

[0213] (S4) 如果存在多条到达某个坐标点的有向边，则只留下最长有向边，并且删除除最长有向边之外的所有其它有向边。

[0214] 在执行了上面的步骤 (S1) ～ (S4) 之后，有向图 H(lv → rv-1) 就完成了。例如，参照作为例子的从图 4 的顶端算起的第三层上位于右侧的有向图 H(33 → 63)，有向图 H(33 → 63) 的实质是由作为拱形曲线和与拱形曲线的一端连接并沿着水平方向延伸的直线的有向边组成的线组。进一步，构成有向图 H(33 → 63) 的曲线和直线是有向边。有向边的端点与垂线之间的交点是坐标点。尽管在图 4 中未清楚地示出水平坐标轴，但水平坐标轴由垂线与有向边的端点之间的一组交点组成。进一步，在有向图 H(33 → 63) 的上面描绘了空心箭头，它指示有向边的方向。具体地说，它指示形成有向图 H(33 → 63) 的所有有向边都向右。

[0215] 以与有向图 H(lv → 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(lv+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(lv+1 ← rv) 和 H(2 ← n) 的坐标轴时，以包含度从右到左越来越大的方式将子集 Si 排列在水平坐标轴上，以便有向边的方向向左。进一步，通过将有向边 E([1,n-1], [1,n]) 加入有向图 H(1 → n-1) 中生成有向图 H(1 → n)。另一方面，通过与有向图 H(lv+1 ← rv) 相同的方法设置有向图 H(2 ← n)。

[0216] 下文将图 4 的有向图 H(1 → 64) 取作一个例子提供附加说明。首先，在有向图 H(1 → 64) 的水平坐标轴中，最左坐标点（与垂线 1 的交点）是 [1,1] = {1}，右邻的坐标点（与垂线 2 的交点）是 [1,2] = {1,2}，而进一步右邻的坐标点是 [1,3] = {1,2,3}。进

一步，正好在每个有向图的上面或下面的箭头指示形成有向图 H 的所有有向边的方向。例如，有向图 H(1 → 64) 含有从坐标点 [1,1] 到 [1,2] 的一条有向边和从坐标点 [1,2] 延伸到 [1,3] 和 [1,4] 的两条有向边。进一步，描绘在图 4 底部的黑圆点从左侧开始分别指示有向图 H(2 → 2)、H(3 → 3)、...、H(63 → 63)。

[0217] 上文描述了配置有向图 H 的方法。图 4 示出了通过上述方法画出与 BT 的中间节点和根节点相对应的有向图 H 的结果。这个例子是 n ＝ 64 和 k ＝ 6 的情况。下文描述使用有向图 H 生成集合密钥的逻辑。

[0218] （集合密钥的生成）

[0219] 如前所述，该基本方案使用指定给构成上面集合系统 Φ 的每个子集 Si 的集合密钥 k(Si) 加密内容密钥 mek 并分发它。因此，上述的有向图 H 的每个坐标点对应于由一个或多个用户组成的子集 Si，并且将集合密钥 k(Si) 指定给它。进一步，中间密钥 t(Si) 也指定给上述的每个子集 Si，并且用于生成集合密钥 k(Si)。

[0220] 顺便说一下，因为在上述有向图 H 生成时步骤 (S2-2) 的处理中的重复次数是 x，其中 1 ≤ x ≤ k，所以最多 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）的一条或不止一条有向边的目的地的坐标点的子集按与某个坐标点的接近次序（按有向边的长度次序）分别是 S1、S2、...、Sk。注意，如果源自坐标点（子集 S0）的有向边的数量是 q(q ＜ k)，将 Sq+1、Sq+2、...、Sk 当作哑元来对待，实际上不使用它们。

[0221] 该基本方案使用响应 λ 个位输入而输出 (k+1)λ 个位输出的上述 PRSG。如果输入与某个坐标点（子集 S0）相对应的中间节点 t(S0)，则 PRSG 输出与尾部在某个坐标点上的有向边的头上的坐标点（子集 S1、S2、...、Sk）相对应的中间密钥 t(S1)、t(S2)、...、t(Sk)、和子集 S0 的集合密钥 k(S0)。因此，t(S1)||...||t(Sk)||k(S0) ← PRSG(t(S0))。通过将 PRSG 的输出定界成每一个都来自左侧的 λ 个位，获得中间密钥 t(S1)、t(S2)、...、t(Sk) 和集合密钥 k(S0)。

[0222] 例如，参照图 4 的有向图 H(1 → 64) 和关注坐标点（子集 S0）＝ [1,8]（从左端算起的第 8 个坐标点），四条有向边源自坐标点 S0，它们的头部在 S1 ＝ [1,9]、S2 ＝ [1,10]、S3 ＝ [1,12] 和 S4 ＝ [1,16] 上。因此，如果将中间密钥 t(S0) 输入 PRSG 中，可以获得 k(S0)、t(S1)、t(S2)、t(S3) 和 t(S4)。进一步，如果将获得的 t(S4) 输入 PRSG 中，则可以获得与 S11 ＝ [1,17]、S12 ＝ [1,18]、S13 ＝ [1,20]、S14 ＝ [1,24] 和 S15 ＝ [1,32] 相对应的 k(S4) 和 t(S11)、t(S12)、t(S13)、t(S14) 和 t(S15)。这样，通过重复使用 PRSG 可以计算出多个集合密钥 k(Si)。

[0223] 从上面的例子中可以容易地推断，对于某个中间密钥，通过重复使用 PRSG 可以导出与从对应于某个中间密钥的坐标点延伸的有向边链可达到的坐标点相对应的中间密钥和集合密钥。于是，每个用户只需保存可以导出与包括该用户的子集相对应的所有中间密钥的最少个中间密钥。另一方面，如果生成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 的初始坐标点相对应的中间密钥，则通过使用 PRSG 重复进行处理，可以导出与有向图的其它坐标点相对应的集合密钥。

[0224] 因此，一旦建立起密钥分发系统，密钥分发系统的管理者就针对密钥分发服务器中的每个有向图 H 的初始坐标点（根），将例如 λ 个位随机数设置成中间密钥。有向图 H 的初始坐标点（根）是有向边源自但没有有向边到达的坐标点。例如，图 4 中的有向图

H(1 → 64) 的初始坐标点是水平坐标轴左端的坐标点 [1,1]。

[0225] 中间密钥用于提高安全性的目的。在需要减少集合密钥生成的处理量而不特殊需要关注安全性的情况下，不使用中间密钥地直接从某个集合密钥中计算另一个集合密钥是可行的。例如，在上例中，将子集 S0 的集合密钥 k(S0) 输入 PRSG 时的输出可以是用作各个子集 S1 ～ S4 的集合密钥的 k(S1)、k(S2)、k(S3) 和 k(S4)。

[0226] 上面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。

[0227] （中间密钥的分发）

[0228] 下文描述中间密钥从密钥分发服务器到每个用户的终端单元的分发。正如前面简述的那样，有必要将能够导出与包括用户的终端单元的所有子集相对应的集合密钥的多个中间密钥提供给每个用户的终端单元。当然，应该避免提供能够导出与不包括用户的终端单元的子集相对应的集合密钥的中间密钥，最好，就存储容量的效率而言，使所提供中间密钥的数量最少。

[0229] 据此，中间密钥的分发器提取含有用户 u 的终端单元所属的子集（下文也称为“用户 u 所属的子集”或“包括用户 u 的子集）作为一个元素的所有有向图 H。然后，如果用户 u 包括在与有向图 H 的初始坐标点（根）相对应的子集中，分发器只将与初始坐标点相对应的中间密钥提供给用户 u 的终端单元。另一方面，如果用户 u 属于与不同于有向图 H 的初始坐标点的坐标点相对应的某个子集，分发器找出这样的子集 S0，即用户 u 包括在子集 S0 中，但不包括在作为子集 S0 的父母的子集 parent(S0) 中，并且将子集 S0 的中间密钥 t(S0) 提供给用户 u 的终端单元。换句话说，如果在有向图 H 中存在与初始坐标点不同和与包括用户 u 的子集相对应的多个坐标点，分发器从那些坐标点中提取这样的坐标点 S0，即用户 u 不包括在与到达对应于子集 S0 的坐标点的有向边的尾部相对应的子集 parent(S0) 中，并且将坐标点 (S0) 的中间密钥 t(S0) 提供给用户 u 的终端单元。如果存在多个这样的坐标点 S0，提供各个坐标点的中间密钥 t(S0)。坐标点的父子关系通过有向边确定，有向边尾部的坐标点用作头部坐标点的父母，而有向边头部的坐标点用作尾部坐标点的子女。在下文中，将到达某个坐标点 S0 的有向边的尾部上的坐标点 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，而如果不是有向图 H 的起点，则只存在一个父坐标点。在一些情况下，在一个有向图 H 中，可能存在多个这样的坐标点，即用户 u 包括在与之相对应的子集中，但用户 u 不包括在与它的父坐标点相对应的子集中。

[0230] 下文参照图 4 的例子具体描述中间密钥的分发方法。

[0231] （例 1）考虑分发给用户 1 的中间密钥。首先，作为搜索含有用户 1 所属的子集作为元素的有向图 H 的结果，只找到有向图 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]。因此，只将中间密钥 t([1,1]) 提供给用户 1。

[0232] （例 2）考虑分发给用户 3 的中间密钥。首先，作为搜索含有用户 3 所属的子集作为元素的有向图 H 的结果，找到有向图 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 不属于初始坐标点上的子集 [1,1]，但属于第 3 和随后坐标点上的子集 [1,3]、[1,4]、...、[1,64]。在那些坐标点当中，父坐标点不包括用户 3 的坐标点只有 [1,3] 和 [1,4]。具体地说，用户 3 不包括在作为包括用户 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。因此，将 t([1,3]) 和 t([1,4]) 提供给用户 3 作为与有向图 H(1 → 64) 相对应的中间密钥。同样，为其它有向图 H(2 ← 64)、H(2 ← 32)、H(2 ← 16)、H(2 ← 8)、H(2 ← 4) 和 H(3 ← 3) 选择相应中间密钥并将其提供给用户 3。因此，将总共八个中间密钥提供给用户 3。

[0233] 下面参照图 5 简要总结一下直到将中间密钥分发给每个用户的终端单元为止的处理。图 5 是示出根据系统建立在密钥分发服务器中分发中间密钥的处理流程的流程图。

[0234] 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、PRSG 的伪随机数生成算法等，并且向所有用户的终端单元公布它们 (S102)。接着，密钥分发服务器将用户的集合划分成给定子集，然后确定并公布用并集表示的集合系统 Φ (参见上面表达式 (1)) (S104)。然后，密钥分发服务器确定并公布有向图 H 和形成各个有向图 H 的有向边 T(S106)。进一步，密钥分发服务器确定与构成集合系统 Φ 的各个子集相对应的中间密钥 (S108)。此后，密钥分发服务器向每个用户分发必要的中间密钥的终端单元 20，以便每个用户可以导出与包括用户的子集相对应的集合密钥 (S110)。

[0235] 上文描述了中间密钥的分发方法。如果使用上面的分发方法，则分发每个许可用户的终端单元生成集合密钥所需的最少个中间密钥，从而能够减少密钥分发服务器与终端单元之间的通信量和每个用户的终端单元中中间密钥的存储容量。

[0236] (内容密钥的分发)

[0237] 下文描述密钥分发服务器分发加密内容密钥 mek 的方法。首先，密钥分发服务器使用只能由许可用户的终端单元 20 生成的集合密钥加密内容密钥 mek。具体地说，密钥分发服务器确定要排除的用户 (下文称为“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 ～ n 的集合 N 中排除掉排除用户的终端单元的集合 R(下文称为“排除用户的集合 (R)”)，确定许可用户的终端单元的集合 N\R(下文称为“许可用户的集合 (N\R)”)。然后，用从构成集合系统 Φ 的子集中选择的子集 Si(i ＝ 1、2、...、m) 的并集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，但选择 m 的值最小的子集 Si。在以这种方式选择子集 Si 之后，密钥分发服务器使用与每个子集 Si 相对应的集合密钥 k(Si) 加密内容密钥 mek。具体地说，内容密钥 mek 被集合密钥 k(S1)、k(S2)、...、k(Sm) 加密，成为 m 个加密内容密钥 mek。然后，将 m 个加密内容密钥 mek 分发给所有用户的终端单元 1 ～ 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 的信息分发给所有用户的终端单元 1 ～ n。

[0238] 下面参照图 6 简要总结一下分发加密内容密钥 mek 的处理流程。图 6 是示出分发内容密钥的处理流程的流程图。

[0239] 如图 6 所示，密钥分发服务器首先确定排除用户的集合 (R)，并获得许可用户的集合 (N\R)(S112)。接着，密钥分发服务器以使 m 的值最小的方式从构成集合系统 Φ 的子集中选择含有 N\R 的并集的 m 个子集 Si(i ＝ 1、2、...、m)(S114)。然后，密钥分发服务器使用分别与所选子集 Si 相对应的集合密钥 k(Si) 加密内容密钥 mek(S116)。进一步，密钥分发服务器将指示许可用户的集合 (N\R) 或各个子集 Si 的信息和 m 个加密内容密钥 mek 分发给所有用户的终端单元 1 ～ n(S118)。

[0240] 上文描述了内容密钥 mek 的加密方法和分发方法。如果使用上面的加密方法，就

可以有效地选择子集 Si，以便使集合密钥的数量是最少必要个。因为从此而使用最少必要个集合密钥加密内容密钥 mek，所以可以节约加密所需的计算量，并且还减少了要分发的加密内容密钥的数量，从而减少了通信量。

[0241] （内容密钥的解密）

[0242] 下文描述每个用户的终端单元中加密内容密钥的解密处理。解密处理是这样的，终端单元根据从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 的信息和 m 个密文获取内容密钥 mek。

[0243] 终端单元从密钥分发服务器接收加密内容密钥和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。进一步，终端单元分析该信息，并且判定它是否属于 m 个子集 Si 的某一个。如果终端单元不属于某个子集，它就结束解密处理，因为它是排除用户的终端单元。另一方面，如果终端单元找出它所属的子集 Si，它就使用上述 PRSG 导出与子集 Si 相对应的集合密钥 k(Si)。PRSG 的配置与前述相同。

[0244] 在这个步骤中，如果在系统建立时事先将与上面子集 Si 相对应的中间密钥 t(Si) 从密钥分发服务器提供给终端单元，并且预先保存它，则通过将中间密钥 t(Si) 输入 PRSG 中可以导出与上面子集 Si 相对应的集合密钥 k(Si)。另一方面，如果终端单元未保存相关中间密钥 t(Si)，终端单元可以通过重复地将保存的中间密钥输入 PRSG 中导出所希望集合密钥 k(Si)。进一步，终端单元使用这样导出的集合密钥 k(Si) 解密加密内容密钥 mek。

[0245] 下面参照图 4 的例子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“1、8”被选为它所属的子集。如上所述，用户 3 的终端单元保存着子集 [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] 延伸到坐标点 [1,8] 的有向边，在尾部在坐标点 [1,4] 上的有向边当中，这个有向边具有第三短长度（跳跃距离）。因此，在将子集 [1,4] 的中间密钥 t([1,4]) 输入 PRSG 时的输出当中，从顶端算起的第三 λ 个位部分是子集 [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])，再次将它输入 PRSG 中，并且提取最后 λ 个位部分，从而获得所希望集合密钥 k([1,8])。

[0246] 同样，在用户 1 的终端单元中，假设“1,8”被选为它所属的子集。用户 1 的终端单元保存着子集 [1,1] 的中间密钥。在这样的情况下，终端单元 20 可以通过从将子集 [1,1] 的中间密钥 t([1,1]) 输入 PRSG 时的输出当中提取从顶端算起的第一 λ 个位部分（对应于中间密钥 t([1,2]))，然后从将中间密钥 t([1,2]) 输入 PRSG 时的输出当中提取从顶端算起的第二 λ 个位部分（对应于中间密钥 t([1,4]))，进一步从将中间密钥 t([1,4]) 输入 PRSG 时的输出当中提取从顶端算起的第三 λ 个位部分（对应于中间密钥 t([1,8]))，和最后从将中间密钥 t([1,8]) 输入 PRSG 时的输出当中提取最后部分（对应于集合密钥 k([1,8]))，获得所希望集合密钥 k([1,8])。

[0247] 下面参照图 7 总结一下在每个用户的终端单元中解密加密内容密钥 mek 的处理流程。图 7 是示出在每个用户的终端单元中解密内容密钥的密钥生成处理流程的流程图。

[0248] 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 个加密内容密钥 mek 和指示许可用户的集合 (N\R) 的信息或指示 m 个子集 Si(i ＝ 1、2、...、m) 的信息 (S120)。接着，终端单元根据该信息搜索它所属的子集 Si(S122)，并且判定它是否属于 m 个子集 Si 的某一个（步骤 S124)。

[0249] 结果，如果终端单元找出它所属的子集Si，它就使用上面PRSG导出与子集Si相对应的集合密钥k(Si)(S126)。PRSG的配置与前述相同。如果在建立时密钥分发服务器事先将与子集Si相对应的中间密钥t(Si)提供给终端单元，并且保存它，则它就可以通过一次性地使用PRSG导出集合密钥k(Si)。另一方面，如果终端单元未保存相关中间密钥t(Si)，它可以通过重复地使用PRSG导出所希望集合密钥k(Si)。此后，终端单元使用这样导出的集合密钥k(Si)解密加密内容密钥mek(S128)。

[0250] 另一方面，如果终端单元在步骤S124中判定它不属于子集Si的某一个，则终端单元显示和输出："它被排除在允许访问内容的终端单元之外（即，它是排除用户）"(S130)，并且结束内容密钥的解密处理。

[0251] 上文描述了终端单元中内容密钥的解密方法。上面的解密方案是使用生成中间密钥和集合密钥的PRSG以及根据有关有向图H的信息执行的。因此，有关有向图的信息和PRSG在每个用户的终端单元中也是必不可少的。但是，使用PRSG的方法能够使每个用户的终端单元要保存的中间密钥的数量最少。

[0252] 上文描述了按照该实施例的基本技术的加密密钥分发方案。通过使用基本方案，每个用户的终端单元要保存的中间密钥的数量是O(k*log(n))，和生成集合密钥所需的计算量（PRSG的操作次数）不超过$(2k-1)*(n^{1/k}-1)$。但是，如后面所述的图13(A)所示，按照基本技术的加密密钥分发方案存在每个用户的终端单元要保存的中间密钥的数量仍然很大的问题。

[0253] 进一步，解密加密内容密钥mek时终端单元所需的计算量的决定因素取决于为了导出所希望中间密钥而运行PRSG的次数。最差值用有向图H中从初始坐标点（根）到最远最后坐标点（没有有向边源自的叶）的有向边的数量（即，跳跃次数）表示。在如图4所示的例子中，为了从有向图H(1→64)的初始坐标点[1,1]到达最后坐标点[1,64]，有必要穿过11条有向边（进行11次跳跃），这意味着运行PRSG多达11次。因此，按照基本技术的加密密钥分发方案存在PRSG的运行次数很多，因此，导出中间密钥的计算量很大的另一个问题。

[0254] ＜第一实施例＞

[0255] 本发明的发明人为了解决上面的问题，进行了广泛的研究，开发出了如下所述的按照本发明实施例（第一实施例）的加密密钥分发方案。按照该实施例的加密密钥分发方案将代表所有用户的终端单元的大二叉树BT划分成多个小基本子树，以创建分层结构，并且将上面基本方案的密钥导出方法用于每个基本子树并设置基本子树之间的有向边。这样既能够减少终端单元20保存的中间密钥的数量又能够减少终端单元20中的计算量。在下文中，将详细描述实现按照该实施例的加密密钥分发方案的密钥分发服务器10和终端单元20的功能配置、和该加密密钥分发方案的特征和优点。

[0256] [密钥分发服务器10的配置]

[0257] 下文参照图8详细描述按照该实施例的密钥分发服务器10的功能配置。图8是示出按照该实施例的密钥分发服务器10和终端单元20的功能配置的方块图。

[0258] 如图8所示，密钥分发服务器10包括树结构设置部分102、坐标轴设置部分104、有向边设置部分106、子树间有向边设置部分108、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。坐标轴设置部分104、有向边设

置部分 106 和子树间有向边设置部分 108 构成有向图生成部分。进一步，树结构设置部分 102 和有向图生成部分 110 统称为密钥生成逻辑构建块。同样，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。

[0259] 下文描述构成密钥生成逻辑构建块的元件。密钥生成逻辑构建块进行与上述的 [基本技术的描述] 中（树结构的设置）和（有向图的生成）相对应的处理。

[0260] （树结构设置部分 102）

[0261] 树结构设置部分 102 通过将含有指定与 n(n 是 2 的乘方）个终端单元 20 相对应的号码 1 ～ n(n 是自然数）的 n 个叶节点的整个树 BT 划分成多个基本子树配置 y 层分层结构。这样，该实施例的特征是在树结构设置部分 102 中配置分层成基本子树的树结构。尽管为了便于描述起见，将终端单元 20 的总数 n 描述成 2 的乘方，但不局限于这样的例子，例如，如果终端单元 20 的总数不是 2 的乘方，可以配置含有超过终端单元 20 的总数的 n 个 (n 是 2 的乘方）叶节点的整个树。

[0262] 除了用在前面所述的基本技术中的参数之外，该实施例还使用指示整个树 BT 的层数的参数 y。注意，y|log(n)，即，y 是 log(n) 的约数。然后，树结构设置部分 102 使用含有 $n^{1/y}$ 个叶节点的基本子树分层代表用户的所有终端单元的二叉树结构的整个树 BT。

[0263] 整个树 BT 具有等效于前面所述的基本技术的二叉树 BT(参见图 3)、高度为 log(n) 的完整二叉树结构。整个树 BT 由指定给终端单元 20 的 n 个叶节点、在整个树 BT 的顶端的根节点、和不同于根节点和叶节点的多个中间密钥组成。另一方面，基本子树具有高度为 ((log(n))/y) 的完整二叉树结构。基本子树由 $n^{1/y}$ 个叶节点、在基本子树的顶端的根节点、和不同于根节点和叶节点的多个中间密钥组成。

[0264] 树结构设置部分 102 首先创建整个树，以便叶节点的数量 n 大于终端单元 20 的总数，并且从左端开始往右将号码 1、2、...、n 指定给各个叶节点。

[0265] 进一步，树结构设置部分 102 将上面的整个树 BT 划分成多个基本子树，以形成 y 层分层结构，并且以这样的方式组合基本子树，即使下层的基本子树的根节点与上层的子树的叶节点一致，从而构建整个树 BT。

[0266] 在图 9 中示出了这样分层树结构的特例。在图 9 的例子中，将终端单元 20 的数量设置成 n ＝ 64，并且将参数 y 设置成 y ＝ 2。如图 9 所示，将整个树 BT(高度为 6 和叶节点的数量为 64) 划分成具有双层分层结构的九个基本子树（高度为 3 和叶节点的数量为 8)。上层的基本子树的数量是 1 个，而下层的基本子树的数量是 8 个。上层的基本子树的根节点与整个树 BT 的根节点相同，而上层的基本子树的叶节点的数量是 8 个，即，a、b、c、...、h。下层的各个基本子树的根节点与上层的基本子树的叶节点 a、b、c、...、h 一致，而下层的各个基本子树的叶节点是作为上述整个树 BT 的叶节点 1 ～ 64 的一部分的八个叶节点（例如，1 ～ 8、9 ～ 16、17 ～ 24、...、57 ～ 64)。

[0267] 这样，图 9 中的符号“a、b、c、...、h”指示上层的基本子树的叶节点和下层的基本子树的根节点两者，并且还指示位于根节点的下层的叶节点的集合 :{Aa}、{Ab}、{Ac}、...、{Ah}。例如，“a”指示集合 {Aa} ＝子集 {1,2,...,8}，而“b”指示集合 {Ab} ＝子集 {9,...,16}。

[0268] 低层上的基本子树的叶节点分别对应于终端单元 20。进一步，假设在下列描述中，终端单元 20 和用户是一一对应的，并且在一些情况下，与整个树 BT 的叶节点 1 ～ n(底层

上的各个基本子树的叶节点）相关联的“终端单元 20”用措词“用户”指示。尽管图 9 示出了 BT 的叶节点的数量是 n ＝ 64 和 y ＝ 2 的例子，但不局限于这样的例子，n 的值可以像 n ＝ 4（＝ 2^2）、8（＝ 2^3）、16（＝ 2^4）、32（＝ 2^5）、128（＝ 2^7）、... 那样，是 2 的任意次方。进一步，除了如图所示的 y ＝ 2 的例子之外，分层参数 y 也可以任意设置，只要它是 log(n) 的约数即可。

[0269] 进一步，树结构设置部分 102 在考虑了节点之间的位置关系之后，将组合与用户的终端单元 20 相对应的叶节点 1 ～ n 的集合与形成如上构成的整个树 BT 的每个节点，即，每个基本子树的根节点和叶节点相关联。这样，树结构设置部分 102 还起集合关联部分的作用。下文详细描述集合的关联。

[0270] 将用在下列描述中的集合和符号定义如下。

[0271] N：所有终端单元 20（用户）的集合 {1，2，...，n} ；

[0272] Aw：位于整个树 BT 的节点 w 的下层上的叶节点的集合。在节点 w 是整个树 BT 的叶节点的情况（节点 w 是底层上的基本子树的叶节点的情况）下，Aw 只指示那些叶节点（即，节点 w 的集合）。那些叶节点统称为“属于 Aw 的叶节点的集合”；

[0273] pw：位于属于 Aw 的叶节点的集合最左侧的叶节点 ；

[0274] qw：位于属于 Aw 的叶节点的集合最右侧的叶节点 ；

[0275] [pw，qw]：{pw，pw+1，pw+2，...qw-1，qw} ；

[0276] $v^{(-i)}$：位于某个叶节点 v 的左侧第 i 位置上的每个基本子树的叶节点 ；

[0277] $v^{(+i)}$：位于某个叶节点 v 的右侧第 i 位置上的每个基本子树的叶节点 ；

[0278] 关于基本子树的两个叶节点 u，v（v 在 u 的右侧）：

[0279] 集合 (u → v) ＝ {Au，Au ∪ $Au^{(+1)}$，...，Au ∪ ... ∪ Av}

[0280] ＝ {[pu，qu]，[pu，$qu^{(+1)}$]，...，[pu，$qv^{(-1)}$]，[pu，qv]} ；

[0281] 集合 (u ← v)：{Av，Av ∪ $Av^{(-1)}$，...，Av ∪ ... ∪ Au}

[0282] lv′：位于位于基本子树的节点 v（根节点或中间节点）的下层上的多个叶节点的左端上的叶节点 ；

[0283] rv′：位于位于基本子树的节点 v（根节点或中间节点）的下层上的多个叶节点的右端上的叶节点 ；

[0284] A：从基本子树的根节点的集合中排除整个树的根节点的集合 ；

[0285] BTL：位于父节点的左侧上的基本子树的中间节点的集合 ；

[0286] BTR：位于父节点的右侧上的基本子树的中间节点的集合 ；

[0287] 本文所指的父子关系指示基本子树上连接的节点的分层关系，指的是父节点位于上层，而子节点位于下层的关系。

[0288] 当使用如上定义的集合和符号时，树结构设置部分 102 在考虑了节点之间的位置关系之后，将组合与终端单元 20 相对应的叶节点 1 ～ n 的集合与如上构成的分层整个树 BT 的每个节点，即，每个基本子树的根节点和叶节点相关联。

[0289] 具体地说，树结构设置部分 102 将集合 (l_{root}′ → r_{root}′) 和集合 (l_{root}′ $^{(+1)}$← r_{root}′) 与顶层的基本子树的根节点（对应于整个树 BT 的根节点）相关联。在图 9 中的例子中，将集合 (a → h) 和集合 (b ← h) 与上层的基本子树的根节点相关联。

[0290] 进一步，对于与底层不同的层上的基本子树的中间节点，如果每个基本子树的

中间节点 v 位于它的父节点左侧，树结构设置部分 102 将集合 $(lv'^{(+1)} \leftarrow rv')$ 与中间节点 v 相关联；另一方面，如果位于它的父节点右侧，树结构设置部分 102 将集合 $(lv' \rightarrow rv'^{(-1)})$ 与中间节点 v 相关联。在图 9 的例子中，将集合 (b ← d)、集合 (e → g)、集合 (b ← b)、集合 (c → c)、集合 (f ← f) 和集合 (g → g) 分别与上层的基本子树的六个中间节点 v 相关联。例如，因为符号 e、f 和 g 分别指示子集 {30，...，40}、子集 {41，...，48} 和子集 {49，...，56}，所以集合 (e → g) 指示那些子集 {Ae，Ae ∪ Af，Ae ∪ Af ∪ Ag} = {{30，...，40}，{33，...，48}，{33，...，56}} 的集合。

[0291] 这样，在这个实施例中，子集不是以整个树的叶节点 1 ～ n 为单位，而是以上层的基本子树的叶节点 a ～ h 为单位与基本子树的节点相关联。尽管图 9 的例子是双层分层结构，因此不存在中间层的基本子树，但如果分层结构含有，例如，三层或更多层，则子集以中间层的基本子树的叶节点为单位与中间层的基本子树的节点相关联。

[0292] 进一步，树结构设置部分 102 将集合 $(lv' \rightarrow rv'^{(-1)})$ 和集合 $(lv'^{(+1)} \leftarrow rv')$ 与不同于顶层的层上的基本子树的根节点 v 相关联。在图 9 的例子中，将两个集合与下层的八个基本子树的根节点 a、b、c、...、h 中的每一个相关联。例如，将集合 (2 ← 8) 和集合 (1 → 7) 与根节点 a 相关联。这样，两个集合与基本子树的每个根节点相关联，而不只与整个树的根节点相关联。

[0293] 更进一步，如果底层的每个基本子树的中间节点 v 位于它的父节点左侧，树结构设置部分 102 将集合 $(lv'^{(+1)} \leftarrow rv')$ 与中间节点 v 相关联，而如果位于它的父节点右侧，树结构设置部分 102 将集合 $(lv' \rightarrow rv'^{(-1)})$ 与中间节点 v 相关联。例如，将集合 (2 ← 4)、集合 (5 → 7)、和集合 (2 → 2) 等与图 9 的下层左端上的基本子树的各个中间节点相关联。

[0294] 如上所述，在按照该实施例的加密密钥分发方案中，使用分层成多个基本子树的二叉树 BT 定义用户集合的子集。这种方法能够以各种各样的组合表示用户的子集。由那些子集组成的全集被叫做集合系统 Ψ，并且定义成下列表达式 (2)。因此，下列表达式 (2) 数学地表示了通过上面方法构建的二叉树结构的整个树 BT。

[0295] [表达式 2]

[0296] $$\Psi = \bigcup_{v \in BTL \cup A} (lv'^{(+1)} \leftarrow rv') \cup \bigcup_{v \in BTR \cup A} (lv' \rightarrow rv'^{(-1)}) \cup (l_{root}' \rightarrow r_{root}') \cup (l_{root}'^{(+1)} \leftarrow r_{root}') \quad \cdots (2)$$

[0297] 上文描述了通过按照该实施例的树结构设置部分 102 配置调节用户的终端单元 20 的子集的二叉树的方法。按照该实施例的加密密钥分发方案的基本构思是对各个子集设置加密内容密钥的集合密钥，使用各个集合密钥加密内容，并且将它分发给所有用户。通过像上述那样定义子集，至少调节了分类用户组合的一种手段。在下文中，将描述使用那些子集创建有向图和根据有向图生成集合密钥的算法。

[0298] 有向图生成部分 110 创建分别对应于与树结构设置部分 102 配置的分层整个树 BT 的节点相关联的集合 $(l_{root}' \rightarrow r_{root}')$、集合 $(lv' \rightarrow rv'^{(-1)})$、集合 $(l_{root}'^{(+1)} \leftarrow r_{root}')$ 和集合 $(lv'^{(+1)} \leftarrow rv')$ 的有向图 H′。有向图 H′ 由以子集的包含度越来越大的方式依次排列与包括在那些集合中的子集相对应的坐标点的水平坐标轴、和连接水平坐标轴上的坐标点的有向边组成。

[0299] 有向图生成部分 110 包括设置每个有向图 H′ 的水平坐标轴的坐标轴设置部分 104、设置每个有向图 H′ 的水平坐标轴上的有向边的有向边设置部分 106、和另外设置与

不同基本子树相对应的有向图 H′ 之间的有向边的子树间有向边设置部分 108。下文描述有向图生成部分 110 的部件。

[0300] （坐标轴设置部分 104）

[0301] 坐标轴设置部分 104 设置以包含度从左到右越来越大的方式排列与包括在与顶层的基本子树的根节点相关联的集合（$l_{root}' \rightarrow r_{root}'$）中的各个子集相对应的坐标点的第一水平坐标轴（例如，图 10 中的 H′ (a → h) 的坐标轴）。进一步，坐标轴设置部分 104 设置以包含度从左到右越来越大的方式排列与包括在与除了顶层之外的其它层的基本子树的根节点 v 或每个基本子树的中间节点 v 相关联的集合（$lv' \rightarrow rv'^{(-1)}$）中的各个子集相对应的坐标点的第一水平坐标轴（例如，图 10 中的 H′ (e → g)、H′ (1 → 7)、H′ (5 → 7) 等的坐标轴）。

[0302] 坐标轴设置部分 104 进一步设置以包含度从右到左越来越大的方式排列与包括在与顶层的基本子树的根节点相关联的集合（$l_{root}'^{(+1)} \leftarrow r_{root}'$）中的各个子集相对应的坐标点的第二水平坐标轴（例如，图 10 中的 H′ (b ← h) 的坐标轴）。进一步，坐标轴设置部分 104 设置以包含度从右到左越来越大的方式排列与包括在与除了顶层之外的其它层的基本子树的根节点 v 或每个基本子树的中间节点 v 相关联的集合（$lv'^{(+1)} \leftarrow rv'$）中的各个子集相对应的坐标点的第二水平坐标轴（例如，图 10 中的 H′ (b ← d)、H′ (2 ← 8)、H′ (2 ← 4) 等的坐标轴）。

[0303] 如上所述，坐标轴设置部分 104 设置构建与树结构设置部分 102 配置的基本子树的各个节点相对应的有向图 H′ 的坐标轴。第一水平坐标轴是向右坐标轴，而第二水平坐标轴是向左坐标轴。因为第一和第二水平坐标轴是针对各个基本子树的根节点和中间节点 v 设置的，所以设置了数根坐标轴。

[0304] 进一步，坐标轴设置部分 104 另外还在第一和第二水平坐标轴中每一根的左端和 / 或右端上总共至少设置两个临时坐标点。在这个实施例中，例如，另外分别在第一和第二水平坐标轴每一根的左端坐标点的左侧上和右端坐标点的右侧上设置一个临时坐标点。在这样的情况下，设置在第一水平坐标轴左端上的临时坐标点在设置有向边时用作起点，而设置在第一水平坐标轴右端上的临时坐标点在设置有向边时用作终点。另一方面，设置在第二水平坐标轴左端上的临时坐标点在设置有向边时用作终点，而设置在第二水平坐标轴右端上的临时坐标点在设置有向边时用作起点。设置临时坐标点的技术不局限于上面的例子，例如，可以在第一和第二水平坐标轴的左端或右端之一上设置至少两个临时坐标点。

[0305] （有向边设置部分 106）

[0306] 有向边设置部分 106 具有在坐标轴设置部分 104 设置的坐标点之间设置形成有向图 I 的有向边的功能。

[0307] 具体地说，有向边设置部分 106 首先设置给定整数 k（其中，$k|\log(n^{1/y})$；于是，k 是 $\log(n^{1/y})$ 的约数），并且计算满足 $n^{(x-1)/k*y} < (rv' - lv' + 1) \leqslant n^{x/k*y}$ 的整数 x。

[0308] 进一步，对于具有上述第一水平坐标轴的有向图 I，有向边设置部分 106 重复地进行从每根第一水平坐标轴左端的临时坐标点（起点）开始延伸到相隔 $n^{i/(k*y)}$ ($i = 0 \sim x-1$) 的坐标点的向右有向边的设置。进一步，对于具有上述第二水平坐标轴的有向图 I，有向边设置部分 106 重复地进行从每根第二水平坐标轴右端的临时坐标点开始延伸到相隔 $n^{i/(k*y)}$ ($i = 0 \sim x-1$) 的坐标点的向左有向边的设置。

[0309] 然后，对于第一和第二水平坐标轴，有向边设置部分 106 排除尾部或头部在每一个位于坐标轴左端和右端上的临时坐标点上的所有有向边。进一步，有向边设置部分 106 从到达第一和第二水平坐标轴上的各个坐标点的有向边中排除除了最长有向边之外的其它有向边。这样，有向边设置部分 106 就在与每个基本子树的根节点和中间节点 v 相关联的每个有向图 I 的每根水平坐标轴上设置了作为连接坐标点的链条的多条有向边。

[0310] 除了叶节点的数量是 $n^{1/y}$ 之外，上面通过按照该实施例的坐标轴设置部分 104 和有向边设置部分 106 生成有向图 I 的技术基本上与按照前述的基本技术生成有向图 H 的技术相同。下文描述一个特例。作为生成有向图 I 的技术的一个例子，下文将描述与如图 9 所示的顶层的基本子树的根节点（整个树 BT 的根节点）相关联的有向图 $I(l_{root}' \rightarrow r_{root}')$ = 有向图 I(a → h) 的例子。

[0311] 与前述的基本技术一样，通过创建与集合 $(lv' \rightarrow rv'^{(-1)})$ 相对应的有向图 I(a → g)，然后加入此后的有向边 E([a, g], [a, h]) 创建作为与根节点相关联的向右图的有向图 I(a → h)。因此，首先如下创建有向图 I(a → h)。

[0312] (S10) 首先，由坐标轴设置部分 104 设置配置有向图 I(a → g) 的第一水平坐标轴。在第一水平坐标轴上，将作为集合 (a → g) 的元素的子集 Si 指定成坐标点。以包含度从左到右越来越大的方式排列形成坐标点的子集 Si。例如，在有向图 I(a → h) = H({[a,a], [a, b], . . . , [a, g]}) 中，坐标轴含有从左侧开始依次指定子集 [a, a]、[a, b]、. . . 、[a, g] 的七个坐标点。此后，坐标轴设置部分 104 在坐标轴上最左的坐标点的左侧设置用作起点的临时坐标点，以便用作起点，和在坐标轴上最右的坐标点的右侧设置用作终点的临时坐标点，以便用作终点。在这样设置的坐标轴中，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 是 Lv = rv′ -lv′ +1 = h-a+1 = 8。

[0313] (S20) 由有向边设置部分 106 设置形成有向图 I(a → g) 的有向边。

[0314] (S20-1) 计算满足 $n^{(x-1)/k*y} < (h-a+1) \leqslant n^{x/k*y}$ 的整数 x。整数 x 满足 $1 \leqslant x \leqslant k$。

[0315] (S20-2) 通过改变从 0 到 x-1 的计数 i 进行下列操作。从第一水平坐标轴左端的起点（临时坐标点）开始，重复设置延伸到与该坐标点相隔 $n^{i/(k*y)}$ (i = 0 ～ x-1) 的坐标点的向右有向边（跳跃到与该坐标点相隔 $n^{i/(k*y)}$ 的坐标点），直到有向边的头部到达水平坐标轴右端的终点（临时坐标点），或下一个设置的有向边的头部超过终点。

[0316] (S30) 删除尾部或头部在第一水平坐标轴两端上的临时坐标点上的所有有向边。

[0317] (S40) 如果存在多条到达某个坐标点的有向边，则只留下最长有向边，并且删除除最长有向边之外的所有其它有向边。

[0318] 如果执行了上面的步骤 (S10) ～ (S40)，则有向图 H(a → g) 就完成了。通过将有向边 E([a, g], [a, h]) 加入有向图 H(a → g) 中，完成有向图 H(a → h)。例如，参照图如图 10 所示的有向图 H(a → h)，设置与子集 [a,a]（如方框“a”所示）、子集 [a,b]（如方框“b”所示）、. . . 、子集 [a, h]（如方框“h”所示）相对应的坐标点、和连接那些坐标点的直线有向边或拱形弯曲有向边。尽管在图 10 中未清楚示出水平坐标轴，但水平坐标轴由坐标点与有向边的端点之间的一组交点组成。进一步，在有向图 I(a → h) 的上面描绘了向右空心箭头，它指示有向边的方向。具体地说，它指示形成有向图 H(a → h) 的所有有向边都向右。因此，在有向图 H(a → h) 中，从子集 [a, a] 的坐标点 a 开始设置到达子集 [a, b] 的坐标点 b 的一条向右有向边，而从子集 [a, b] 的坐标点 b 开始设置到达子集 [a, c] 的坐标点 c 和子

集 [a，d] 的坐标点 d 的两条向右有向边。

[0319] 以与有向图 H(a → g) 相同的方式，生成与顶层的基本子树的根节点相关联的有向图 $I(l_{root}' \overset{(+1)}{\leftarrow} r_{root}')$、和与其它基本子树的根节点或基本子树的中间节点相关联的有向图 $I(lv' \rightarrow rv' \overset{(-1)}{})$ 和有向图 $I(lv' \overset{(+1)}{\leftarrow} rv')$。注意，当设置有向图 $I(lv' \rightarrow rv' \overset{(-1)}{})$ 和有向图 $I(lv' \overset{(+1)}{\leftarrow} rv')$ 的坐标轴时，在第二水平坐标轴上以包含度从右到左越来越大的方式排列子集 Si，以便使有向边的方向向左。

[0320] 这样就生成了有向图 I。图 10 代表使用有向图 I 的如图 9 所示的集合系统 ψ。图 10 示出了 y ＝ 2 和 k ＝ 3 的情况。

[0321] 如图 10 所示的有向图 I(a → h) 和 I(b ← h) 是与顶层的基本子树的根节点相关联的有向图 I。进一步，有向图 I(b ← d) 和 I(e → g) 是与顶层的基本子树的上层中间节点相关联的有向图 I，和有向图 I(b ← b)、I(c → c)、I(f ← f) 和 I(g → g) 是与顶层的基本子树的下层中间节点相关联的有向图 I。

[0322] 进一步，有向图 I(1 → 7) 和 I(2 ← 8)、有向图 I(9 → 15) 和 I(10 ← 16)、...、和有向图 I(57 → 63) 和 I(58 ← 64) 是分别与下层的八个基本子树的根节点 v 相关联的有向图 I。有向图 I(2 ← 4)、I(5 → 7)、...、I(58 ← 60)、I(61 → 63) 是分别与下层的八个基本子树的上层中间节点 v 相关联的有向图 I。更进一步，用一个坐标点（黑圆点）指示的有向图 I(2 ← 2)、I(3 → 3)、...、I(62 ← 62)、I(63 → 63) 是分别与下层的八个基本子树的下层中间节点 v 相关联的有向图 I。

[0323] 如图 10 所示，通过将整个树 BT 划分和分层成多个基本子树和生成与之相对应的有向图 I，可以缩短每个有向图 I 的长度，并且还可以减少和缩短每个有向图 I 中有向边的数量和长度（跳跃的次数和距离）。从而，可以减少终端单元 20 要保存的密钥的数量和终端单元 20 的计算量。

[0324] （子树间有向边设置部分 108）

[0325] 如图 8 所示的子树间有向边设置部分 108 另外还在分层整个树 BT 中设置从与下层的基本子树相对应的有向图 I 到与上层的基本子树相对应的有向图 I 的有向边。具体地说，子树间有向边设置部分 108 设置从与下层的基本子树相对应的有向图 I 中的第一坐标点（例如，图 11 中有向图 I(1 → 7) 的子集 [1,7] 的坐标点）到与上层的基本子树相对应的有向图 I 中的第二坐标点（例如，图 11 中有向图 I(a → h) 的子集 [a，a] 的坐标点）的有向边。由第二坐标点表示的子集（例如，[a，a]）包括与第一坐标点相对应的子集（例如，[1,7])。

[0326] 图 11 示出了在以子集 Si 存在包含关系的方式在与不同基本子树相对应的有向图 I 之间设置有向边的情况下的有向图 I。

[0327] 如图 10 和图 11 所示，用方框“a”指示的第二坐标点的子集 [a，a] ＝ {1,2，...，8} 包括子集 {1,2,...,7}，也就是说，子集 [a，a] 是子集 [1,7] 的父集。因此，子树间有向边设置部分 108 另外还设置从与有向图 I(1 → 7) 中的子集 [1,7] 相对应的坐标点（第一坐标点）到与有向图 I(a → h) 中的子集 [a,a] 相对应的坐标点（第二坐标点）的有向边。

[0328] 同样，子树间有向边设置部分 108 另外还设置从与有向图 I(58 ← 64) 中的子集 [64,58] 相对应的坐标点（第一坐标点）到与有向图 I(b ← h) 中的子集 [h，h] 相对应的坐标点（第二坐标点）的有向边。进一步，子树间有向边设置部分 108 另外还设置从与有

向图 I(26 ← 32) 中的子集 [32,26] 相对应的坐标点（第一坐标点）到与有向图 I(b ← d) 中的子集 [d, d] 相对应的坐标点（第二坐标点）的有向边，并且另外还设置从与有向图 I(33 → 39) 中的子集 [33,39] 相对应的坐标点（第一坐标点）到与有向图 I(e → g) 中的子集 [e, e] 相对应的坐标点（第二坐标点）的有向边。更进一步，子树间有向边设置部分 108 另外还设置从与有向图 I(10 ← 16)、I(17 → 23)、I(42 ← 48)、I(49 → 55) 中的子集 [16,10]、[17,23]、[48,42]、[49,55] 相对应的坐标点（第一坐标点）到与包括上面子集的有向图 I(10 ← 16)、I(17 → 23)、I(42 ← 48)、I(49 → 55) 中的子集 [b,b]、[c,c]、[f,f]、[g,g] 相对应的坐标点（第二坐标点）的有向边。这样，通过在有向图 I 之间另外设置有向边，可以进一步减少终端单元 20 要保存的中间密钥的数量。例如，通过另外设置从有向图 I(1 → 7) 的子集 [1,7] 到有向图 I(a → h) 的子集 [a, a] 的有向边，号码为 1 ～ 7 的终端单元 20 无需保存子集 [a, a] 等的中间密钥，可以通过输入自身保存的中间密钥（例如，中间密钥 t([1,7]))，导出八个子集 [a, a]、[a, b]、...、[a, h] 的中间密钥 t([a, a])、t([a, b])、...、t([a, h])。从而减少了那些终端单元 20 保存的中间密钥 t(S) 的数量。加在其它基本子树之间的有向边也有助于减少终端单元 20 保存的中间密钥 t(S) 的数量。

[0329] 上文描述了密钥分发服务器 10 中的密钥生成逻辑构建块的部件。参照图 8，除了密钥生成逻辑构建块之外，密钥分发服务器 10 进一步包括包含初始中间密钥设置部分 112 和密钥生成部分 114 的密钥生成块、加密部分 116、传送部分 118 和子集确定部分 120。

[0330] （初始中间密钥设置部分 112）

[0331] 初始中间密钥设置部分 112 针对与基本子树的每个节点相对应的每个有向图 I，生成与有向图 I 的初始坐标点相对应的中间密钥。在含有向右第一水平坐标轴的有向图 I 中初始坐标点是位于左端的坐标点（例如，有向图 I(1 → 7) 中子集 [1,1] 的坐标点），而在含有向左第二水平坐标轴的有向图 I 中它是位于右端的坐标点（例如，有向图 I(58 ← 64) 中子集 [64,64] 的坐标点）。初始中间密钥是初始坐标点的中间密钥 t(S)。如果获得初始中间密钥，可以使用，例如，伪随机数发生器 PRSG，根据与初始中间密钥相对应的有向图 I 依次导出包括在有向图 I 中的其它坐标点的中间密钥。初始中间密钥设置部分 112 可以使用伪随机数发生器 PRSG 生成随机数并将随机数设置成中间密钥，或可以将给定数值设置成中间密钥。

[0332] （密钥生成部分 114）

[0333] 密钥生成部分 114 根据上述有向图生成部分 110 生成的有向图 I，为与有向图 I 中的坐标点相对应的每个子集 Si 生成加密内容密钥的集合密钥 k(Si)。具体地说，当输入与有向图 I 中的某个坐标点相对应的子集 S 的中间密钥 t(S0) 时，密钥生成部分 114 输出与子集 S0 相对应的集合密钥 k(S0)、和与尾部在坐标点 S 上的有向边的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。因此，对于形成有向图 I 的某条有向边，一旦输入与有向边的尾部所指坐标点相对应的给定中间密钥 t(S0)，密钥生成部分 114 就输出与该有向边的尾部所指的坐标点相对应的集合密钥 k(S0)、和与从该有向边的尾部延伸的所有至少 k 条有向边的头部相对应的中间密钥 t(S1)、t(S2)、...、t(Sk)。

[0334] 例如，密钥生成部分 114 由按照基本技术的伪随机数发生器 (PRSG) 和控制 PRSG 的控制部分组成。作为密钥生成部分 114 的 PRSG，例如，可以使用响应 λ 个位输入而输出 (k+1)λ 个位输出，以便生成集合密钥 k(Si) 的上述 PRSG。当输入与某个坐标点（子集 S0)

相对应的中间密钥 t(S0) 时，PRSG 输出与尾部在某个坐标点上的有向边的头上的坐标点（子集 S1、S2、...、Sk）相对应的中间密钥 t(S1)、t(S2)、...、t(Sk)、和子集 S0 的集合密钥 k(S0)。因此，t(S1)||...||t(Sk)||k(S0) ← PRSG(t(S0))。通过将 PRSG 的输出定界成每一个都来自左侧的 λ 个位，获得中间密钥 t(S1)、t(S2)、...、t(Sk) 和集合密钥 k(S0)。

[0335] （加密部分 116）

[0336] 加密部分 116 使用集合密钥 k(Si) 加密用于加密内容的内容密钥 mek。尽管内容密钥 mek 的数量是一个，但集合密钥 k(Si) 的数量与构成集合系统 ψ 的子集 Si 的数量相同。加密部分 116 使用与下述的子集确定部分 120 从构成集合系统 ψ 的所有子集中选择的子集相对应的集合密钥加密内容密钥。因此，加密部分 116 生成与各个集合密钥 k(Si) 相对应的加密内容密钥 mek。因此，如果所选子集的数量是 m，生成 m 个加密内容密钥 mek。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 mek 加密内容，或可以使用各个集合密钥 k(Si) 加密内容。使用集合密钥 k(Si) 加密内容的配置是该实施例的一个可替代例子。

[0337] （传送部分 118）

[0338] 传送部分 118 通过网络 5 将各种类型的信息传送给每个终端单元 20。例如，传送部分 118 将加密部分 116 使用各个集合密钥 k(Si) 加密的内容密钥 mek 传送给与整个树 BT 的叶节点 1 ～ n 相关联的所有终端单元 20。可替代地，传送部分 118 可以将使用各个集合密钥 k(Si) 加密的内容，而不是加密内容密钥 mek 传送给终端单元 20。

[0339] 进一步，传送部分 118 在建立时将中间密钥 t(S0) 分发给每个终端单元 20。例如，传送部分 118 可以参照有向图 I 将终端单元 20 所属的子集 Si 的中间密钥 t(Si) 分发给每个终端单元 20。此时，传送部分 118 可以分发最少必要个中间密钥 t，以便每个终端单元 20 可以导出它所属的所有子集 Si 的中间密钥。具体地说，传送部分 118 可以从构成集合系统 ψ 的子集中提取终端单元 20 所属的子集 Si，从与提取子集 Si 相对应的有向图 I 的坐标点中选择这样的坐标点，即终端单元 20 不包括在与到达该坐标点的有向边的尾部相对应的子集 Sj 中，并且只将与所选坐标点相对应的中间密钥 t(Sj) 分发给终端单元 20。但是，如果作为中间密钥 t(Si) 的分发目的地的终端单元 20 所属的子集 Si 对应于有向图 I 的初始坐标点，传送部分 118 可以只将与初始坐标点相对应的中间密钥 t(Si) 分发给分发目的地用户。

[0340] 更进一步，传送部分 118 还可以起将与集合系统 ψ 有关的信息（例如，有关 n、λ、k、y、PRSG 等的信息）、和与有向图 I 有关的信息（例如，有向图生成部分 110 等生成的多个有向图 I）分发给每个终端单元 20 的有向图信息分发部分的作用。具体地说，一旦输入，例如，每个中间密钥 t(Si)，传送部分 118 就可以根据有向图 I，分发与输出给定中间密钥 t(Si) 和集合密钥 k(Si) 的 PRSG 的密钥生成算法（例如，密钥生成程序）有关的信息。

[0341] 传送部分 118 对中间密钥 t(Si) 的分发可以使用与用于分发内容的那个不同的通信信道，在分发内容之前进行。例如，每个终端单元 20 的中间密钥 t(Si) 可以从密钥分发服务器 10 输出并记录在记录媒体上，而从记录媒体读取的每个终端单元 20 的中间密钥 t(Si) 可以在终端单元 20 的制造车间中制造终端单元 20 时记录到每个终端单元 20 中。

[0342] （子集确定部分 120）

[0343] 子集确定部分 120 确定应该禁止使用集合密钥 k(Si) 解密内容密钥 mek 或内容

的、要排除的终端单元 20 的集合 (R)(下文称为“排除用户的集合 (R)”),并且从指定给整个树 BT 的叶节点 1 ～ n 的所有终端单元 20 的集合 (N) 中删除排除用户的集合 (R),从而确定允许使用集合密钥 k(Si) 解密内容密钥 mek 或内容的终端单元 20 的集合 (N\R)(下文称为“许可用户的集合 (N\R)”)。进一步,子集确定部分 120 确定满足许可用户的集合 (N\R) = {S1 ∪ S2 ∪ ... ∪ Sm} 的 m 个 (m 是自然数) 子集 S1 ～ Sm,以便使 m 是最小值。

[0344] 子集确定部分 120 可以由确定许可用户的集合 (N\R) 的许可用户集合确定部分和确定构成许可用户的集合 (N\R) 的一组子集 Si 的许可用户子集确定部分组成。通过将子集 Si 确定成使 m 的值最小,可以减少要保存的中间密钥 t(Sm) 和集合密钥 k(Sm) 的数量和生成那些密钥所需的计算量。

[0345] 在子集确定部分 120 以上面的方式确定了满足许可用户的集合 (N\R) = {S1 ∪ S2 ∪ ... ∪ Sm} 的子集 (S1、S2、...、Sm) 之后,传送部分 118 将标识允许解密内容密钥 mek 的终端单元 20 的许可终端标识信息等传送给每个终端单元 20。例如,许可终端标识信息可以是指示许可用户的集合 (N\R) 的信息、指示排除用户的集合 (R) 的信息、指示构成许可用户的集合 (N\R) 的子集 (S1、S2、...、Sm) 的信息、指示用于加密内容密钥 mek 的一个或不止一个集合密钥 k(Si) 的信息等。根据许可终端标识信息,终端单元 20 可以判定它是否被排除。

[0346] 进一步,加密部分 116 使用与子集确定部分 120 确定的子集 (S1、S2、...、Sm) 相对应的集合密钥加密内容密钥 mek,并且将加密内容密钥 mek 传送给每个终端单元 20。

[0347] 上文描述了按照本发明优选实施例的密钥分发服务器 10 的配置。如上所述,该配置的特征主要是密钥生成逻辑构建块的配置。尤其,该实施例具有生成决定密钥生成逻辑的有向图 I 的子树间有向边设置部分 108 配置含有基本子树的分层结构的特征。按照该实施例的子树间有向边设置部分 108 可以生成能够减少每个终端单元 20 要保存的中间密钥 t(Si) 的数量,但不会使用户的每个终端单元 20 生成集合密钥 k(Si) 所需的计算量增大的密钥生成逻辑 (有向图)。因此,可以节约每个终端单元 20 保存中间密钥 t(Si) 所需的存储容量,和降低将中间密钥 t(Si) 分发给终端单元 20 的分发成本。

[0348] 上文描述了密钥分发服务器 10 的部件的功能配置。尽管在这个实施例中通过在密钥分发服务器 10 中安装实现上面功能的程序来配置密钥分发服务器 10 的部件,但不局限于这样的例子,一些或所有部件可以由专用硬件构成。程序可以存储在诸如便携式存储媒体的计算机可读存储媒体中并提供给密钥分发服务器 10,或可以通过诸如网络 5 的通信信道从外部单元传送到密钥分发服务器 10。

[0349] [终端单元 20 的配置]

[0350] 下文参照图 8 描述按照该实施例的终端单元 20 的功能配置。图 8 是示出按照该实施例的终端单元 20 的功能配置的方块图。

[0351] 如图 8 所示,终端单元 20 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。终端单元 20 被指定给整个树底部上的叶节点 1 ～ n 的某一个。

[0352] (接收部分 124)

[0353] 接收部分 124 通过网络 5 接收从包括在密钥分发服务器 10 中的传送部分 118 传送的各种类型的信息。例如,接收部分 124 从密钥分发服务器 10 接收通过内容密钥 mek 或每个集合密钥 k(Si) 加密的内容、通过每个集合密钥 k(Si) 加密的内容密钥 mek、给定一个

或不止一个中间密钥 t(Si)、与集合系统 ψ 或有向图 I 有关的信息、上述的许可终端标识信息（例如，指示许可用户的集合 (N\R) 的信息、指示构成许可用户的集合 (N\R) 的子集 (S1、S2、...、Sm) 的信息等）等。

[0354] 进一步，接收部分 124 可以从多个信息源中收集信息，而不仅从单个信息源接收信息。例如，接收部分 124 可以从有线或无线地通过网络 5 连接的多个信息源（例如，密钥分发服务器 10）或不通过网络 5 地直接或间接连接的信息源（例如，像光盘单元、磁盘单元和便携式终端单元那样的信息媒体）中获取信息。因为接收部分 124 当然可以从另一个终端单元 20 接收信息，所以可以配置成与属于，例如，相同分发目的地组的其它终端单元 20 共享有向图 I 的信息。在这样的情况下，相同分发目的地组指的是授权成从，例如，与上述的整个树 BT 的叶节点 1 ～ n 的某一个相对应的同一个或多个密钥分发服务器 10 分发的内容的观众用户组的一组多个终端单元 20。如前所述，可以事先将中间密钥提供给终端单元 20，并且由终端单元 20 保存。

[0355] （判定部分 126）

[0356] 当接收部分 124 接收到许可终端标识信息时，判定部分 126 根据接收到的许可终端标识信息判定终端单元 20 是否属于包括在许可用户的集合 (N\R) 中的子集 S1 ～ Sm 的某一个。许可终端标识信息是指示许可用户的集合 (N\R) 的信息、指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息等。根据判定结果，判定部分 26 进一步判定是否允许终端单元 20 解密加密内容。

[0357] 因此，终端单元 20 只保存生成与它所属的子集 Si 相对应的集合密钥 k(Si) 的中间密钥 t(Si)。从而，有必要根据来自密钥分发服务器 10 的指示许可用户的集合 (N\R) 的信息或指示构成集合 (N\R) 的子集 S1 ～ Sm 的信息，事先判定终端单元 20 所属的子集 Si 是否包括在构成集合 (N\R) 的子集 S1 ～ Sm 中。该判定是由判定部分 126 作出的。例如，除了上述信息之外，用于判定的从密钥分发服务器 10 接收到的信息还可以是指示用于加密内容密钥 mek 的一个或不止一个集合密钥 k(Sj) 的信息。

[0358] 许可终端标识信息等是事先或与内容密钥 mek 同时从密钥分发服务器 10 分发的，并且被接收部分 124 接收。如果判定终端单元 20 所属的子集 Si 未包括在构成许可用户的集合 (N\R) 的子集 S1 ～ Sm 中，终止内容密钥 mek 的解密处理，因为不能进行从终端单元 20 保存的中间密钥 t(Si) 中生成集合密钥 k(Si) 的处理。相反，如果判定终端单元 20 所属的子集 Si 包括在终端单元 20 所属的子集 S1 ～ Sm 中，终端单元 20 的密钥生成部分 128 使用 PRSG 从自身保存的中间密钥 t(Si) 中生成集合密钥 k(Si)。

[0359] （密钥生成部分 128）

[0360] 密钥生成部分 128 根据从密钥分发服务器 10 接收到的有向图 I 等的信息，生成解密加密内容或内容密钥 mek 的集合密钥。密钥生成部分 128 根据从密钥分发服务器 10 接收到的有向图 I 等的信息，为与有向图 I 内的坐标点相对应的每个子集 Si 生成加密内容密钥 mek 的集合密钥 k(Si)。具体地说，当输入与有向图 I 中的某个坐标点相对应的子集 S 的中间密钥 t(S0) 时，密钥生成部分 128 输出与子集 S0 相对应的集合密钥 k(S0)、和与尾部在坐标点 S 上的每条有向边的头上的坐标点相对应的子集 S1、S2、...、Sk 的中间密钥 t(S1)、t(S2)、...、t(Sk)。密钥生成部分 128 基本上具有与上述的密钥分发服务器 10 的密钥生成部分 114 相同的功能配置，因此省略对它的详细描述。

[0361] （解密部分 130）

[0362] 解密部分 130 使用集合密钥 k(Si) 解密内容密钥 mek。具体地说，解密部分 130 从与集合密钥 k(Si) 相对应的子集 Si 中提取作为一个元素包括在其中的子集 Sii，并且使用与子集 Sii 相对应的集合密钥 k(Sii) 解密内容密钥 mek。

[0363] 上文描述了终端单元 20 的部件的功能配置。尽管在这个实施例中通过在终端单元 20 中安装实现上面功能的程序来配置终端单元 20 的部件，但不局限于这样的例子，一些或所有部件可以由专用硬件构成。程序可以存储在诸如便携式存储媒体的计算机可读存储媒体中并提供给终端单元 20，或可以通过诸如网络 5 的通信信道从外部单元传送到终端单元 20。

[0364] 如上所述，按照该实施例的终端单元 20 可以根据包括在上述密钥分发服务器 10 中的有向图生成部分 110 生成的特殊密钥生成逻辑（有向图 I）生成所希望集合密钥 k(Si)。因此，终端单元 20 可以减少为生成用于解密内容密钥 mek 等的集合密钥 k(Si) 而保存的中间密钥 t(Si) 的数量。进一步，因为由于上述的整个树 BT 的分层结果，有效地设置了有向图 I 中的有向边，所以可以减少密钥生成部分 128 生成集合密钥 k(Si) 的计算量。

[0365] [密钥分发服务器 10 和终端单元 20 的操作]

[0366] （中间密钥的分发）

[0367] 下文将描述将中间密钥从密钥分发服务器 10 分发给每个用户的终端单元 20 的操作。如上所述，为了灵活地应付大量排除用户和许可用户的加入 / 删除，有必要将能够导出与终端单元 20 包括在其中的所有子集 Si 相对应的集合密钥 k(Si) 的多个中间密钥 t(Si) 提供给每个终端单元 20。当然，应该避免提供能够导出与终端单元 20 不包括在其中的子集 Si 相对应的集合密钥 k(Si) 的中间密钥 t(Si)，最好，就终端单元 20 存储容量的效率而言，使所提供中间密钥 t(Si) 的数量最少。

[0368] 因此，当根据密钥分发系统 100 的建立将中间密钥 t(Si) 从密钥分发服务器 10 分发给终端单元 20 时，提取含有每个终端单元 20 所属的子集 Si 作为元素的所有有向图 I。然后，如果终端单元 20 包括在与有向图 I 的初始坐标点（根）相对应的子集 Si 中，只将与初始坐标点相对应的中间密钥 t(Si) 提供给终端单元 20。另一方面，如果终端单元 20 属于与不同于有向图 I 的初始坐标点的坐标点相对应的子集 Si 的某一个，找出这样的子集 S0，即终端单元 20 包括在子集 S0 中，但不包括在作为子集 S0 的父母的子集 parent(S0) 中，并且将子集 S0 的中间密钥 t(S0) 提供给终端单元 20。如果存在多个这样的子集 S0，提供各个子集的中间密钥 t(S0)。子集 Si 的父子关系通过有向边确定，有向边尾部的坐标点用作头部坐标点的父母，而有向边头部的坐标点用作尾部坐标点的子女。在下文中，将到达某个坐标点 S0 的有向边的尾部上的坐标点 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，而如果不是有向图 H 的起点，则只存在一个父坐标点。在一些情况下，在一个有向图 H 中，可能存在多个这样的坐标点，即用户 u 包括在与之相对应的子集中，但用户 u 不包括在与它的父坐标点相对应的子集中。

[0369] 下文参照图 11 的例子具体描述中间密钥的分发方法。

[0370] （例 1）考虑分发给用户 1 的终端单元 20 的中间密钥 t(Si)。首先，作为搜索含有用户 1 所属的子集 Si 作为元素的有向图 I 的结果，找到有向图 I(1 → 7) 和有向图 I(a → h)。用户 1 的终端单元 20 属于作为有向图 I(1 → 7) 的初始坐标点的子集 [1,1]。因此，将中间

密钥 t([1,1]) 提供给用户 1。

[0371] 虽然用户 1 的终端单元 20 属于有向图 I(a → h) 的子集 [a, a],但因为从有向图 I(1 → 7) 到有向图 I(a → h) 设置了图间有向边,所以如果保存了中间密钥 t([1,1]),用户 1 的终端单元 20 可以根据有向图 I(1 → 7) 和图间有向边导出中间密钥 t([a, a])。因此,没有必要将中间密钥 t([a, a]) 提供给用户 1 的终端单元 20。于是,用户 1 的终端单元 20 保存的中间密钥只是中间密钥 t([1,1])。

[0372] 与用户 1 的终端单元 20 一样,对于有向图 I(1 → 7),将子集 [1,7] = {1,2, ..., 7} 的中间密钥或能够使用 PRSG 导出子集 [1,7] 的中间密钥的中间密钥提供给用户 1 ～ 7 的终端单元 20。在这种情况下,因为如上所述,从有向图 I(1 → 7) 到有向图 I(a → h) 设置了图间有向边,所以用户 1 ～ 7 的终端单元 20 可以通过将子集 [1,7] 的中间密钥应用于 PRSG 导出中间密钥 t([a,a]),并且进一步从中间密钥 t([a,a]) 中导出中间密钥 t([a,*])(注意,* 是 b ～ h 的某一个)。因此,没有必要将有向图 I(a → h) 的中间密钥提供给用户 1 ～ 7 的终端单元 20。

[0373] (例 2) 接着,考虑分发给用户 12 的终端单元 20 的中间密钥。首先,作为搜索含有用户 12 的终端单元 20 所属的子集 Si 作为元素的有向图 I 的结果,找到有向图 I(a → h)、I(b ← h)、I(b ← d)、I(b ← b)、I(9 ← 15)、I(10 ← 16) 和 I(10 ← 12)。观察有向图 H(10 → 16),用户 12 的终端单元 20 不属于初始坐标点上的子集 [16,16],但属于第 5 和随后坐标点上的子集 [16,12]、[16,11]、[16,10]。在那些坐标点当中,在它们的父坐标点上不包括用户 12 的坐标点只有 [16,12] 和 [16,11]。具体地说,用户 12 不包括在作为包括用户 12 的坐标点 [16,12] 和 [16,11] 的父坐标点 parent([16,12]) 和 parent([16,11]) 的坐标点 [16,13] 中。因此,将 t([16,12]) 和 t([16,11]) 提供给用户 12 作为与有向图 H(10 ← 16) 相对应的中间密钥。

[0374] 同样,为其它有向图 I(a → h)、I(b ← h)、I(b ← d)、I(9 ← 15) 和 I(10 ← 12) 选择相应中间密钥,并且将其提供给用户 12。但是,因为从 I(10 ← 16) 到 I(b ← b) 设置了图间有向边,所以用户 12 的终端单元 20 可以使用上面的中间密钥 t([16,13]) 导出中间密钥 t([b, b]),从而没有必要将中间密钥 t([b, b]) 提供给用户 12 的终端单元 20。因此,将总共七个中间密钥提供给用户 12。

[0375] 下面参照图 12 简要总结一下直到将中间密钥分发给每个用户的终端单元的处理。图 12 是示出按照该实施例,根据系统建立在密钥分发服务器 10 中分发中间密钥的处理流程的流程图。

[0376] 如图 12 所示,密钥分发系统 100 的密钥分发服务器 10 首先设置各种各样参数等。例如,密钥分发服务器 10 确定指定给终端单元 20 的整个树 BT 的叶节点的数量 n(用户的数量)、集合密钥和中间密钥的位数 λ、指示整个树 BT 的分层的数量的参数 y、给定参数 k、PRSG 的伪随机数生成算法等,并且向所有用户的终端单元 20 公布它们 (S202)。这样,除了在上述基本方案中公布的参数 n、λ、k 和 PRSG 算法之外,该实施例还确定并公布了指示整个树 BT 的分层的数量的参数 y。

[0377] 接着,密钥分发服务器 10 将指定给叶节点的终端单元 20 的集合划分成给定子集 Si,确定用并集表示的集合系统 ψ(参见上面表达式 (2)),并公布集合系统 ψ(S204)。

[0378] 然后,密钥分发服务器 10 生成上述的多个有向图 I,确定由那些有向图 I 的集合组

成的结构 T，并且公布多个有向图 I 的结构 T(S206)。进一步，密钥分发服务器 10 确定与构成集合系统 ψ 的每个子集相对应的中间密钥 (S208)。此后，密钥分发服务器 10 使用确定的中间密钥和密钥生成部分 114 的 PRSG 导出与其它坐标点相对应的中间密钥，并且向每个用户分发必要的中间密钥的终端单元 20，以便导出与包括每个终端单元 20 的所有子集相对应的集合密钥 (S210)。然后，终端单元 20 从密钥分发服务器 10 接收有关中间密钥等的信息，并且安全地将它存储到安全存储部分 208 中。

[0379] 上文描述了按照该实施例在建立时对中间密钥的分发方法。如果使用上面的分发方法，则分发每个许可用户的终端单元生成集合密钥所需的最少个中间密钥，从而能够减少密钥分发服务器 10 与终端单元 20 之间的通信量和每个用户的终端单元 20 中中间密钥的存储容量。

[0380] （内容密钥的分发）

[0381] 下文简要总结一下按照该实施例在密钥分发服务器 10 中分发加密内容密钥 mek 的处理流程。因为按照该实施例分发内容密钥的方法基本上与按照前述基本技术的内容分发方法相同，所以回头参照图 6 来描述。

[0382] 如图 6 所示，在分发内容密钥的时候，按照该实施例的密钥分发服务器 10 首先确定排除用户的集合 (R) 从而获得许可用户的集合 (N\R)(S112)。接着，密钥分发服务器 10 从构成集合系统 ψ 的子集中选择含有 (N\R) 的并集的 m 个子集 Si(i ＝ 1、2、...、m)，以便使 m 的值最小 (S114)。然后，密钥分发服务器 10 使用分别与所选子集 Si 相对应的 m 个集合密钥 k(Si) 加密内容密钥 mek(S116)。进一步，密钥分发服务器 10 将指示许可用户的集合 (N\R) 或它的子集 Si 的信息和 m 个加密内容密钥 mek 分发给所有用户的终端单元 20(S118)。

[0383] 上文描述了按照该实施例的密钥分发服务器 10 中内容密钥 mek 的加密方法和分发方法。如果使用上面的加密方法，就可以有效地选择子集 Si，以便使集合密钥的数量是最少必要个。因为从此使用最少必要个 (m 个) 集合密钥加密内容密钥 mek，所以可以节约加密所需的计算量，并且还减少了要分发的加密内容密钥的数量，从而减少了通信量。

[0384] （内容密钥的解密）

[0385] 下文描述按照该实施例在每个用户的终端单元 20 中解密加密内容密钥的处理流程。因为按照该实施例解密内容密钥的方法基本上与按照前述基本技术的内容密钥解密方法相同，所以回头参照图 7 来描述。

[0386] 如图 7 所示，每个用户的终端单元 20 首先从密钥分发服务器 10 接收 m 个加密内容密钥 mek 和诸如指示许可用户的集合 (N\R) 的信息或指示 m 个子集 Si(i ＝ 1、2、...、m) 的信息的许可终端标识信息 (S120)。接着，终端单元 20 根据该许可终端标识信息搜索它所属的子集 Si(S122)，并且判定它是否属于 m 个子集 Si 的某一个 (步骤 S124)。

[0387] 结果，如果终端单元 20 找出它所属的子集 Si，它就根据密钥分发服务器 10 事先提供的中间密钥和有向图 I，使用上述的密钥生成部分 128 的 PRSG 导出与子集 Si 相对应的集合密钥 k(Si)(S126)。PRSG 的配置与前述相同。如果事先将与子集 Si 相对应的中间密钥 t(Si) 从密钥分发服务器 10 提供给终端单元 20，并且终端单元 20 保存它，则它就可以通过一次性地使用 PRSG 导出集合密钥 k(Si)。另一方面，如果终端单元 20 未保存中间密钥 t(Si)，它可以通过重复地使用 PRSG 导出所希望集合密钥 k(Si)。此后，终端单元 20 使

用这样导出的集合密钥 k(Si) 解密加密内容密钥 mek，从而能够解密加密内容 (S128)。

[0388] 另一方面，如果终端单元 20 在步骤 S124 中判定它不属于子集 Si 的某一个，则终端单元 20 显示和输出 :“它被排除在允许访问内容的终端单元 20 之外 (即，它是排除用户)”(S130)，并且结束内容密钥 mek 的解密处理。

[0389] 因为如上所述的按照该实施例的内容密钥解密处理不仅通过将整个树 BT 分层成基本子树适当地配置了有向图 I 的有向边，而且设置了图间有向边，所以与前述的基本技术相比，可以在终端单元 20 中减少使用 PRSG 获得中间密钥和集合密钥的计算量。

[0390] [本发明的优点]

[0391] 上文详细描述了按照该实施例的密钥分发系统 100。在这个实施例中，将由终端单元 20 的子集组成的集合系统 ψ 变更成用上面的表达式 (2) 表示，从而与前述的基本技术相比，改进了有向图 I。该实施例将向其指定所有终端单元 20 的整个大树 BT 划分成小基本子树，以便将它分层成 y 层，和在每个基本子树中使用按照基本技术的密钥导出方法，并且进一步在与不同基本子树相对应的子集之间设置有向图 I 的有向边，和应用使用伪随机数发生器 PRSG 的密钥导出方法。

[0392] 这种配置能够减少每个用户的终端单元 20 要保存的中间密钥的数量，和减少导出密钥所需的终端单元 20 的计算量。终端单元 20 要保存的中间密钥的数量存在 $k*\log(n)$ 的位置关联，和导出密钥所需的终端单元 20 的计算量存在 $k*\log n^{(1/k)}$ 的位置关联。因为这个实施例通过将整个大树 BT 划分成 $n^{(1/y)}$ 个叶节点的小基本子树以便减少树结构的叶节点的数量 n 来配置集合系统 ψ 和有向图 I，所以可以减少终端单元 20 要保存的密钥的数量、和导出密钥所需的计算量。

[0393] 下文参照图 13 在按照前述基本技术的密钥分发方案和按照该实施例的密钥分发方案之间比较终端单元 20 要保存的中间密钥的数量。图 13(A) 是示出在按照前述基本技术的密钥分发方案中每个终端单元要保存的中间密钥的数量 (如图 4 所示的 n ＝ 64 和 k ＝ 6 的情况) 的表格，而图 13(B) 是示出在按照该实施例的密钥分发方案中每个终端单元 20 要保存的中间密钥的数量 (如图 11 所示的 n ＝ 64、y ＝ 2 和 k ＝ 3 的情况) 的表格。

[0394] 如图 13 所示，当比较按照该实施例的密钥分发方案和按照基本技术的密钥分发方案时，虽然在用户 1 和 64 的终端单元 20 中在两种方案之间中间密钥 t 的数量是相同的，即，1 个和 2 个，但在其它用户 2 ～ 63 的终端单元 20 中密钥的数量在按照该实施例的密钥分发方案中少于在按照基本技术的密钥分发方案中。进一步，虽然在按照基本技术的密钥分发方案中所有终端单元 20 要保存的密钥的总数是 705 个，但在按照该实施例的密钥分发方案中是 400 个。更进一步，虽然在按照基本技术的密钥分发方案中每个终端单元 20 的平均密钥数是大约 11.02 个，但在按照该实施例的密钥分发方案中是 6.25 个。这样，按照该实施例的密钥分发方案与按照基本技术的密钥分发方案相比，能够将密钥的数量减少到大约 56.7％，因此使每个终端单元 20 要保存的密钥的数量显著减少，并且减轻了终端单元 20 的存储负担。

[0395] 接着，对在终端单元 20 中解密内容密钥 mek 所需的终端单元 20 的计算量作如下研究。计算量的最差值用有向图中从初始坐标点 (根) 到最远最后坐标点 (有向边的叶) 的有向边的数量 (即，设置有向边时的跳跃次数) 表示。在如图 4 的例子所示的按照基本技术的密钥分发方案中，为了从有向图 H(1 → 64) 的初始坐标点 [1,1] 到达最后坐标点 [1,

64]，有必要穿过 11 条有向边（进行 11 次跳跃），这意味着运行 PRSG 多达 11 次。

[0396] 另一方面，在如图 11 的例子所示的按照该实施例的密钥分发方案中，在有向图 H(1 → 7) 和 H(a → h) 中从初始坐标点 [1,1] 到最后坐标点 [1, h] 最远，而所需的有向边的数量（即，跳跃次数）是 10，小于按照基本技术的密钥分发方案中的 11。这样，按照该实施例的密钥分发方案与按照基本技术的密钥分发方案相比，能够减少在解密等时计算密钥所需的每个终端单元 20 中的计算量。

[0397] 在按照基本技术的密钥分发方案中，如果使参数 k 的值较小，可以减少每个终端单元 20 要保存的密钥的数量，因为在图 4 中删除了长的有向边（长距离跳跃），而只保留了短的有向边（短距离跳跃）；但是，这引起了每个有向图 H 中从初始坐标点到最后坐标点的有向边的数量所代表的终端单元 20 中的计算量增大的问题。

[0398] 如上所述，在按照该实施例的密钥分发方案中，即使终端单元 20（接收者）的数量很大，也可以减少终端单元 20 要保存的密钥的数量和使用加密密钥解密时所需的终端单元中的计算量两者。

[0399] [加密密钥分发系统 100 的应用]

[0400] 下文描述上述加密密钥分发系统 100 的应用。

[0401] （应用 1）

[0402] 首先，作为应用 1，在图 14 中示出了广播加密系统 300 的配置。

[0403] 图 14 是示出使用广播卫星的广播加密系统的配置的方块图。在广播加密系统 300 中，通过广播信道将加密数据（所谓的密文）传送到接收器 310。广播加密系统 300 中的广播信道是，例如，卫星广播分发信道。作为密文传送的数据是包含，例如，加密密钥、音频数据、视频数据、文本数据等的内容。卫星电视广播电台 302 中的广播信托中心 304 将数据传送到广播卫星 306。广播信托中心 304 选择用于加密的密钥或控制例如数据的加密和数据的分发。广播卫星 306 广播数据。安装在住宅 308 中的接收器 310 包括例如卫星广播接收器，并且接收所广播的数据。多个其它接收器 310 也可以接收广播的数据。这样，广播信托中心 304 可以将数据传送给由接收器 310 组成的接收器组中的每个接收器 310。如后所述，广播信托中心 304 以只有授权接收器 310 才能解密广播数据的方式加密广播数据。尽管图 14 示出了使用广播卫星 306 的广播系统，但也可以使用其它广播信道，譬如闭路电视和计算机网络。

[0404] 上文描述了作为加密密钥分发系统 100 的一种应用的广播加密系统 300 的配置。下面简要总结一下与加密密钥分发系统 100 的关系，广播信托中心 304 对应于密钥分发服务器 10（按照本发明的信息处理单元），和接收器 310 对应于终端单元 20（按照本发明的终端单元）。广播卫星 306 作为连接它们的网络的媒介。

[0405] （应用 2）

[0406] 接着，作为应用 2，在图 15 中示出了广播加密系统 400 的配置。

[0407] 图 15 是示出使用数据媒体的广播加密系统 400 的配置的方块图。在广播加密系统 400 中，广播信道是数据存储媒体的分发。媒体制造商 402 中的广播信托中心 404 将数据存储在诸如只读存储媒体（例如，CD-ROM、DVD-ROM 等）和可重写存储媒体（例如，CD-RW、DVD-RW 等）之类的存储媒体 406 的每件数据媒体中。在只读存储媒体中，广播信托中心 404 记录加密内容密钥和加密内容，以便只有授权用户才能解密数据和访问加密内容（例如，

声音、视频、文本等）。另一方面，在可重写存储媒体中，广播信托中心 404 记录加密内容密钥，以便只有授权记录单元才能将相应数据记录到记录媒体中。媒体制造商 402 将存储媒体 406 传送到诸如零售商店等的分发中间商。分发中间商 408 将存储媒体 410 提供给住宅 412 中的接收器 414。例如，分发中间商 408 将存储媒体 410 销售给某个人，这个人将存储媒体 410 拿到住宅 412 中，并且将存储媒体 410 插入接收器 414 中。例如，接收器 414 可以是诸如 CD 播放器、DVD 播放器和计算机之类，读取和播放记录在存储媒体 410 中的数据的单元。作为另一个特例，接收器 414 可以是能够将数据记录到存储媒体 410 中和从存储媒体 410 中读取数据的盘单元，如 DVD-RW 驱动器。广播信托中心 404 以只有授权接收器 414 才能解密加密数据的方式加密数据。

[0408] 上文描述了作为加密密钥分发系统 100 的一种应用的广播加密系统 400 的配置。下面简要总结一下与加密密钥分发系统 100 的关系，广播信托中心 404 对应于密钥分发服务器 10（按照本发明的信息处理单元），和接收器 414 对应于终端单元 20（按照本发明的终端单元）。进一步，取代连接它们的网络，存在由分发中间商 408 分发的存储媒体 406 和 410 作为媒介。

[0409] 尽管上面参照附图描述了本发明的优选实施例，但本发明当然不局限于此。对于本领域的普通技术人员来说，显而易见，可以不偏离权利要求书范围地作出各种各样的改变和修改，因此，这意味着这些改变和修改也包含在本发明的技术范围之内。

[0410] 例如，在上述树结构设置部分 102 中假设了树枝从顶部到底部越来越宽的树结构，但不局限于此，树结构可以是这样的，即树枝沿着任意方向，譬如，从底部到顶部、从左侧到右侧和从右侧到左侧越来越宽。在这样的情况下，有必要改变与各个中间节点相关联的子集的定义以便适应它。但是，该改变是简单地旋转通过上述树结构设置部分 102 设置的树结构，在任何情况下都意味着完全相同。进一步，尽管上述有向边设置部分 106 和子树间有向边设置部分 108 通过设置从左到右或从右到左的坐标轴来构建有向图 I′ 和 I，但坐标轴的方向可以相反或改变成非水平方向、诸如垂直方向的任意方向。因此，尽管在上面的描述中为了方便起见根据垂直方向或水平方向定义参数，但根据一般人或本领域普通技术人员的常识，即使将树结构或有向图旋转或反向，改变了垂直和水平关系，也意味着包含在相同技术范围之内。

[0411] 进一步，尽管在上述实施例中，如图 9 所示，将叶节点的数量 $n = 64$ 的整个树 BT 分层成 $y = 2$ 个层，但本发明不局限于此，可以将指示分层层数的参数 y 设置成任何自然数，和可以将整个树分层成三层或更多层。例如，可以将 $n = 64$ 的整个树 BT 划分成高度为 2 和含有四个叶节点的基本子树，以便将它分层成 $y = 3$ 个层。在这样的情况下，可以以这样的方式配置树结构，即，将整个树 BT 划分成顶层的一个基本子树、中间层的四个基本子树和底层的十六个基本子树，使中间层的基本子树的根节点与顶层的基本子树的叶节点一致，和使底层的基本子树的根节点与中间层的基本子树的叶节点一致。

[0412] 更进一步，通过子树间有向边设置部分 108 设置在不同基本子树的有向图 I 之间设置的有向边的技术不局限于图 11 的例子，各种各样的设计改变都是可行的。尽管就减少密钥的数量而言，以这样的方式设置子树之间的有向边是优选的，即，使下层的基本子树中的有向图的子集包括在上层的基本子树中的有向图 I 的子集中，但不局限于此，可以与包含关系无关地设置有向边。

[0413] ＜第二实施例＞

[0414] 下文描述按照本发明第二实施例的加密密钥分发方案。按照该实施例的加密密钥分发方案通过生成含有较长有向边的有向图，能够减少终端单元 20 中所需的计算量。在下文中，将详细描述实现按照该实施例的加密密钥分发方案的密钥分发服务器 10 和终端单元 20 的功能配置、和该加密密钥分发方案的特征和优点。

[0415] ［密钥分发服务器 10 的配置］

[0416] 首先，下文参照图 16 详细描述按照该实施例的密钥分发服务器 10 的配置。图 16 是示出按照该实施例的密钥分发服务器 10 和终端单元 20 的配置的方块图。

[0417] 如图 16 所示，密钥分发服务器 10 包括树结构设置部分 154、坐标轴设置部分 156、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。尤其，树结构设置部分 154、坐标轴设置部分 156 和有向图生成部分 160 统称为密钥生成逻辑构建块。同样，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。

[0418] 下文描述构成密钥生成逻辑构建块的元件。密钥生成逻辑构建块进行与上述的［基本技术的描述］中（树结构的设置）和（有向图的生成）相对应的处理。

[0419] （树结构设置部分 154）

[0420] 树结构设置部分 154 配置由指定号码 1 ～ n(n 是自然数）的 n 个叶节点、根节点、和与根节点和叶节点不同的多个中间密钥 t(S0) 组成的二叉树，并且在位于某个中间节点 v 或根节点 v 的下层上的多个叶节点当中，将位于左端的叶节点的号码设置成 lv，而将位于右端的叶节点的号码设置成 rv。进一步，树结构设置部分 154 将集合 (1 → n) 和集合 (2 ← n) 指定给根节点，如果某个中间节点 v 位于它的父节点左侧，则将集合 (lv+1 ← rv) 指定给该中间节点，而如果中间节点 v 位于它的父节点右侧，则将集合 (lv → rv-1) 指定给该中间节点。

[0421] 如上所述，树结构设置部分 154 具有能够构建 m 层树结构的配置，例如，假设 m ＝ 2 的情况（二叉树），它可以构建与按照基本方案（图 3）的二叉树结构相同的树结构。因此，通过树结构设置部分 154 构建的树结构的每个节点的含义基本上与按照前述基本方案构建的二叉树结构的每个节点的含义相同。尽管为了便于描述起见，下文只描述二叉树结构，但不局限于此。

[0422] （坐标轴设置部分 156）

[0423] 坐标轴设置部分 156 设置在水平坐标轴上以包含度从左到右越来越大的方式排列与包括在集合 (1 → n) 中的子集相关联的坐标点的与根节点相对应的第一水平坐标轴。接着，坐标轴设置部分 156 设置在水平坐标轴上以包含度从右到左越来越大的方式排列与包括在集合 (2 ← n) 中的子集相关联的坐标点的与根节点相对应的第二水平坐标轴。然后，对于每个中间节点，坐标轴设置部分 156 设置在水平坐标轴上以包含度从左到右越来越大的方式排列与包括在集合 (lv → rv-1) 中的子集相关联的坐标点的与某个中间节点 v 相对应的第三水平坐标轴。进一步，坐标轴设置部分 156 设置在水平坐标轴上以包含度从右到左越来越大的方式排列与包括在集合 (lv+1 ← rv) 中的子集相关联的坐标点的与某个中间节点 v 相对应的第四水平坐标轴。此后，坐标轴设置部分 156 放置每一个在位于第三水平坐标轴右端的坐标点的右侧和在位于第二和第四水平坐标轴左端的坐标点的左侧上的两

个临时坐标点，将位于第一水平坐标轴右端的坐标点设置成第一临时坐标点，并且将第二临时坐标点放置在第一临时坐标点的右边。

[0424] 如上所述，坐标轴设置部分 156 设置构建与树结构设置部分 154 配置的树结构的各个节点相对应的有向图 H 的坐标轴。第一水平坐标轴指示与集合 (1 → n) 相对应的坐标轴，第二水平坐标轴指示与集合 (2 ← n) 相对应的坐标轴，第三水平坐标轴指示与集合 (lv → rv-1) 相对应的坐标轴，和第四水平坐标轴指示与集合 (lv+1 ← rv) 相对应的坐标轴。因为第三水平坐标轴和第四水平坐标轴是针对每个中间节点 v 设置的，所以分别设置了数根坐标轴。具体地说，设置了数量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。

[0425] (有向图生成部分 160)

[0426] 有向图生成部分 160 设置给定整数 k 和计算满足 $n^{(x-1)/k} < (rv-lv+1) \leqslant n^{x/k}$ 的整数 x。接着，对于整数 i ＝ 0 ～ x-1 中的每一个，有向图生成部分 160 通过耦合长度为 $n^{i/k}$ 的一条或多条向右有向边，形成尾部在第一和第三水平坐标轴上的最左坐标点上的有向路径，并且进一步通过耦合长度为 $n^{i/k}$ 的一条或多条向左有向边，形成尾部在第二和第四水平坐标轴上的最右坐标点上的有向路径。然后，对于第一到第四水平坐标轴的每一根，有向图生成部分 160 排除尾部或头部在每个临时坐标点上的所有有向边。进一步，有向图生成部分 160 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其它有向边，从而生成分别与集合 (1 → n-1)、集合 (2 ← n)、集合 (lv+1 → rv) 和集合 (lv ← rv-1) 有关的有向图。此后，有向图生成部分 160 将头部在第一水平坐标轴上的第一临时坐标点上的长度为 1 的有向边加入与集合 (1 → n-1) 有关的有向图中，从而生成与集合 (1 → n) 有关的有向图。

[0427] 如上所述，有向图生成部分 160 通过与基本方案类似的方法生成有向图。但是，与基本方案的有向图相比，有向图生成部分 160 可以生成由较长有向边组成的有向图。如后所述，这减少了每个用户导出集合密钥所需的计算量。下文参照图 17 详细描述由有向图生成部分 160 进行的处理的处理流程。图 17 是示出有向图生成部分 160 生成有向图的处理流程的流程图。

[0428] 参照图 17，有向图生成部分 160 通过如下所述的步骤生成有向图。下文通过例示描述生成与集合 (lv+1 → rv) 相对应的有向图 I(lv+1 → rv) 的方法。

[0429] (步骤 1 ;S140) 有向图生成部分 160 通过以包含度从左到右越来越大的方式排列它们将包括在集合 (lv+1 → rv) 中的子集放置在水平直线 (水平坐标轴) 上。精确地说，有向图生成部分 160 将作为集合 (lv+1 → rv) 元素的子集指定给水平坐标轴上的各个坐标点，并且以指定子集的包含度朝右越来越大的方式放置坐标点。然后，有向图获取部分 160 在水平坐标轴上最右的坐标点的右侧放置两个临时坐标点。坐标轴上从最左坐标点到最右临时坐标点的长度 Lv 是 Lv ＝ rv-lv+1。此时，有向图生成部分 160 计算满足 $n^{(x-1)/k} < Lv \leqslant n^{x/k}$ 的整数 x(1 ≤ x ≤ k)。

[0430] (步骤 2 ;S142) 有向图生成部分 160 将整数值 i 设置成计数，并且使计数 i 从 0 变化到 x-1 地进行下列操作。从水平坐标轴左端的起点开始，有向图生成部分 160 重复设置延伸到与该坐标点相隔 $n^{i/k}$ 的坐标点的向右有向边 (跳跃到与该坐标点相隔 $n^{i/k}$ 的坐标点)，直到有向边的头部到达水平坐标轴右端或它的左侧的临时坐标点，或下一个设置的有

向边的头部超过临时坐标点的某一个为止。

[0431] （步骤 3 ;S144) 有向图生成部分 160 从上面（步骤 2) 创建的有向边中删除到达临时坐标点的所有有向边。

[0432] （步骤 4 ;S146) 如果存在多条到达某个坐标点的有向边，有向图生成部分 160 删除除最长有向边之外的所有其它有向边。

[0433] 通过上面的过程，有向图生成部分 160 可以生成由与基本方案相比较长的有向边组成的有向图。进一步，对于构成树结构的所有中间节点和根节点，有向图生成部分 160 通过与上面有向图 I(lv → rv-1) 相同的方法生成有向图。例如，有向图生成部分 160 生成与某个中间节点 v 相对应的有向图 I(lv+1 ← rv)，并且进一步生成与根节点相对应的有向图 I(1 → n) 和 I(2 ← n)。有向图 I(lv+1 ← rv) 和 I(2 ← n) 是在以包括在每个图中的子集的包含度朝“左向”越来越大的方式排列坐标点的水平坐标轴上形成的。因此，通过上面（步骤 1) 设置的水平坐标轴上的坐标点排列规则相反。进一步，形成有向图 I(lv+1 ← rv) 和 I(2 ← n) 的两个临时坐标点被放置在水平坐标轴上最左的坐标点的左侧。通过将有向边 E([1,n-1],[1,n]) 加入有向图 I(1 → n-1) 中生成有向图 I(1 → n)。

[0434] 通过使用上述的有向图生成方法，生成如图 18 所示的有向图 I。图 18 示出了根据如图 3 所示的叶节点的数量 n ＝ 64 的完全二叉树设置参数 k ＝ 6 时形成的有向图 I。

[0435] 首先，比较根据基本方案生成的有向图 H(图 4) 和按照该实施例的有向图 I(图 18) 得出，有向图 I 包括较长有向边。当作出有关最长有向路径 V([1,1],[1,64]) 的比较时，虽然有向图 H 由 11 条有向边组成，但有向图 I 只由 6 条有向边组成。因此，可以肯定，有向图生成部分 160 生成集合密钥所需的计算量减少了。同样，在图 19 中示出了在参数 k 被设置成 k ＝ 3 的情况下的有向图 I。

[0436] 下文简要描述针对每个有向图评估每个用户所需的集合密钥的数量的评估方法。首先，为了选择每个用户要保存的中间密钥，有必要提取用户 u 所属的有向图。具体地说，从构成树结构的中间节点中提取与用户 u 相对应的叶节点 u 包括在位于下层的叶节点中的所有中间节点，并且选择与那些中间节点相对应的有向图。因为所有叶节点都存在于根节点的下层上，所以当然选择与根节点相对应的有向图。如果包括 n 个叶节点的树结构通过层来分类，存在一个根层、一个叶层、和 log(n)-1 个中间节点层。如图 3 所示，在每个中间节点层上只有一个包括与某个用户 u 相对应的子组作为元素的有向图 I。因此，存在包括与根节点相关联的两个有向图的最少 log(n)+1 个有向图作为目标。

[0437] 进一步，对于每个有向图，用户要保存的中间密钥的最大数量由其尾部位于一个坐标点上的有向边的最大数量决定。因此，对于某个有向图的每个坐标点，计数从一个坐标点开始的有向边的数量，当提取出号码最大的坐标点时，其尾部在该坐标点上的有向边的数量等于用户要保存的中间密钥的最大数量。至少对于有向图，用户无需保存超过最大数量的中间密钥。进一步，容易理解，根据有向图生成逻辑，其尾部在每个坐标点上的有向边的数量不会超过参数 k。

[0438] 结果，用户要保存的中间密钥的数量最多不会超过 k*(log(n)+1)。因为用户的数量足够大，密钥数量的上限一般通过 O(k*log(n)) 评估。但是，该评估值实际上是过高评估的，如果有关，例如，基本方案的情况计算出更具体的评估值，密钥数量的上限通过下列表达式 (3) 表示。在按照该实施例的密钥分发方案中，密钥数量的评估模型也是下列表达式

(3)，用户要保存的中间密钥的数量没有变化。

[0439] [表达式 3]

[0440] $$\sum_{x=1}^{k-1} x\left(\frac{\log n}{k}\right)+k\left(\frac{\log n}{k}-1\right)+2k=\frac{k+1}{2}\log n+k \quad \cdots(3)$$

[0441] 另一方面，每个用户生成集合密钥所需的计算量的评估取决于构成有向图的有向路径的长度。具体地说，随着形成每条有向路径的有向边的数量减少，每个用户的计算量也减少。例如，在按照基本方案的有向图 H 的情况下，最长有向路径是有向图 H(1 → n) 的有向路径 V([1,1],[1,n])。该有向路径包括 (2*k-1)*($n^{1/k}$-1) 条有向边。另一方面，在按照该实施例的有向图 I 的情况下，最长有向路径是有向图 I(1 → n) 的有向路径 V([1,1],[1,n])，该有向路径包括 (k*($n^{1/k}$-1) 条有向边。因此，与基本方案相比，该实施例能够将用户的每个终端单元所需的计算量减少大约一半。

[0442] 上文描述了生成不会使每个用户保存的中间密钥的数量增加地能够减小生成集合密钥所需的计算量的最差值的有向图的逻辑。上述的密钥生成逻辑（有向图）的构建主要由构成密钥分发服务器 10 的密钥生成逻辑构建块实施。但是，为了根据上面的密钥生成逻辑进行加密密钥分发，其它元件也是必要的。因此，下文回头参照图 16 描述其它元件。

[0443] 回头参照图 16，除了上述的密钥生成逻辑构建块之外，密钥分发服务器 10 还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。

[0444] (初始中间密钥设置部分 162)

[0445] 初始中间密钥设置部分 162 针对与树的每个中间节点相对应的每个有向图 I，生成与有向图 I 的初始坐标点相对应的中间密钥。例如，初始中间密钥设置部分 162 可以使用伪随机数发生器生成随机数，并且将随机数设置成与上面初始坐标点（根）相对应的每个中间密钥，或可以将给定数值设置成每个中间密钥。

[0446] (密钥生成部分 164)

[0447] 对于构成有向图 I 的某条有向边，当输入指定给有向边的尾部所指的坐标点的给定中间密钥时，密钥生成部分 164 输出与有向边的尾部所指的坐标点相对应的集合密钥、和与从该有向边的尾部延伸的所有有向边的头部相对应的中间密钥。因此，密钥生成部分 164 对应于基本方案的 PRSG。但是，密钥生成部分 164 与基本方案的 PRSG 的不同之处在于，它根据有向图生成部分 160 生成的有向图 I 输出中间密钥。如果将密钥生成部分 164 表示成与 PRSG 相同，当输入与有向图 I 的某个坐标点 S0 相对应的中间密钥 t(S0) 时，它输出与尾部在该坐标点 (对应于子集 S0) 上的有向边的头部相对应的中间密钥 t(S1)、t(S2)、...、t(Sm)、和集合密钥 k(S0)。注意，m 指示尾部在某个坐标点 S0 上的有向边的数量。

[0448] (加密部分 166)

[0449] 加密部分 166 使用集合密钥加密用于内容密钥。尽管内容密钥的数量是一个，但集合密钥的数量与构成集合系统 Φ 的子集的数量相同。因此，加密部分 166 使用构成集合系统 Φ 的所有子集的相应集合密钥加密内容密钥。因此，加密部分 166 生成与各个集合密钥相对应的加密内容密钥。于是，如果构成集合系统 Φ 的子集的数量是 m，生成 m 个加密内容密钥。可替代地，加密部分 166 可以加密内容。例如，加密部分 166 可以使用内容密钥加密内容，或可以使用各个集合密钥加密内容。使用集合密钥加密内容的配置是该实施例的

一个可替代例子。

[0450] （传送部分 168）

[0451] 传送部分 168 将加密部分 166 加密的内容密钥传送给与叶节点相对应的所有用户。进一步，传送部分 168 可以参照上述有向图 I 将中间密钥传送给每个用户。此时，传送部分 168 可以分发最少必要个中间密钥，以便每个用户可以导出与它所属的子集相对应的中间密钥。具体地说，传送部分 168 可以从构成集合系统 Φ（参见上面表达式 (1)）的子集中提取中间密钥的分发目的地用户所属的子集，从与提取子集相对应的有向图 I 的坐标点中选择这样的坐标点，即分发目的地用户不包括在与到达该坐标点的有向边的尾部相对应的子集中，并且只将与所选坐标点相对应的中间密钥分发给分发目的地用户。但是，如果中间密钥的分发目的地用户所属的子集对应于有向图 I 的初始坐标点，传送部分 168 可以只将与初始坐标点相对应的中间密钥分发给分发目的地用户。进一步，传送部分 168 还可以起将有向图 I 的信息分发给每个用户的有向图信息分发部分的作用。具体地说，一旦输入每个中间密钥，传送部分 168 就可以根据有向图 I，分发与输出给定中间密钥和集合密钥的 PRSG 的密钥生成算法（例如，密钥生成程序）有关的信息。

[0452] （子集确定部分 170）

[0453] 子集确定部分 170 确定应该禁止解密内容或内容密钥的排除用户的集合 (R)，并且通过使用从与有向图 I 的坐标点相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) 中删除排除用户的集合 (R)，定义许可用户的集合 (N\R)，然后以使构成许可用户的集合 (N\R) 的子集的数量最少的方式确定构成许可用户的集合 (N\R) 的一组子集。子集确定部分 170 可以由确定许可用户的集合 (N\R) 的许可用户集合确定部分和确定构成许可用户的集合 (N\R) 的一组子集的许可用户子集确定部分组成。

[0454] 在子集确定部分 170 以上面的方式确定了构成许可用户的集合 (N\R = {S1 ∪ S2 ∪ ... ∪ Sm} ;m 是自然数）的子集 (S1、S2、...、Sm) 之后，传送部分 168 将指示许可用户的集合 (N\R) 或构成许可用户的集合 (N\R) 的子集 (S1、S2、...、Sm) 的信息分发给每个用户。进一步，加密部分 166 使用与子集确定部分 170 确定的子集 (S1、S2、...、Sm) 相对应的集合密钥加密内容或内容密钥，而传送部分 168 将加密内容或内容密钥传送给每个用户。

[0455] 上文描述了按照本发明优选实施例的密钥分发服务器 10 的配置。如上所述，该配置的特征主要是密钥生成逻辑构建块的配置。尤其，该实施例在生成决定密钥生成逻辑的有向图 I 的有向图生成部分 160 的配置方面具有特征。按照该实施例的有向图生成部分 160 可以生成能够减少每个终端单元生成集合密钥所需的计算量，但不会使每个用户的终端单元要保存的密钥的数量增加的密钥生成逻辑（有向图）。

[0456] [终端单元 20 的配置]

[0457] 下文参照图 16 描述按照该实施例的终端单元 20 的配置。图 16 是示出终端单元 20 的配置的方块图。

[0458] 参照图 16，终端单元 20 包括接收部分 174、判定部分 176、密钥生成部分 178 和解密部分 180。终端单元 20 对应于上述的用户。

[0459] （接收部分 174）

[0460] 接收部分 174 接收从包括在密钥分发服务器 10 中的传送部分 168 传送的信息。例

如，接收部分 174 从密钥分发服务器 10 接收分发的内容、加密内容密钥、给定中间密钥、与有向图 I 有关的信息、与许可用户有关的信息等。进一步，接收部分 174 可以从多个信息源中收集信息，而不仅从单个信息源接收信息。例如，接收部分 174 可以从通过有线或无线网络连接的多个信息源（例如，密钥分发服务器 10）或不通过网络地直接或间接连接的信息源（例如，像光盘单元、磁盘单元和便携式终端单元那样的信息媒体）中获取信息。因为接收部分 174 当然可以从另一个终端单元 20 接收信息，所以可以配置成与属于，例如，相同分发目的地组的其它终端单元 20 共享有向图 I 的信息。在这样的情况下，相同分发目的地组指的是授权成从与对应于上述树结构的叶节点的用户的集合相对应的同一个或多个密钥分发服务器 10 分发的内容的观众用户的一个组。

[0461] （判定部分 176）

[0462] 判定部分 176 判定是否作为元素包括在与集合密钥相对应的子集的某一个中。因为终端单元 20 只保存生成与它所属的子集相对应的集合密钥的中间密钥，所以有必要根据有关密钥分发服务器 10 用于加密内容或内容密钥的集合密钥的信息事先判定它所属的子集是否包括在与集合密钥相对应的子集中。这样的判定由判定部分 176 作出。有关集合密钥的信息在与内容密钥相同或不同的时刻从密钥分发服务器 10 分发，并且被接收部分 174 接收。如果判定与所属的子集相对应的集合密钥未包括在用于加密的集合密钥中，终端单元 20 不进行使用自身保存的中间密钥生成集合密钥的处理地结束内容密钥的解密处理。相反，如果找到与所属的子集相对应的集合密钥，终端单元 20 使用自身保存的中间密钥和使用 PRSG 生成集合密钥。

[0463] （密钥生成部分 178）

[0464] 对于构成有向图 I 的某个有向边，当输入指定给有向边的尾部所指的坐标点的给定中间密钥时，密钥生成部分 178 输出与有向边的尾部所指的坐标点相对应的集合密钥、和与从该有向边的尾部延伸的所有有向边的头部相对应的中间密钥。因此，密钥生成部分 178 对应于包括在密钥分发服务器 10 中的密钥生成部分 164。如果将密钥生成部分 178 表示成 PRSG，如果输入与有向图 I 的某个坐标点 S0 相对应的中间密钥 t(S0)，它输出与尾部在坐标点 S0 上的有向边的头部相对应的中间密钥 t(S1)、t(S2)、...、t(Sk)、和集合密钥 k(S0)。注意，m 指示尾部在坐标点 S0 上的有向边的数量。有向图 I 的信息可以从密钥分发服务器 10 中获得，或可以存储在包括在终端单元 20 中的存储部分（未示出）中。

[0465] （解密部分 180）

[0466] 解密部分 180 使用集合密钥解密内容密钥。具体地说，解密部分 180 从与集合密钥相对应的子集中提取作为一个元素包括在其中的子集，并且使用与子集相对应的集合密钥）解密内容或内容密钥。

[0467] 上文描述了按照该实施例的终端单元 20 的配置。如上所述，终端单元 20 可以根据包括在上述密钥分发服务器 10 中的有向图生成部分 160 生成的特殊密钥生成逻辑（有向图 I）生成所希望集合密钥。因此，终端单元 20 可以减少生成用于解密内容密钥的集合密钥所需的计算量。

[0468] 尽管上面参照附图描述了本发明的优选实施例，但本发明当然不局限于此。对于本领域的普通技术人员来说，显而易见，可以不偏离权利要求书范围地作出各种各样的改变和修改，因此，这意味着这些改变和修改也包含在本发明的技术范围之内。

[0469] 例如，在上述树结构设置部分 154 中假设了树枝从顶部到底部越来越宽的树结构，但不局限于此，树结构可以是这样的，即树枝沿着任意方向，譬如，从底部到顶部、从左侧到右侧和从右侧到左侧越来越宽。在这样的情况下，有必要改变与各个中间节点相关联的子集的定义以便适应它。但是，该改变是简单地旋转通过上述树结构设置部分 154 配置的树结构，在任何情况下都意味着完全相同。进一步，尽管有向图生成部分 160 通过设置从左到右或从右到左的坐标轴来构建有向图 I′ 和 I，但使左右反向的改变也是可行的。具体地说，尽管在上面的描述中为了方便起见根据垂直方向或水平方向定义参数，但根据一般人或本领域普通技术人员的常识，即使将树结构或有向图 I 旋转或反向，改变了垂直和水平关系，也意味着包含在相同技术范围之内。进一步，按照该实施例的信息处理单元可以包括获取，例如，给定有向图或与有向图有关的信息，以便根据获取的有向图生成集合密钥的获取部分。

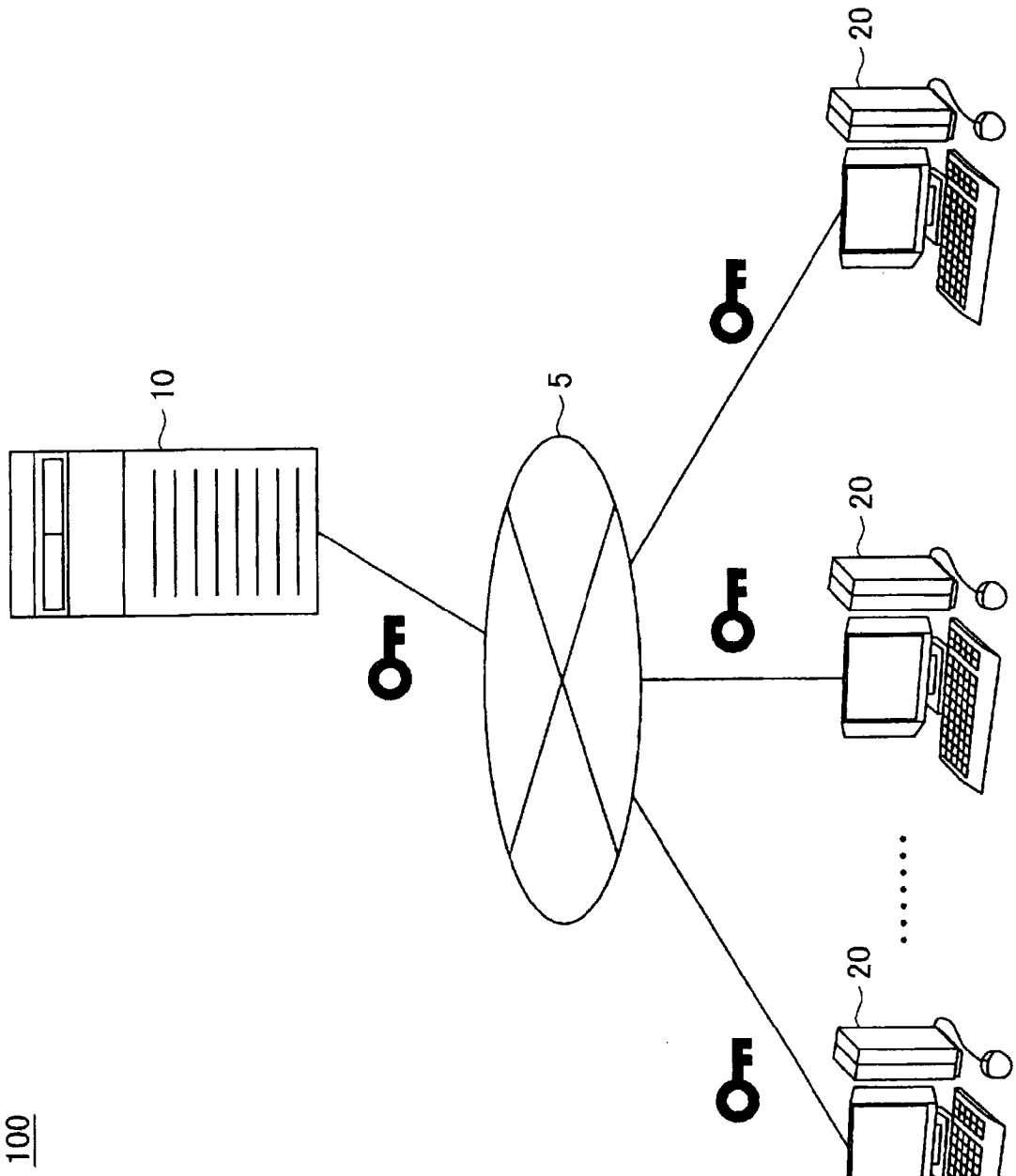


图 1

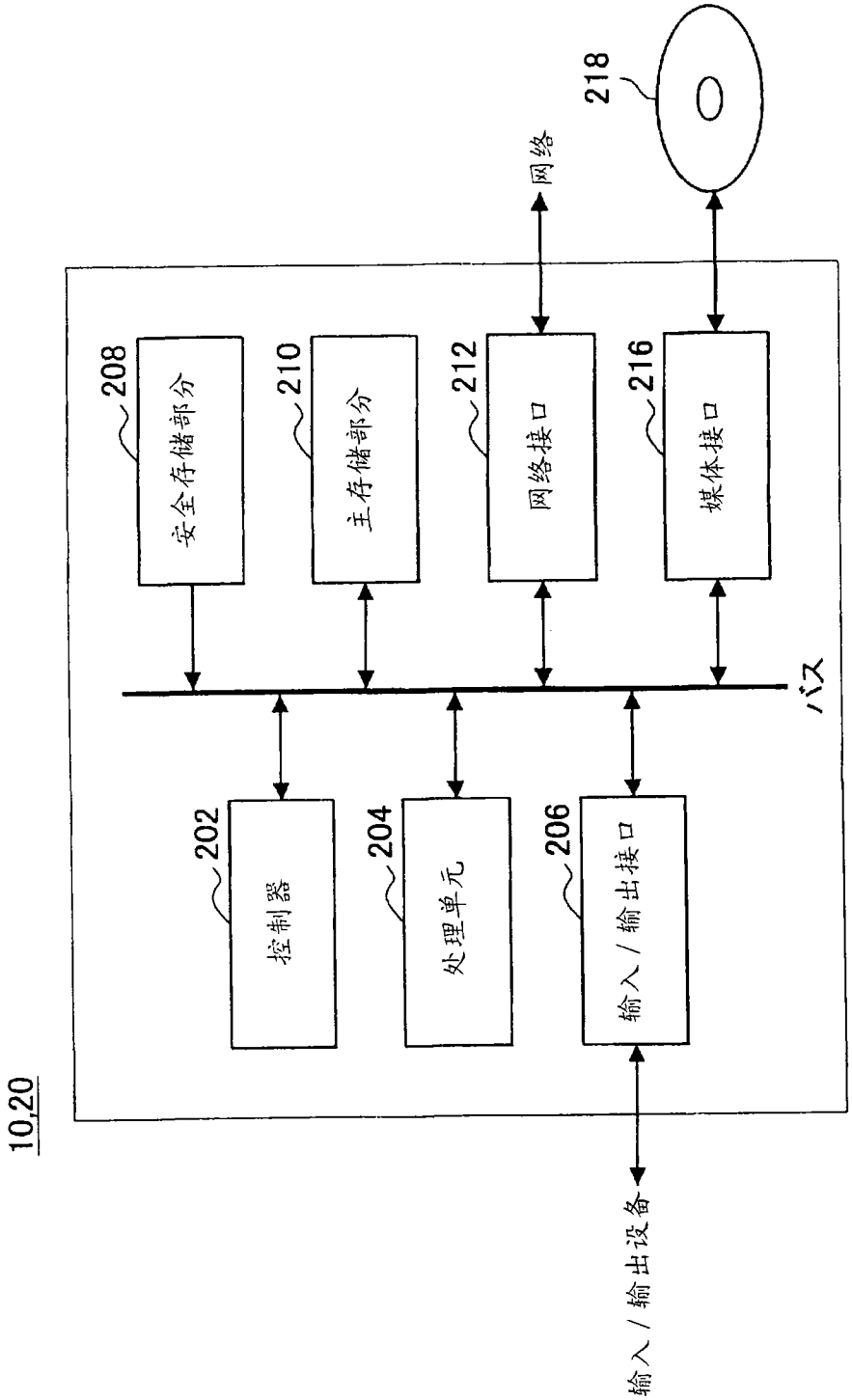

10,20
控制器
202
处理单元
204
输入 / 输出接口
206
安全存储部分
208
主存储部分
210
网络接口
212
媒体接口
216
总线
网络
218
输入 / 输出设备

图 2

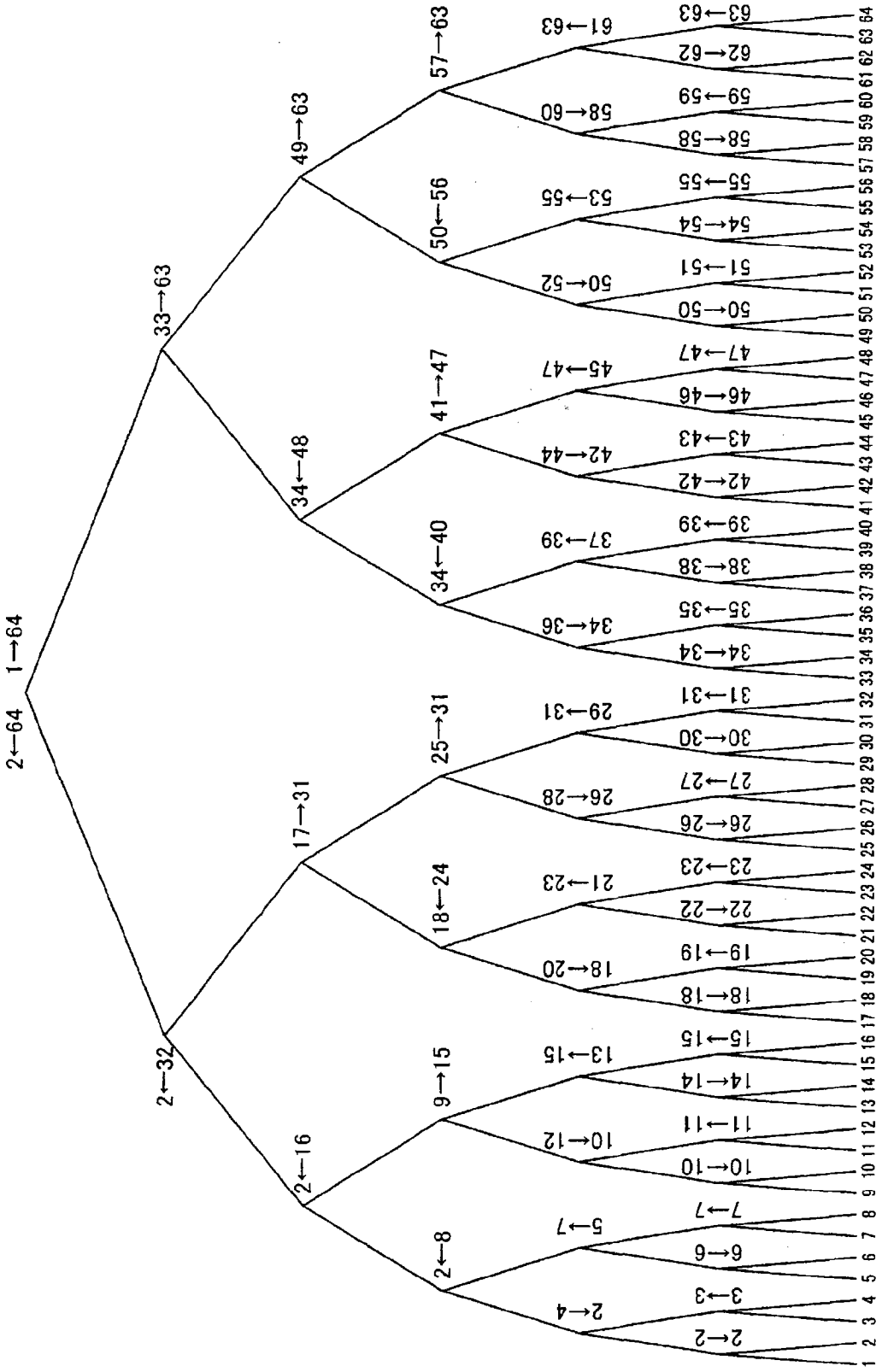

1→64
2←64
33→63
2←32
49→63
17→31
57→63
50←56
25→31
18←24
9→15
2←16
61←63
58←60
53←55
50←52
41→47
34←40
29←31
26←28
21←23
18←20
13←15
10←12
5←7
2←4
63←63
62←62
59←59
58←58
55←55
54←54
51←51
50←50
47←47
46←46
43←43
42←42
39←39
38←38
35←35
34←34
31←31
30←30
27←27
26←26
23←23
22←22
19←19
18←18
15←15
14←14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

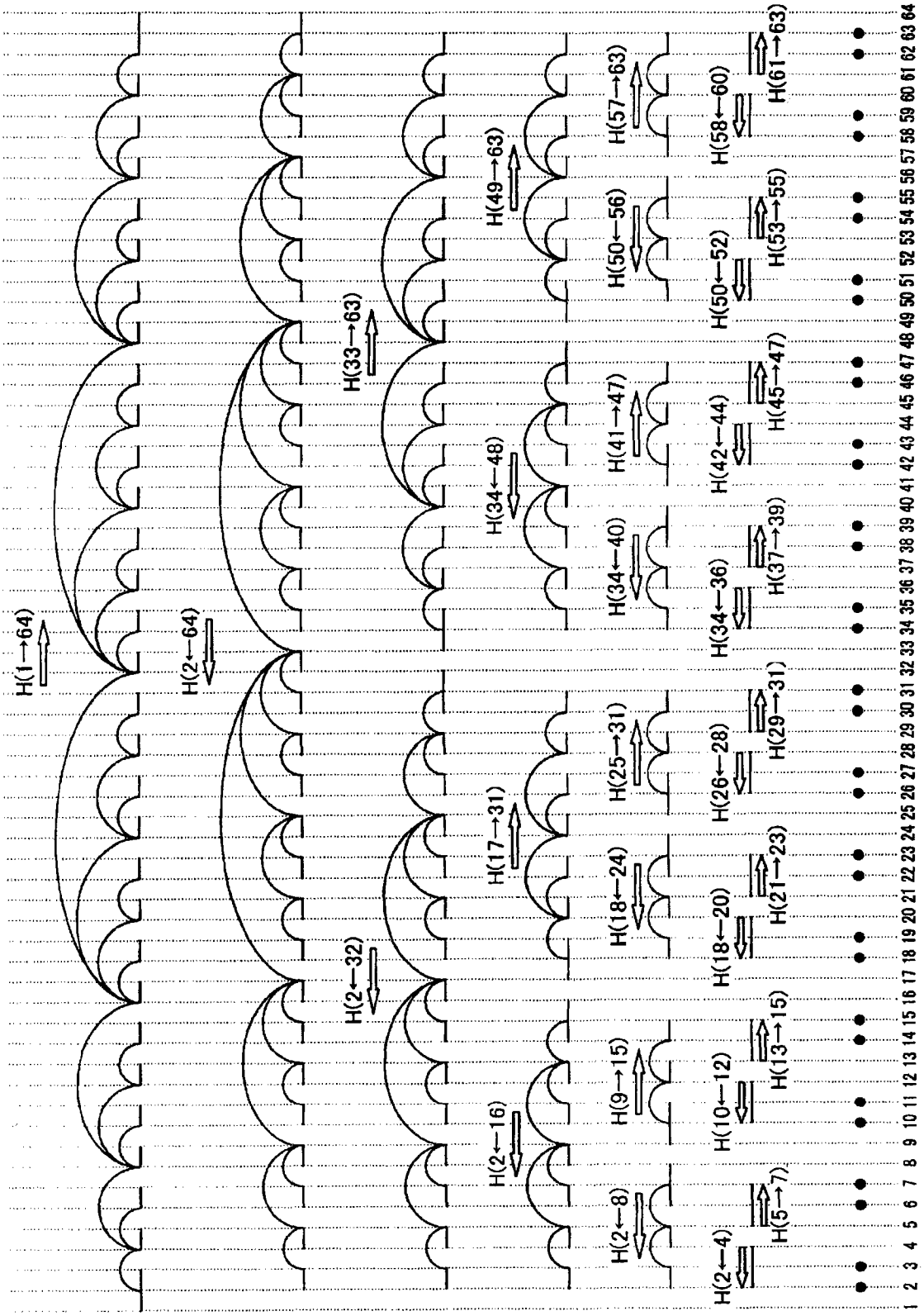

H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(17→31)
H(49→63)
H(34←48)
H(2←16)
H(9→15)
H(25→31)
H(41→47)
H(50←56)
H(57→63)
H(2←8)
H(18←24)
H(34←40)
H(42←44)
H(50←52)
H(58←60)
H(5→7)
H(10←12)
H(13→15)
H(18←20)
H(21→23)
H(26←28)
H(29→31)
H(34←36)
H(37→39)
H(45→47)
H(53→55)
H(61→63)
H(2←4)
1 2 3 4 5 6 7 8 9 10 11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

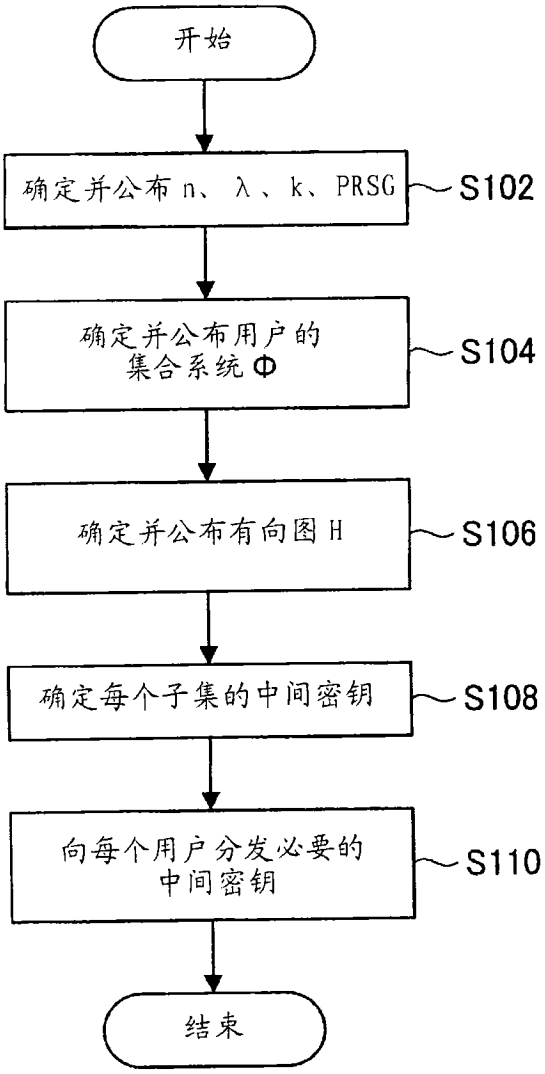

开始
确定并公布 n、λ、k、PRSG
S102
确定并公布用户的集合系统 Φ
S104
确定并公布有向图 H
S106
确定每个子集的中间密钥
S108
向每个用户分发必要的中间密钥
S110
结束

图 5

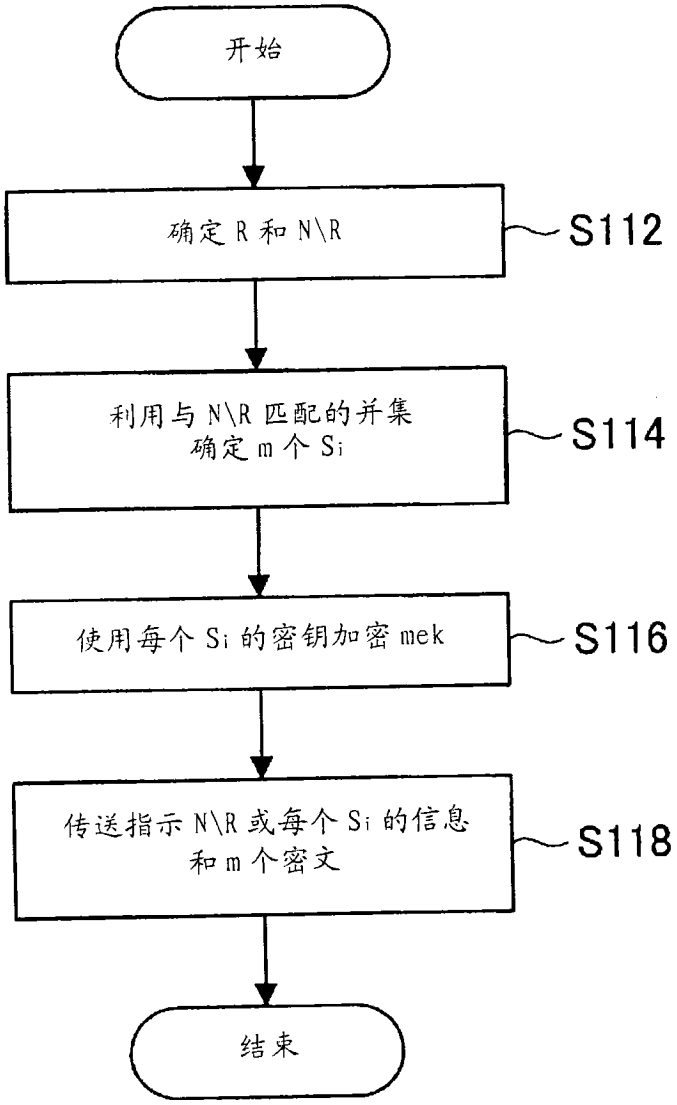

开始
确定 R 和 N\R
S112
利用与 N\R 匹配的并集
确定 m 个 Si
S114
使用每个 Si 的密钥加密 mek
S116
传送指示 N\R 或每个 Si 的信息
和 m 个密文
S118
结束

图 6

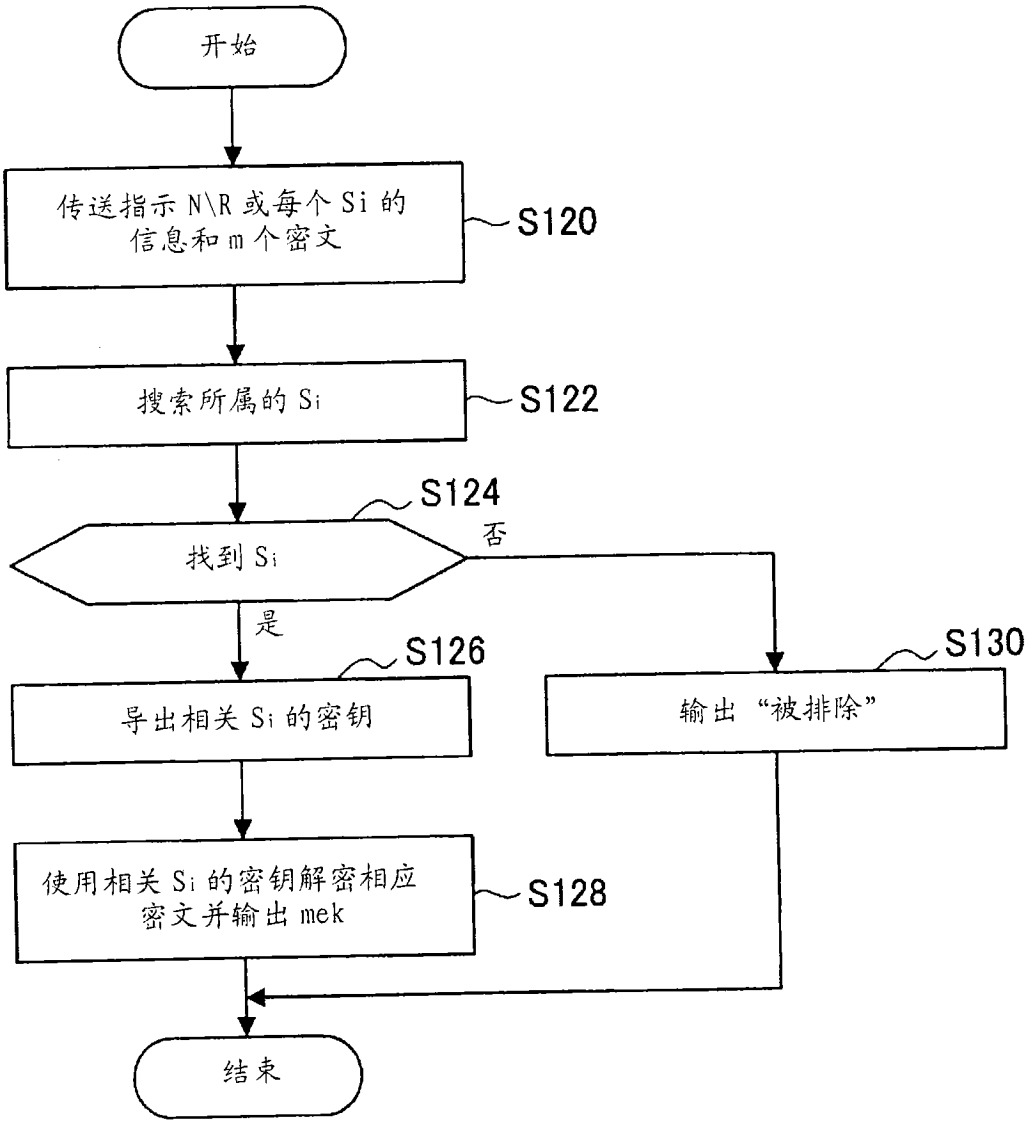

开始
传送指示 N\R 或每个 Si 的信息和 m 个密文
S120
搜索所属的 Si
S122
S124
找到 Si
否
是
S126
导出相关 Si 的密钥
S130
输出“被排除”
使用相关 Si 的密钥解密相应密文并输出 mek
S128
结束

图 7

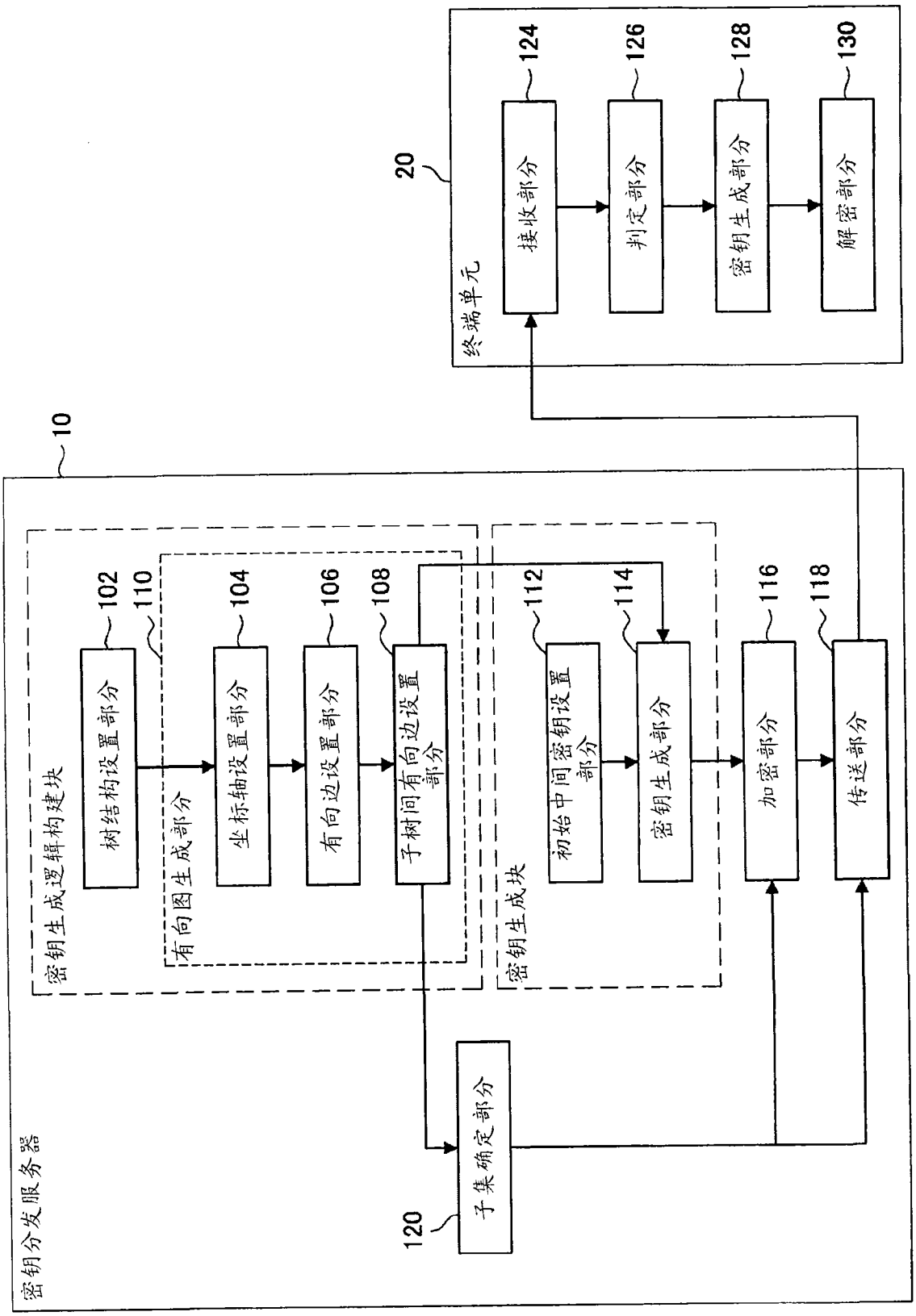

密钥分发服务器
10
密钥生成逻辑构建块
树结构设置部分
102
有向图生成部分
110
坐标轴设置部分
104
有向边设置部分
106
子树间有向边设置部分
108
密钥生成块
初始中间密钥设置部分
112
密钥生成部分
114
加密部分
116
传送部分
118
子集确定部分
120
终端单元
20
接收部分
124
判定部分
126
密钥生成部分
128
解密部分
130

图 8

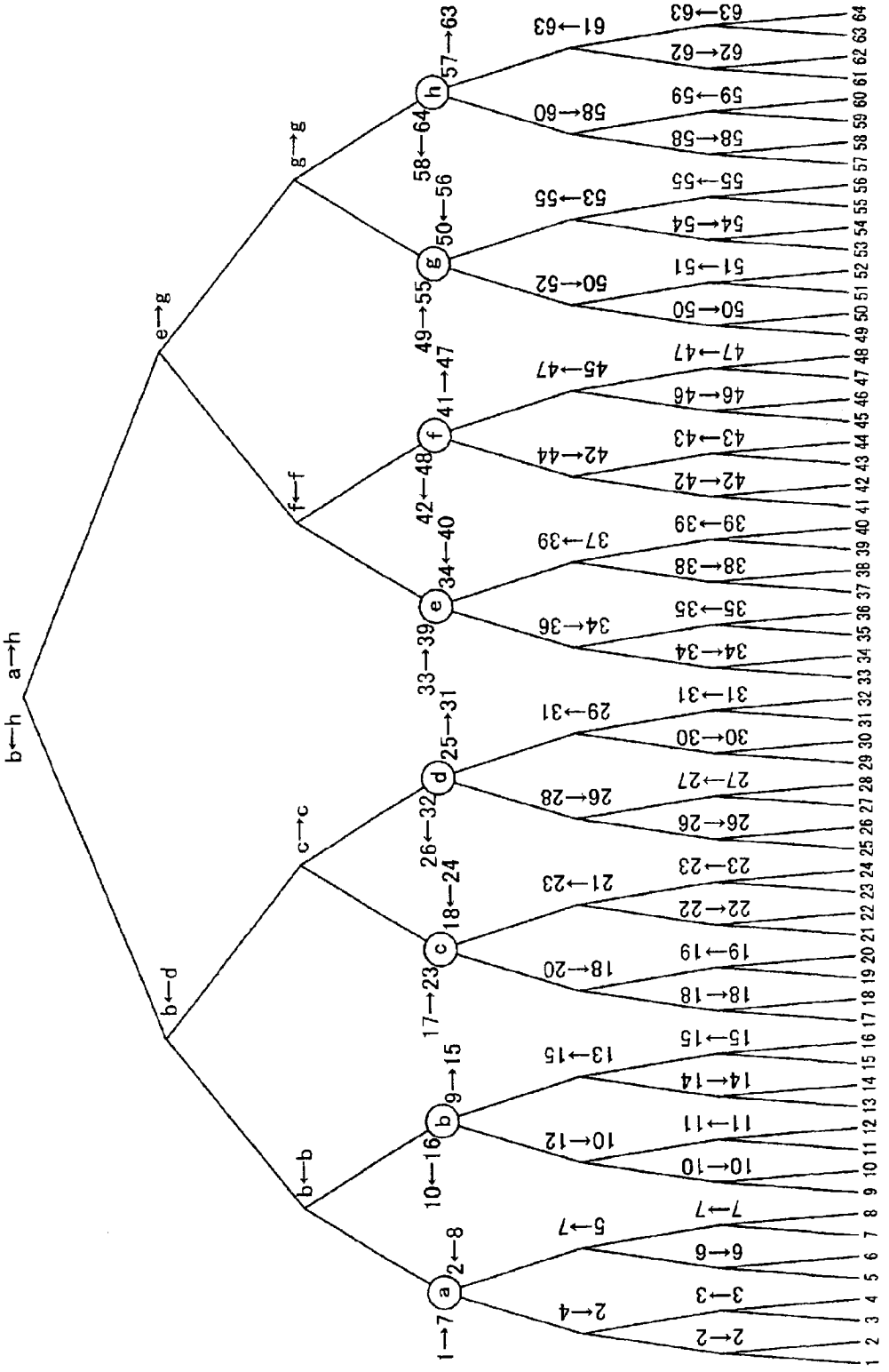

b←h a→h
e→g
g→g
h 57→63
61←63
63←63
62→62
58→60
59→59
58→58
58←64
g 50←56
53←55
55→55
54←54
50←52
51→51
50→50
49→55
f←f
f 41→47
45←47
47→47
46→46
42←48
42→44
43→43
42→42
e 34←40
37←39
39→39
38→38
34→36
35→35
34→34
33→39
b←d
c→c
d 25→31
29←31
31→31
30→30
26←32
26→28
27→27
26→26
c 18←24
21←23
23→23
22→22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

图 9

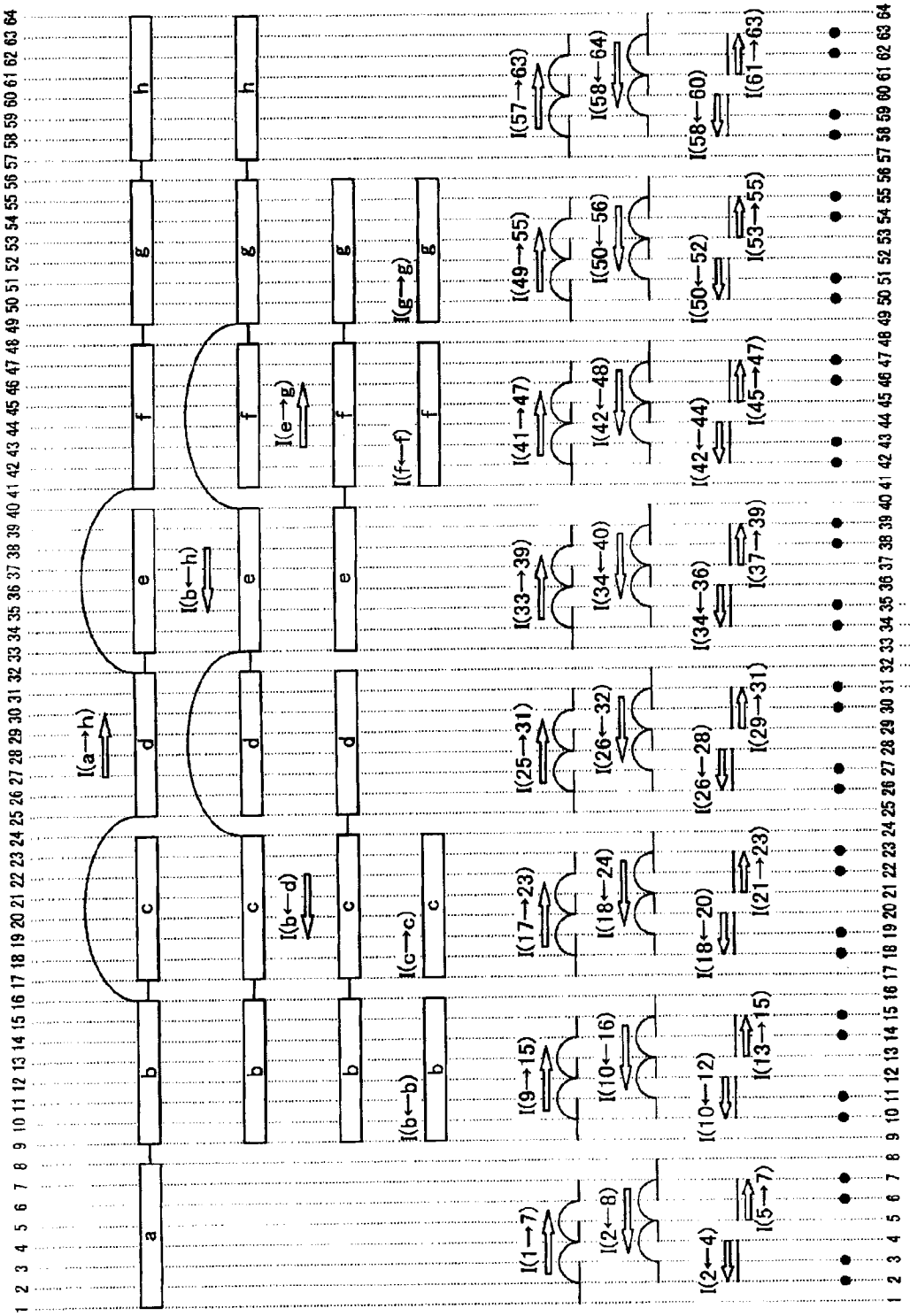

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
a
b
c
d
e
f
g
h
I(a→h)
I(b←h)
I(e→g)
I(b←d)
I(c→c)
I(f←f)
I(g→g)
I(b←b)
I(1→7)
I(2←8)
I(9→15)
I(10←16)
I(17→23)
I(18←24)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

图 10

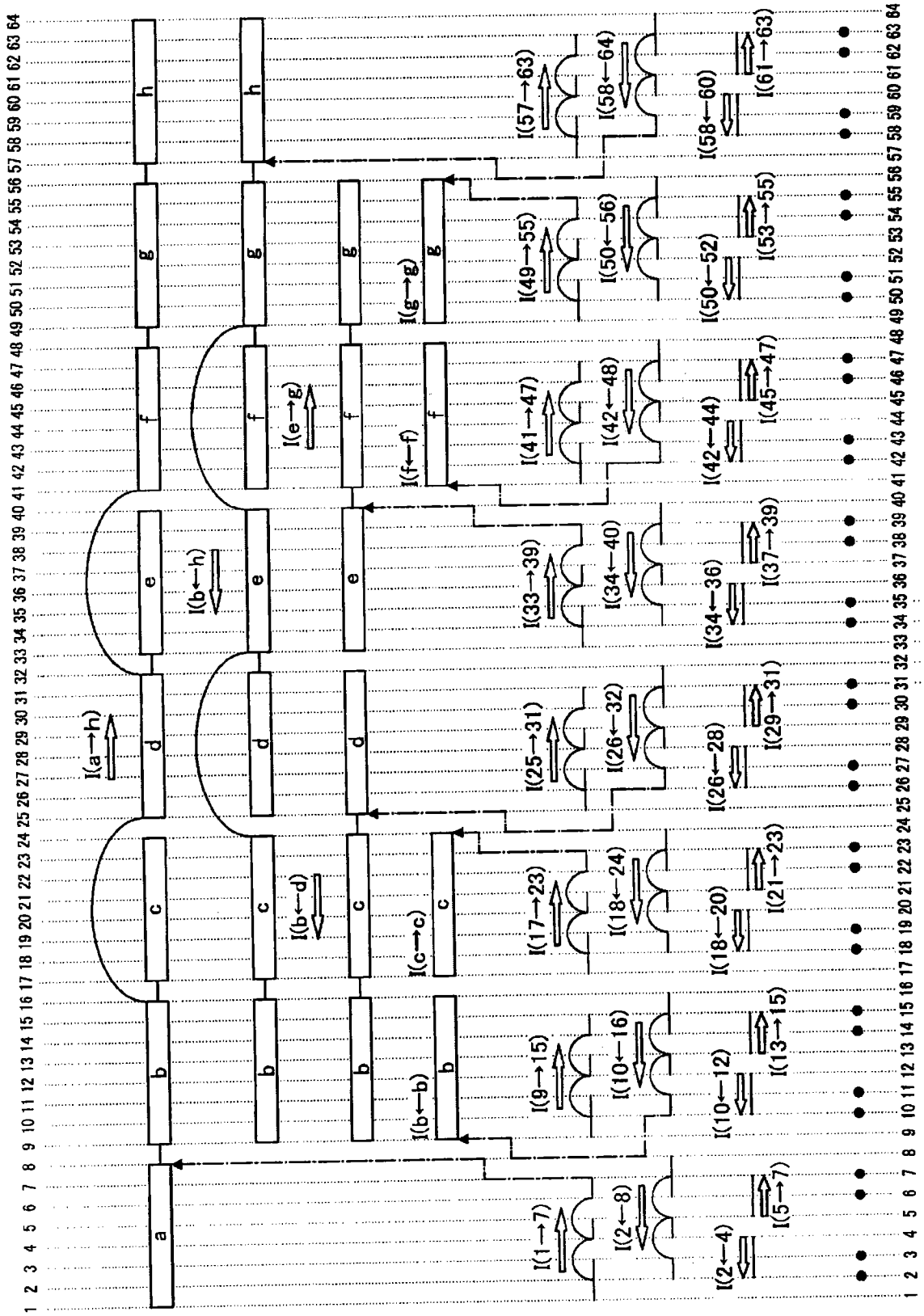

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
a
b
c
d
e
f
g
h
I(a→h)
I(b←h)
I(b←d)
I(c→c)
I(b←b)
I(e→g)
I(f←f)
I(g→g)
I(1→7)
I(2←8)
I(9→15)
I(10←16)
I(17→23)
I(18←24)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

图 11

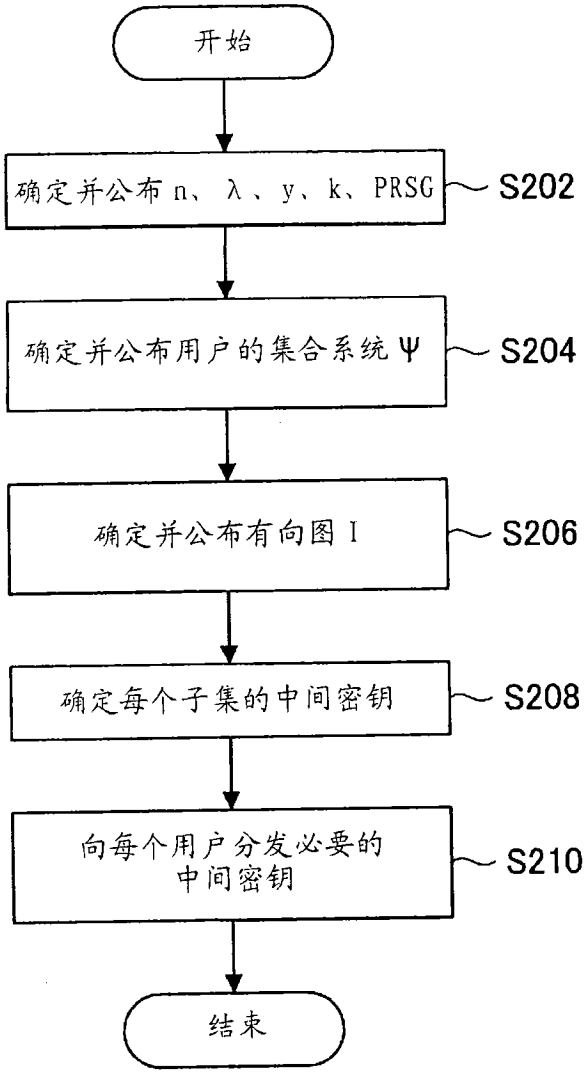

开始
确定并公布 n、λ、y、k、PRSG
S202
确定并公布用户的集合系统 Ψ
S204
确定并公布有向图 I
S206
确定每个子集的中间密钥
S208
向每个用户分发必要的中间密钥
S210
结束

图 12

	(A)	(B)
用户编号	基本技术	本发明
1	1	1
2	7	4
3	8	5
4	10	4
5	8	4
6	12	5
7	11	4
8	11	2
9	8	5
10	12	7
11	13	8
12	13	7
13	11	7
14	13	8
15	12	7
16	10	4
17	8	5
18	12	8
19	13	9
20	13	8
21	13	8
22	15	9
23	14	8
24	12	6
25	11	5
26	13	7
27	14	8
28	12	7
29	12	7
30	12	8
31	11	7
32	7	4
33	7	4
34	11	7
35	12	8
36	12	7
37	12	7
38	14	8
39	13	7
40	11	5
41	12	6
42	14	8
43	15	9
44	13	8
45	13	8
46	13	9
47	12	8
48	8	5
49	10	4
50	12	7
51	13	8
52	11	7
53	13	7
54	13	8
55	12	7
56	8	5
57	11	3
58	11	5
59	12	6
60	8	5
61	10	5
62	8	6
63	7	5
64	2	2
总计	705	400
每个用户的平均密钥数	11.015625	6.25

图 13

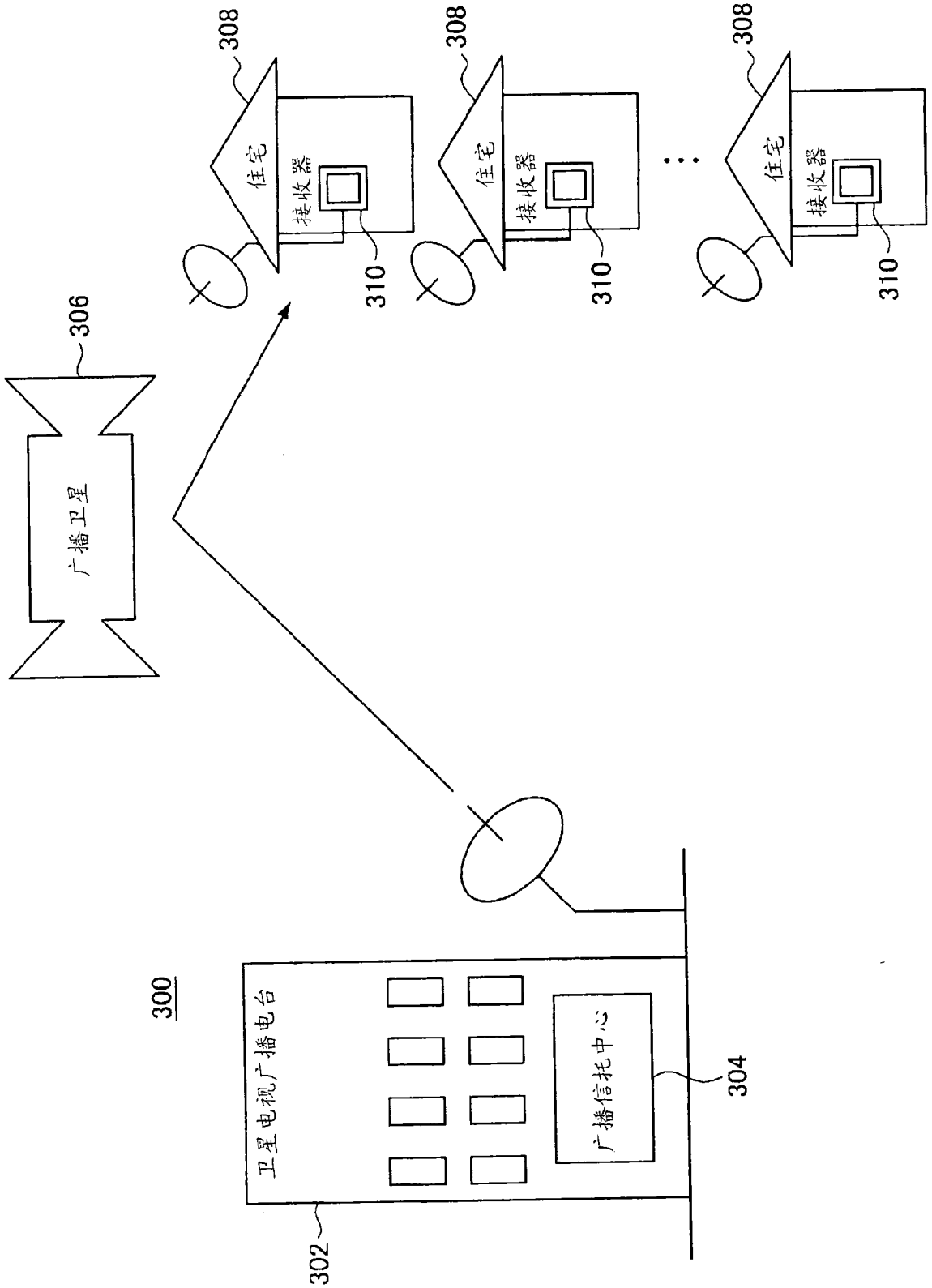

300
卫星电视广播电台
302
广播信托中心
304
306
广播卫星
308
住宅
接收器
310
308
住宅
接收器
310
308
住宅
接收器
310

图 14

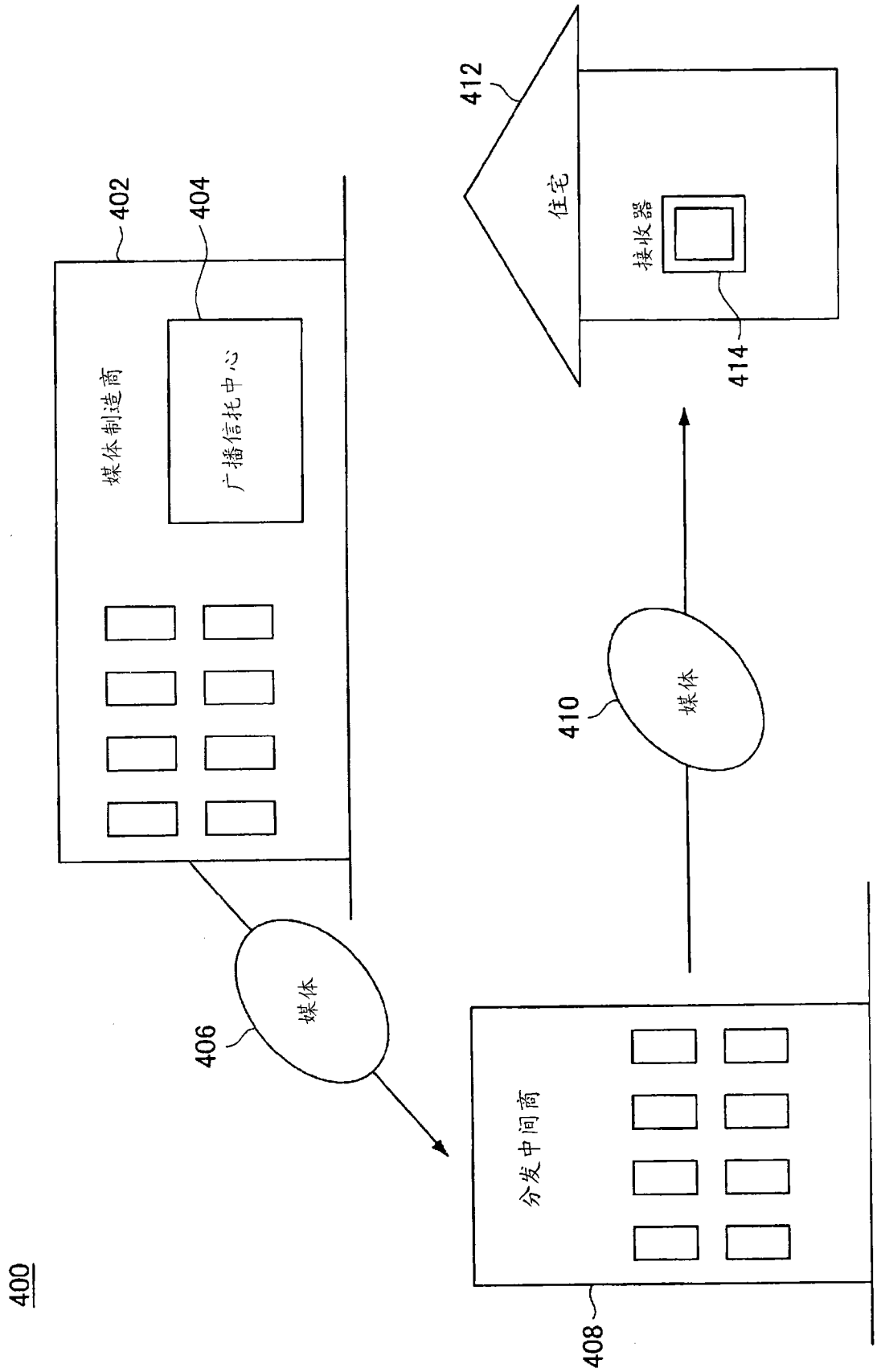


图 15

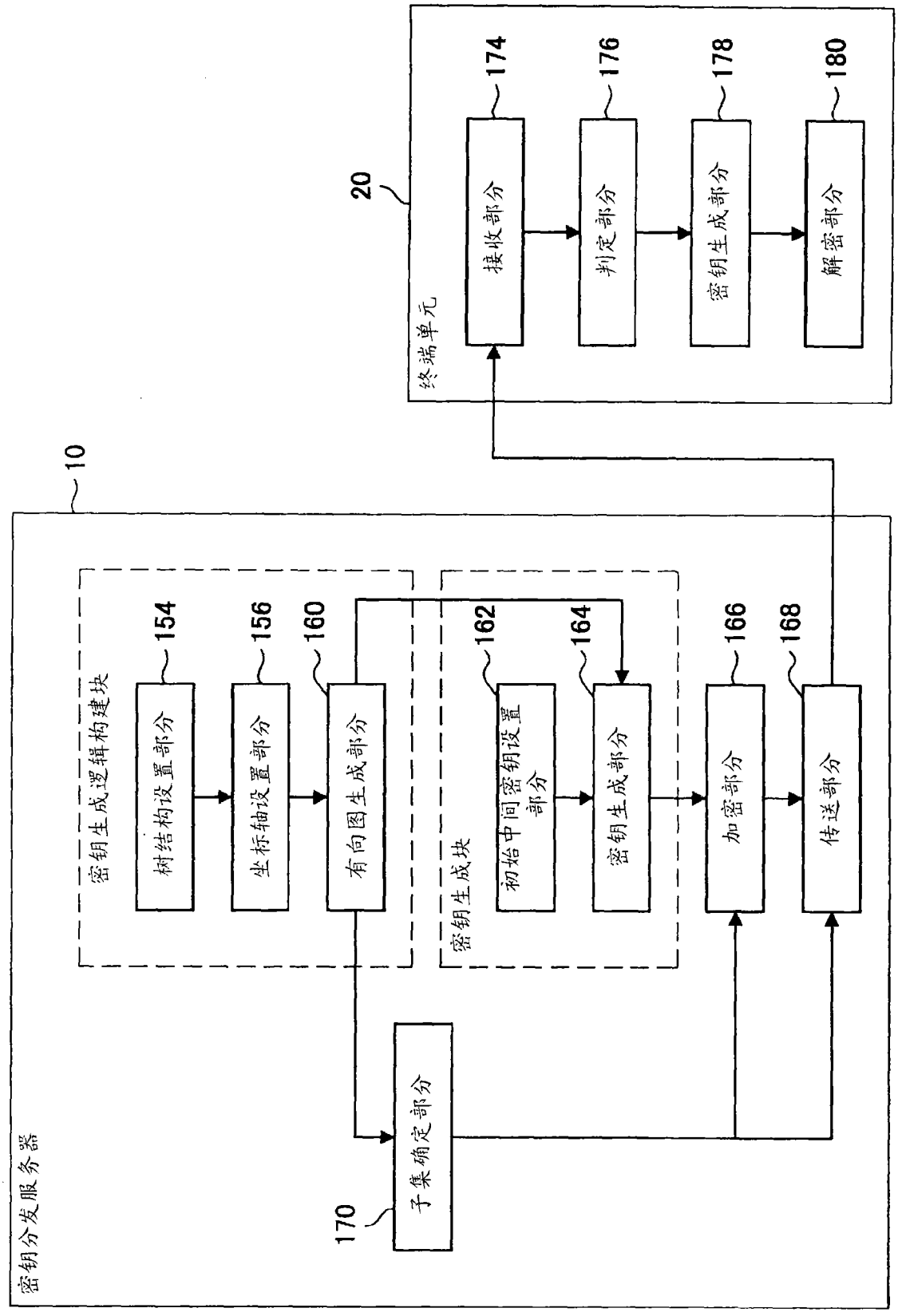

密钥分发服务器
10
密钥生成逻辑构建块
树结构设置部分
154
坐标轴设置部分
156
有向图生成部分
160
密钥生成块
初始中间密钥设置部分
162
密钥生成部分
164
加密部分
166
传送部分
168
子集确定部分
170
终端单元
20
接收部分
174
判定部分
176
密钥生成部分
178
解密部分
180

图 16

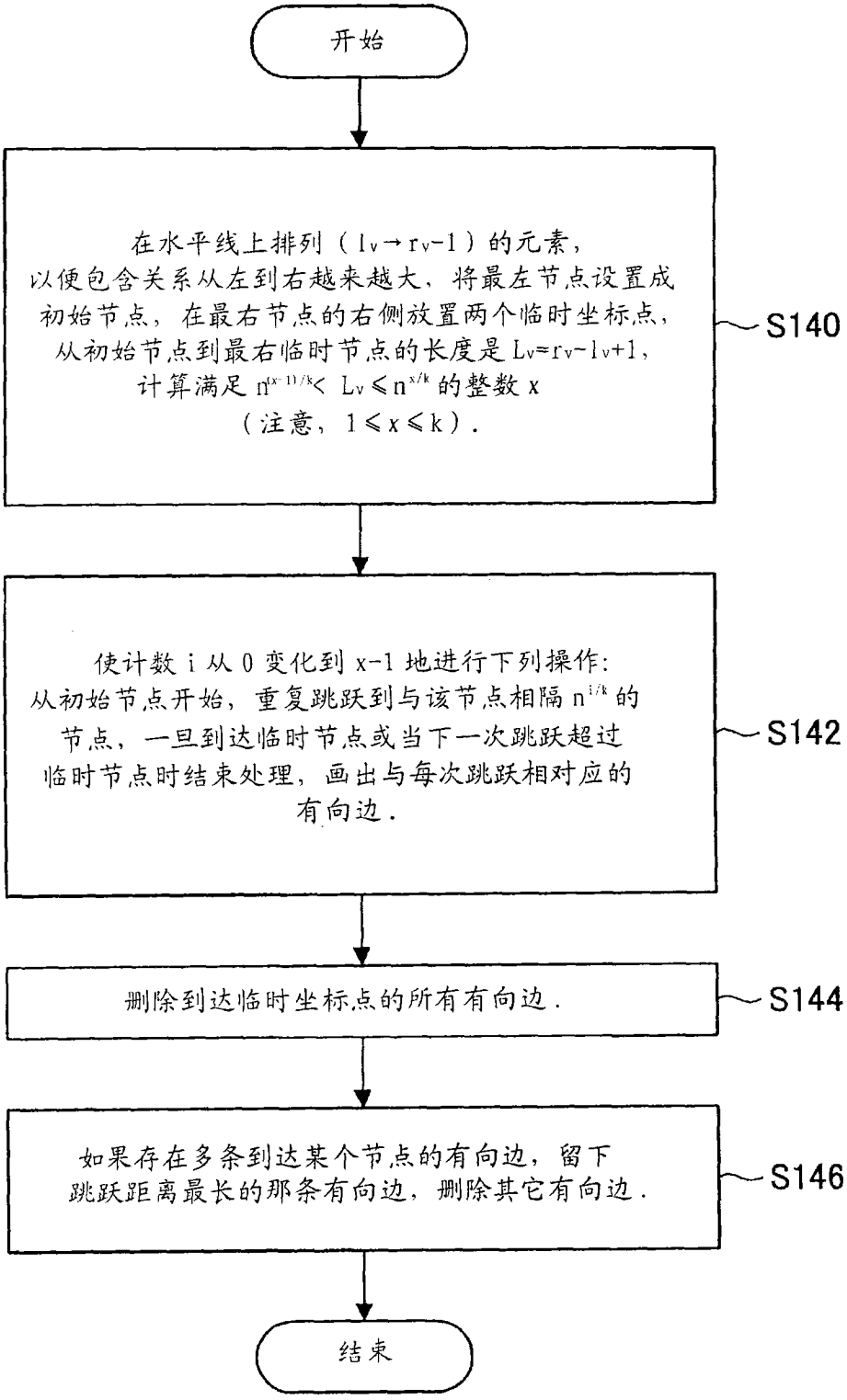

开始
在水平线上排列（$l_v \rightarrow r_v-1$）的元素，
以便包含关系从左到右越来越大，将最左节点设置成
初始节点，在最右节点的右侧放置两个临时坐标点，
从初始节点到最右临时节点的长度是 $L_v=r_v-l_v+1$，
计算满足 $n^{(x-1)/k} < L_v \leqslant n^{x/k}$ 的整数 x
（注意，$1 \leqslant x \leqslant k$）.
S140
使计数 i 从 0 变化到 x-1 地进行下列操作:
从初始节点开始，重复跳跃到与该节点相隔 $n^{i/k}$ 的
节点，一旦到达临时节点或当下一次跳跃超过
临时节点时结束处理，画出与每次跳跃相对应的
有向边.
S142
删除到达临时坐标点的所有有向边.
S144
如果存在多条到达某个节点的有向边，留下
跳跃距离最长的那条有向边，删除其它有向边.
S146
结束

图 17

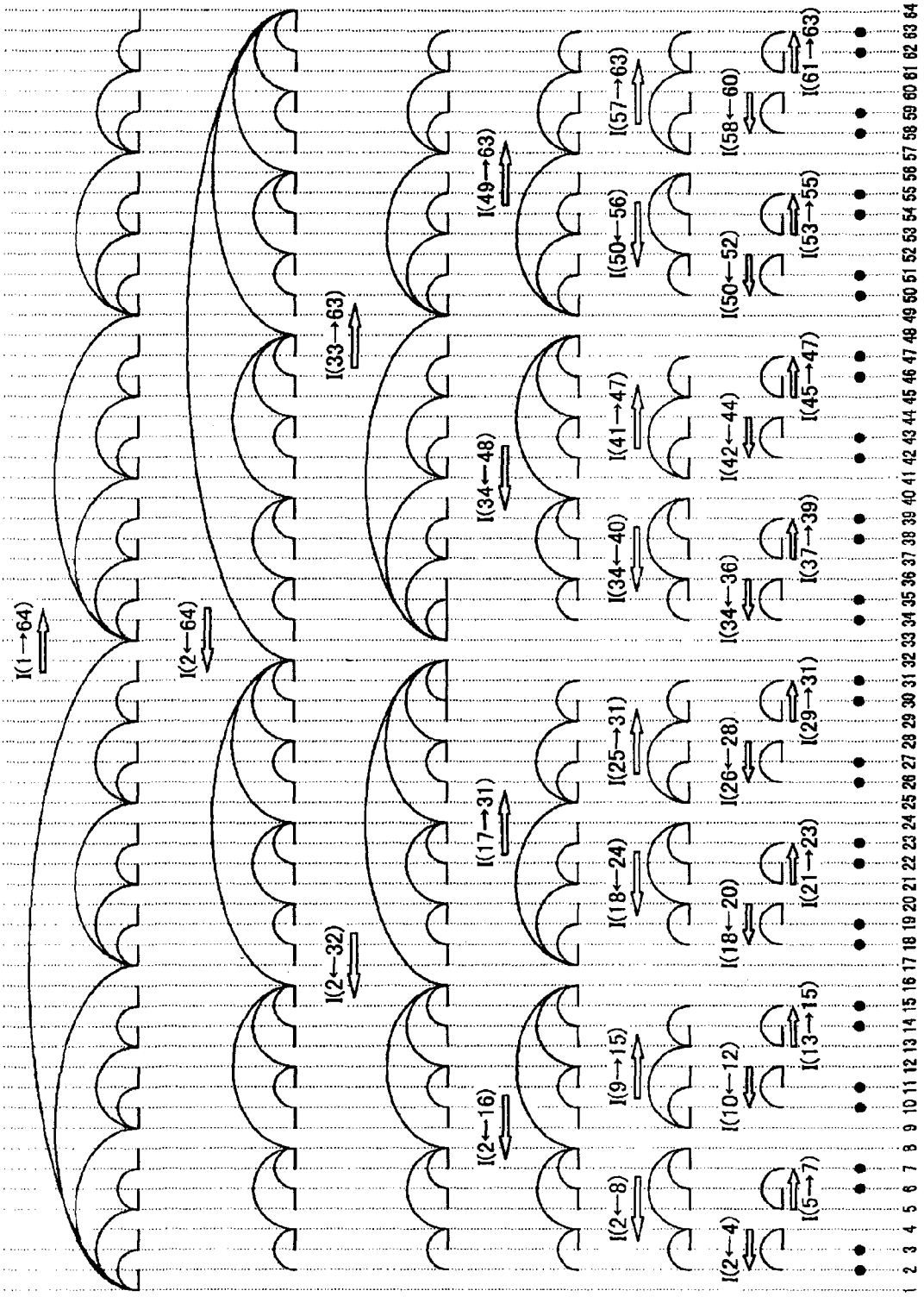

I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(17→31)
I(34←48)
I(49→63)
I(2←16)
I(9→15)
I(18←24)
I(25→31)
I(34←40)
I(41→47)
I(50←56)
I(57→63)
I(2←8)
I(5→7)
I(10←12)
I(13→15)
I(18←20)
I(21→23)
I(26←28)
I(29→31)
I(34←36)
I(37→39)
I(42←44)
I(45→47)
I(50←52)
I(53→55)
I(58←60)
I(61→63)
I(2←4)
1 2 3 4 5 6 7 8 9 10 11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

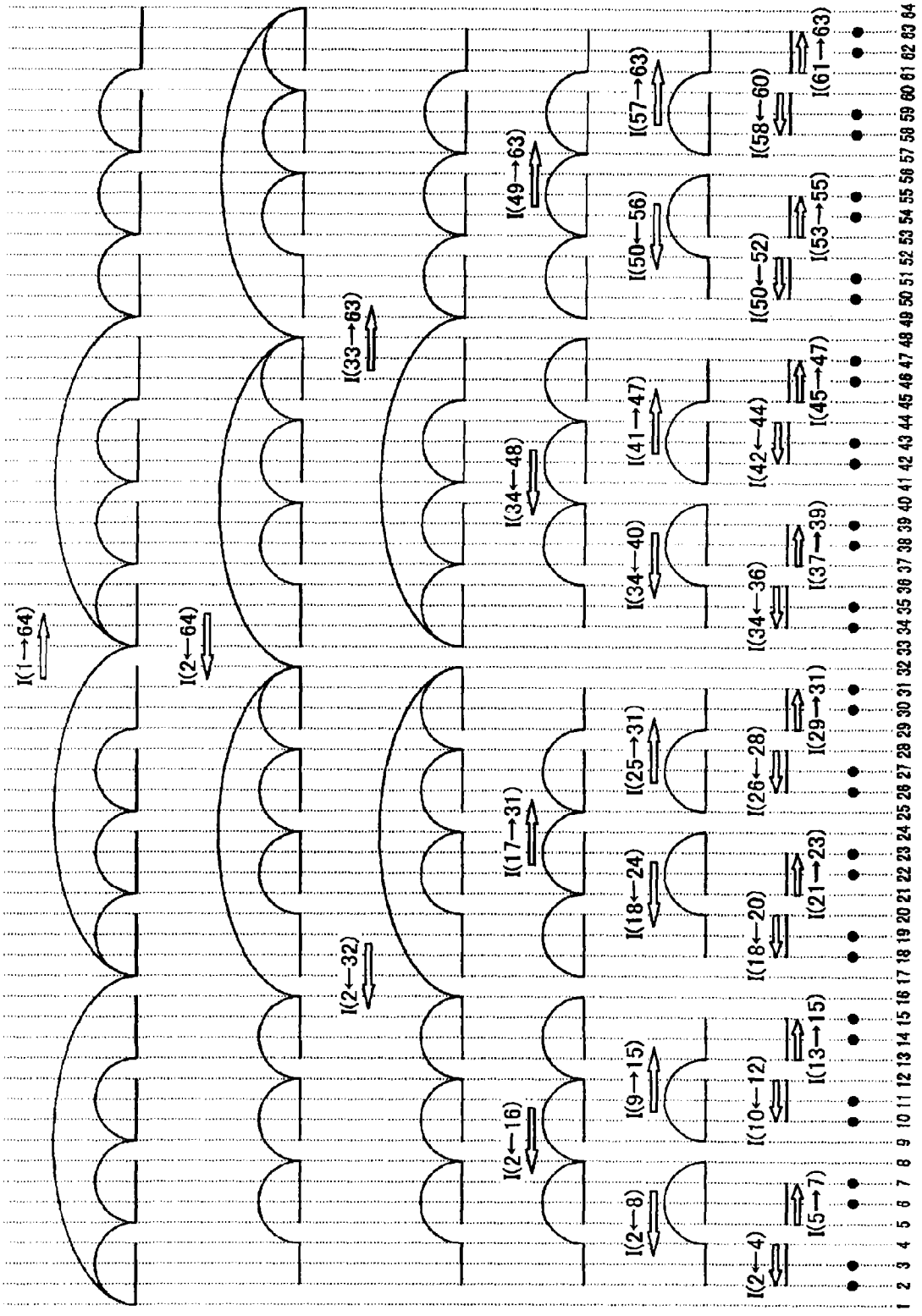

I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(17→31)
I(49→63)
I(34←48)
I(2←16)
I(9→15)
I(25→31)
I(41→47)
I(57→63)
I(2←8)
I(18←24)
I(34←40)
I(50←56)
I(5→7)
I(13→15)
I(21→23)
I(29→31)
I(37→39)
I(45→47)
I(53→55)
I(61→63)
I(2←4)
I(10←12)
I(18←20)
I(26←28)
I(34←36)
I(42←44)
I(50←52)
I(58←60)
1 2 3 4 5 6 7 8 9 10 11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