(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 101536400 B

(45)授权公告日 2013.06.26

(21)申请号 200780040810.8

(22)申请日 2007.08.17

(30)优先权数据

294639/2006 2006.10.30 JP

(85)PCT申请进入国家阶段日

2009.04.30

(86)PCT申请的申请数据

PCT/JP2007/066002 2007.08.17

(87)PCT申请的公布数据

WO2008/053629 JA 2008.05.08

(73)专利权人 索尼株式会社

地址 日本东京都

(72)发明人 草川雅文 浅野智之

(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 1656792 A,2005.08.17,

CN 1713566 A,2005.12.28,

DODIS Y 等.Public Key Broadcast Encryption for Stateless Receivers.《LECTURE NOTES IN COMPUTER SCIENCE》.2003, 第2696卷

DODIS Y 等.Public Key Broadcast Encryption for Stateless Receivers.《LECTURE NOTES IN COMPUTER SCIENCE》.2003, 第2696卷第68页第13-22行.

BONEH D 等.Collusion Reisistant Broadcast Encryption With Short Ciphertexts and Private Keys.《LECTURE NOTES IN COMPUTER SCIENCE》.2005, 第3621卷

审查员 陈晓伟

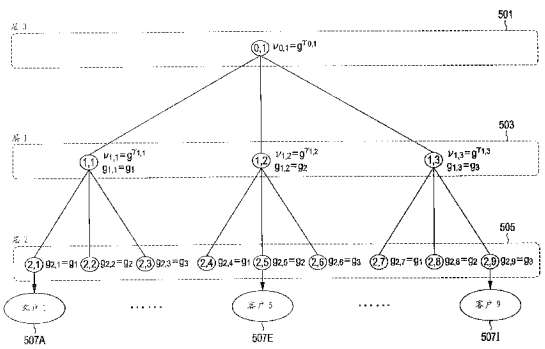
权利要求书5页 说明书30页 附图26页

(54)发明名称

密钥生成设备、加密设备、接收设备、密钥生成方法、加密方法及密钥处理方法

(57)摘要

密钥生成设备构建分配了n个接收设备的分级Y分支树结构。使用存在于该Y分支树结构的树叶和根之间的中间节点作为父节点将新参数分别提供至每个子群,以便于可以灵活地配置该子群。当不存在或存在少量待排除的合同者时,可以减小待分布的首标大小以及该合同者将要执行的运算的计算量。



CN 101536400 B

1. 一种密钥生成设备，其特征在于包括：

树结构构造单元，其分级地构造将 n 个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的 Y 元树结构，并且用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群；

随机数判定单元，其随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数；

叶密钥分配单元，其按照以下表达式 A 计算叶密钥 g_y

$g_y = g^{(\alpha)^y}$ ……表达式 A

其中，y = 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元树结构的 n 个树叶以及其所有中间节点；

参数分配单元，其向所述 Y 元树结构的所有中间节点及所述根分配作为随机整数的节点参数 $\gamma_{x,z}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式 B 所表示的参数 $v_{x,z}$：

$v_{x,z} = g^{(\gamma_{x,z})}$ ……表达式 B

其中，x：层，z：1，2，……，Y^x；以及

密钥计算单元，其识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,z}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,z}$ 次幂来计算该路径中的多组保密密钥。

2. 如权利要求 1 所述的密钥生成设备，其特征在于进一步包含传递单元，其向该树叶所对应的接收设备传递密钥计算单元计算出的该路径中的多组保密密钥。

3. 如权利要求 2 所述的密钥生成设备，其特征在于：

所述密钥计算单元基于叶密钥 g_y 和参数 $v_{x,z}$，按照以下公式来形成公钥 PK = (g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,X}$)，其中 $X = \left\lceil \frac{n}{Y} \right\rceil$；以及

所述传递单元包含公布该公钥的公钥公布部分。

4. 如权利要求 2 所述的密钥生成设备，其特征在于：所述传递单元进一步包含将所述密钥计算单元计算出的保密密钥传送至该树叶所对应的接收设备的传输部分。

5. 一种加密设备，其特征在于包括：

接收单元，其从密钥生成设备接收其所生成并公开的公钥

PK = (g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,X}$)，其中 $X = \left\lceil \frac{n}{Y} \right\rceil$ 以及生成所述公钥时所使用的素数 p、所使用的 Y 元树结构的信息以及关于非排除接收设备的组 S 的信息，其中

该 Y 元树结构的 n 个树叶中的每一个树叶对应于一个接收设备，

该 Y 元树结构的高度表示为 $H = \log_Y n$，

该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，

叶密钥 g_y 是按照以下表达式计算出的：

$$g_y = g^{(\alpha)^y}$$

其中，g 是以随机选择的素数 p 作为阶的双线性群 G 的生成元，整数 α 是随机选择的保密随机数，y ＝ 1、2、……、Y、Y+2、……、2Y，而

参数 $v_{x,z}$ 是根据以下表达式从作为随机整数分别分配给所述 Y 元树结构的所有中间节点及所述根的节点参数计算出来的：

$$v_{x,z} = g^{(r_{x,z})}$$

其中，x：层，z：1，2，……Y^x，而；

存储单元，其存储关于该素数 p 的信息、所使用的 Y 元树结构的信息、关于非排除接收设备的组 S 的信息和公钥；

排除接收设备识别单元，其识别 n 个接收设备之中的排除接收设备，并且确定非排除接收设备的组 S；

会话密钥确定单元，其随机地选择整数 t，并且确定会话密钥 $s = [e(g_Y, g_1)]^t$ 并生成首标信息，其中，$e(g_Y, g_1)$ 表示关于双线性群的两个元素 g_Y 和 g_1 的双线性映射；

内容存储单元，其存储未加密的任何内容；

加密单元，其通过使用会话密钥 s 对从内容存储单元中选择的待传递的内容加密；以及

内容传输单元，其向每个接收设备传送通过加密单元加密的已加密内容、首标信息以及排除接收设备识别单元所确定的非排除接收设备的组 S，其中，该会话密钥确定单元进一步包含

首标元素计算部分，其在分级树结构中标记在从根延伸至向其分配了排除接收设备的树叶的路径中存在的所有各节点，并且基于分配给已标记节点的参数 $v_{x,z}$ 以及分配给该已标记节点用作其父节点的中间节点的叶密钥 g_y，计算以下表达式 C 表示的 $c_{x,z}$：

$$c_{x,z} = (v_{x,z} \cdot \prod_{j \in S_{x,z}} g_{Y+1-j})^t \quad \cdots\cdots \text{表达式 C}$$

其中 $S_{x,z}$ 表示属于已标记节点用作父节点的每个子群的一组未标记子节点，x：层，z：1，2，……Y^x；以及

首标信息生成部分，其将所述首标元素计算部分得到的 $c_{x,z}$ 和 g^t 设置为首标信息。

6. 一种能够与权利要求 1 所述的密钥生成设备及加密设备通信的接收设备，包括：

接收单元，其接收密钥生成设备得到的密钥，

其特征在于：

该接收单元进一步接收作为用于识别排除接收设备的信息的、关于非排除接收设备的组 S 的信息；并且

该接收设备进一步包括

解密单元，通过使用会话密钥 s 来对经加密的内容进行解密，和

确定单元，其确定该组 S 中是否包含该接收设备，

其中在该确定单元确定组 S 中包含接收设备的情况下，解密单元通过基于以下所示的表达式 D 计算会话密钥 s 并且使用计算出的会话密钥 s 来对经加密的内容进行解密：

$$s=\frac{e(g_{i_{x'}},c_{x,z})}{e(g_{i_{x'}}^{\gamma_{i_{x'-1}}}\cdot\prod_{j\in S_{x,z},j\neq i_{x'}}g_{Y+1-j+i_{x'}},g')}\cdots\cdots$$ 表达式 D

其中 e(u,v) 表示关于双线性群的两个元素 u 和 v 的双线性映射，组 S 中包含的节点的节点索引被设置为（x′，z′）并由下面的表达式表示节点（x′，z′）与其父节点（x，z）的关系：

$$(x,z)=(x'-1,\lceil z'/Y\rceil)$$

$c_{x,z}=(v_{x,z}\cdot\prod_{j\in S_{x,z}}g_{Y+1-j})^{t}$，t 表示随机地选择的整数，而 $i_{x'}$ 表示层 x′ 中的接收设备 i 的索引。

7. 一种密钥生成方法，其特征在于包括：

树结构构造步骤，其分级地构造将 n 个接收设备分配给树叶并且由 $H=\log_Y n$ 表示高度的 Y 元树结构，并且用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群；

随机数判定步骤，其随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数；

叶密钥分配步骤，其按照以下表达式计算叶密钥 g_y

$$g_y=g^{(\alpha)^y}$$

其中，y = 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元树结构的 n 个树叶以及其所有中间节点；

参数分配步骤，其向所述 Y 元树结构的所有中间节点及所述根分配作为随机整数的节点参数 $\gamma_{x,z}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式所表示的参数 $v_{x,z}$：

$$v_{x,z}=g^{(\gamma_{x,z})}$$

其中，x：层，z：1，2，……Y^x，而 $\gamma_{x,z}$ 表示作为随机整数的节点参数；以及

密钥计算步骤，其识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,z}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,z}$ 次幂来计算该路径中的多组保密密钥。

8. 一种加密方法，其特征在于包括

接收步骤，其从密钥生成设备接收其所生成并公开的公钥

PK =（g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,X}$），其中 $X=\left\lceil\frac{n}{Y}\right\rceil$ 以及生成所述公钥时所使用的素数 p、所使用的 Y 元树结构的信息以及关于非排除接收设备的组 S 的信息，其中

该 Y 元树结构的 n 个树叶分别对应于一个接收设备，

该 Y 元树结构的高度表示为 $H=\log_Y n$，

该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，

叶密钥 g_y 是按照以下表达式计算出的：

$$g_y = g^{(\alpha)^y}$$

其中，g 是以随机选择的素数 p 作为阶的双线性群 G 的生成元，整数 α 是随机选择的保密随机数，y ＝ 1、2、……、Y、Y+2、……、2Y，而

参数 $v_{x,z}$ 分别是根据以下表达式从作为随机整数分别分配给所述 Y

元树结构的所有中间节点及所述根的节点参数计算出的：

$$v_{x,z} = g^{(\gamma_{x,z})}$$

其中，x：层，z：1，2，……Y^x；

存储步骤，其存储关于该素数 p 的信息、所使用的 Y 元树结构的信息、关于非排除接收设备的组 S 的信息和公钥；

排除接收设备识别步骤，其识别 n 个接收设备之中的排除接收设备，并且确定非排除接收设备的组 S；

会话密钥确定步骤，其随机地选择整数 t，并且确定会话密钥 $s = [e(g_Y, g_1)]^t$，其中，$e(g_Y, g_1)$ 表示关于双线性群的两个元素 g_Y 和 g_1 的双线性映射；

首标元素计算步骤，其在分级树结构中标记在从根延伸至向其分配了排除接收设备的树叶的路径中存在的所有各节点，并且基于分配给已标记节点的参数 $v_{x,z}$ 以及分配给该已标记节点用作其父节点的中间节点的叶密钥 g_y，计算以下表达式 C 表示的 $c_{x,z}$：

$$c_{x,z} = (v_{x,z} \cdot \prod_{j \in S_{x,z}} g_{Y+1-j})^t$$

其中 $S_{x,z}$ 表示属于已标记节点用作父节点的每个子群的一组未标记子节点，x：层，z：1，2，……Y^x；

首标信息生成步骤，其将所述首标元素计算步骤得到的 $c_{x,z}$ 和 g^t 设置为首标信息；

加密步骤，其通过 $E_s(M)$ 使用会话密钥 s 对待传递的内容加密，$E_s(M)$ 表示通过使用密钥 s 对纯文本 M 的加密；以及

内容传输步骤，其向每个接收设备传送已加密内容、首标信息以及非排除接收设备的组 S。

9. 一种密钥处理方法，其特征在于包括接收通过如下处理得到的密钥的步骤，所述处理包含：

分级地构造将 n 个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的 Y 元树结构，

用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，

随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数，

按照以下表达式计算叶密钥 g_y

$$g_y = g^{(\alpha)^y}$$

其中，y ＝ 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元树结构的 n 个树叶以及其所有中间节点，

向所述 Y 元树结构的所有中间节点及所述 Y 元树结构的根分配作为随机整数的节点参数 $\gamma_{x,z}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式所表示的参数 $v_{x,z}$：

$$v_{x,z} = g^{(\gamma_{x,z})}$$

识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,z}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,z}$ 次幂来计算该路径中的多组保密密钥，其中，x：层，z：1，2，……Y^x。

密钥生成设备、加密设备、接收设备、密钥生成方法、加密方法及密钥处理方法

技术领域

[0001] 本发明涉及密钥生成设备、加密设备、接收设备、密钥生成方法、加密方法、密钥处理方法以及程序。

[0002] 背景技术

[0003] 近年来，不仅由于个人计算机 (PC) 的普遍使用，而且由于便携式电话、数字家用电器等的普遍使用，针对音乐、图像等的内容传递业务 (delivery business) 已经变得越来越重要。例如，作为内容传递业务，存在使用有线电视、卫星广播或因特网的付费广播，使用诸如 CD 或 DVD 之类的物理介质的内容的销售等。在任意这些情况下，均需要配置仅有客户才可获取内容的机制。

[0004] 通常，在这种内容传递系统中，系统的管理员（在下文中，称为中心）预先仅向客户提供密钥，并且在内容传递时，传递已经通过使用会话密钥 s 对内容 M 加密而生成的加密文本 C，以及用于仅允许该客户获取会话密钥 s 的首标 h。因此，只有该客户可获取内容 M。

[0005] 作为用于实现上述情形的内容传递方法，例如，使用公钥的方法是可用的（例如，见非专利文献 1）。

[0006] 非专利文献 1 :D.Boneh,C.Gentry,B.Waters,″ Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys″ , CRYPTO′ 05, Proceedings of 25th Annual International Cryptology Conference on Advances in Cryptology, London,UK,Springer Verlag,2005,58-75 页。

[0007] 发明内容

[0008] 技术问题

[0009] 然而，在上述非专利文献 1 描述的公钥加密方法中，即使在对其取消传递的排除用户的数量很少的情况下，也总是需要传递恒定大小的首标 h。因 此在实际可能的情形（诸如，排除客户的数量为零的情况或者排除用户的数量相对于用户的总数的百分比很小的情况）下，不能降低首标大小。因此，存在在传递已加密内容时数据冗余度增大的问题。

[0010] 因此，鉴于上述问题作出本发明。本发明的目的是提供 :即使在排除用户的数量很小的情况下也能够降低首标大小的、新颖的并且改进的密钥生成设备、加密设备、接收设备、密钥生成方法、加密方法、密钥处理方法以及程序。

[0011] 技术方案

[0012] 为了实现上述目的，根据本发明的第一方面，提供密钥生成设备，其包含 :树结构构造单元，其分级地构造将 n 个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的 Y 元树结构，并且用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群 ;随机数判定单元，其随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数 ;叶密钥分配单元，其按照以下表达式 A 计算叶密钥 g_y

[0013] $g_y = g^{(\alpha)^y}$……表达式 A

[0014] 其中，y ＝ 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元树结构的 n 个树叶以及其所有中间节点；参数分配单元，其向所述 Y 元树结构的所有中间节点及所述根分配作为随机整数的节点参数 $\gamma_{x,y}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式 B 所表示的参数 $v_{x,y}$：

[0015] $v_{x,y} = g^{(\gamma_{x,y})}$……表达式 B

[0016] 其中，x：层，y：1，2，……Y^x；以及密钥计算单元，其识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,y}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,y}$ 次幂来计算该路径中的多组保密密钥。

[0017] 上述密钥生成设备可配置为进一步包含传递单元，其向该树叶所对应的接收设备传递密钥计算单元计算出的该路径中的多组保密密钥。

[0018] 上述密钥计算单元可基于叶密钥 g_y 和参数 $v_{x,y}$，按照以下公式来形成公钥

[0019] PK ＝（g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,x}$）

[0020] 其中

[0021] $X = \left\lceil \frac{n}{Y} \right\rceil$ 以及；

[0022] 上述传递单元可包含公布该公钥的公钥公布部分。

[0023] 上述传递单元可进一步包含将密钥计算单元计算出的保密密钥传送至该树叶所对应的接收设备的传输部分。

[0024] 为了取得上述目的，根据本发明的第二方面，提供一种加密设备，其特征在于包括：接收单元，其从密钥生成设备接收其所生成并公开的公钥

[0025] PK ＝（g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,X}$）以及生成所述公钥时所使用的素数 p、所使用的 Y 元树结构的信息以及关于非排除接收设备的组 S 的信息，其中该 Y 元树结构的 n 个树叶中的每一个树叶对应于一个接收设备，该 Y 元树结构的高度表示为 H ＝ $\log_Y n$，该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，叶密钥 g_y 是按照以下表达式计算出的：

[0026] $g_y = g^{(\alpha)^y}$

[0027] 其中，g 是以随机选择的素数 p 作为阶的双线性群 G 的生成元，整数 α 是随机选择的保密随机数，y ＝ 1、2、……、Y、Y+2、……、2Y，而参数 $v_{x,y}$ 是根据以下表达式计算出来的：

[0028] $v_{x,y} = g^{(\gamma_{x,y})}$

[0029] 其中，x：层，y：1，2，……Y^x；存储单元，其存储关于该素数 p 的信息、所使用的 Y 元树结构的信息、关于非排除接收设备的组 S 的信息和公钥；排除接收设备识别单元，其识别 n 个接收设备之中的排除接收设备，并且确定非排除接收设备的组 S；会话密钥确定单

元，其随机地选择整数 t，并且确定会话密钥 $s = [e(g_Y, g_1)]^t$ 并生成首标信息，其中，$e(g_Y, g_1)$ 表示关于双线性群的两个元素 g_Y 和 g_1 的双线性映射；内容存储单元，其存储未加密的任何内容；加密单元，其通过使用会话密钥 s 对从内容存储单元中选择的待传递的内容加密；以及内容传输单元，其向每个接收设备传送通过加密单元加密的已加密内容、首标信息以及排除接收设备识别单元所确定的非排除接收设备的组 S，其中，该会话密钥确定单元进一步包含首标元素计算部分，其在分级树结构中标记在从根延伸至向其分配了排除接收设备的树叶的路径中存在的所有各节点，并且基于分配给已标记节点的参数 $v_{x,y}$ 以及分配给该已标记节点用作其父节点的中间节点的叶密钥 g_y，计算以下表达式 C 表示的 $c_{x,y}$：

[0030] $$c_{x,y} = (v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t$$ ……表达式 C

[0031] 其中 $S_{x,y}$ 表示属于已标记节点用作父节点的每个子群的一组未标记子节点，x：层，y：1，2，……Y^x；以及首标信息生成部分，其将所述首标元素计算部分得到的 $c_{x,y}$ 和 g^t 设置为首标信息。为了取得上述目的，根据本发明的第三方面，提供能够与密钥生成设备及加密设备通信的接收设备，该接收设备包括：接收单元，其接收密钥生成设备得到的密钥，其中，该密钥生成设备分级地构造将 n 个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的 Y 元树结构，用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数，按照以下表达式计算叶密钥 g_y

[0032] $$g_y = g^{(\alpha)^y}$$

[0033] 其中，y = 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元树结构的 n 个树叶以及其所有中间节点，向所述 Y 元树结构的所有中间节点及所述根分配作为随机整数的节点参数 $\gamma_{x,y}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式所表示的参数 $v_{x,y}$：

[0034] $$v_{x,y} = g^{(\gamma_{x,y})}$$

[0035] 识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,y}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,y}$ 次幂来计算该路径中的多组保密密钥，其中，x：层，y：1，2，……Y^x。

[0036] 为了取得上述目的，根据本发明的第四方面，提供密钥生成方法，其包含：树结构构造步骤，其分级地构造将 n 个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的 Y 元树结构，并且用该 Y 元树结构中任意能够与树叶和根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群；随机数判定步骤，其随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数；叶密钥分配步骤，其按照以下表达式计算叶密钥 g_y

[0037] $$g_y = g^{(\alpha)^y}$$

[0038] 其中，y = 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所述 Y 元

树结构的n个树叶以及其所有中间节点；参数分配步骤，其向所述Y元树结构的所有中间节点及所述根分配作为随机整数的节点参数 $\gamma_{x,y}$，并向所述Y元树结构的所有中间节点及所述根分配以下表达式所表示的参数 $v_{x,y}$：

[0039] $$v_{x,y} = g^{(\gamma_{x,y})}$$

[0040] 其中，x：层，y：1，2，……Y^x；以及密钥计算步骤，其识别从所述Y元树结构的根延伸至所述Y元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,y}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,y}$ 次幂来计算该路径中的多组保密密钥。

[0041] 为了取得上述目的，根据本发明的第五方面，提供一种加密方法，其特征在于包括接收步骤，其从密钥生成设备接收其所生成并公开的公钥

[0042] $PK = (g、g_1、\cdots\cdots、g_Y、g_{Y+2}、\cdots\cdots、g_{2Y}、v_{0,1}、\cdots\cdots、v_{H-1,X})$

[0043] 以及生成所述公钥时所使用的素数p、所使用的Y元树结构的信息以及关于非排除接收设备的组S的信息，其中该Y元树结构的n个树叶分别对应于一个接收设备，该Y元树结构的高度表示为 $H = \log_y n$，该Y元树结构中任意能够与树叶和根之间存在的中间节点形成Y元子树结构的Y个树叶构成子群，叶密钥 g_y 是按照以下表达式计算出的：

[0044] $$g_y = g^{(\alpha)^y}$$

[0045] 其中，g是以随机选择的素数p作为阶的双线性群G的生成元，整数 α 是随机选择的保密随机数，y = 1、2、……、Y、Y+2、……、2Y，而参数 $v_{x,y}$ 分根据以下表达式计算出的：

[0046] $$v_{x,y} = g^{(\gamma_{x,y})}$$

[0047] 其中，x：层，y：1，2，……Y^x；存储步骤，其存储关于该素数p的信息、所使用的Y元树结构的信息、关于非排除接收设备的组S的信息和公钥；排除接收设备识别步骤，其识别n个接收设备之中的排除接收设备，并且确定非排除接收设备的组S；会话密钥确定步骤，其随机地选择整数t，并且确定会话密钥 $s = [e(g_Y, g_1)]^t$，其中，$e(g_Y, g_1)$ 表示关于双线性群的两个元素 g_Y 和 g_1 的双线性映射；首标元素计算步骤，其在分级树结构中标记在从根延伸至向其分配了排除接收设备的树叶的路径中存在的所有各节点，并且基于分配给已标记节点的参数 $v_{x,y}$ 以及分配给该已标记节点用作其父节点的中间节点的叶密钥 g_y，计算以下表达式C表示的 $c_{x,y}$：

[0048] $$c_{x,y} = (v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t$$

[0049] 其中 $S_{x,y}$ 表示属于已标记节点用作父节点的每个子群的一组未标记子节点，x：层，y：1，2，……Y^x；首标信息生成步骤，其将所述首标元素计算步骤得到的 $c_{x,y}$ 和 g^t 设置为首标信息；加密步骤，其通过使用会话密钥s对待传递的内容加密；以及内容传输步骤，其向每个接收设备传送已加密内容、首标信息以及非排除接收设备的组S。

[0050] 为了取得上述目的，根据本发明的第六方面，提供一种密钥处理方法，其特征在于包括接收通过如下处理得到的密钥的步骤，所述处理包含：分级地构造将n个接收设备分配给树叶并且由 $H = \log_Y n$ 表示高度的Y元树结构，用该Y元树结构中任意能够与树叶和

根之间存在的中间节点形成 Y 元子树结构的 Y 个树叶构成子群，随机地选择素数 p 以确定将该素数 p 作为阶的双线性群 G，随机地选择用作 G 的生成元的 g，并且随机地选择保密随机数 α，其中 α 是整数，按照以下表达式计算叶密钥 g_y

[0051] $$g_y = g^{(\alpha)^y}$$

[0052] 其中，y = 1、2、……、Y、Y+2、……、2Y，并且将算出的叶密钥 g_y 分配给所 述 Y 元树结构的 n 个树叶以及其所有中间节点，向所述 Y 元树结构的所有中间节点及所述 Y 元树结构的根分配作为随机整数的节点参数 $\gamma_{x,y}$，并向所述 Y 元树结构的所有中间节点及所述根分配以下表达式所表示的参数 $v_{x,y}$：

[0053] $$v_{x,y} = g^{(\gamma_{x,y})}$$

[0054] 识别从所述 Y 元树结构的根延伸至所述 Y 元树结构的树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点及根分配的节点参数 $\gamma_{x,y}$，通过求该叶密钥 g_y 的参数 $\gamma_{x,y}$ 次幂来计算该路径中的多组保密密钥，其中，x：层，y：1，2，……Y^x。

[0055] 为了取得上述目的，根据本发明的第七方面，提供用于促使计算机实现以下功能的程序：树结构构造功能，其分级地构造将 n 个接收设备分配给树叶并且由 $\log_Y n$ 表示高度的 Y 元树结构，并且形成由比树叶和根之间存在的中间节点更低的层中存在的多个树叶构成的子群；叶密钥分配功能，其将叶密钥 g_y 分配给各树叶以及各中间节点；参数分配功能，其向所述各中间节点及所述根分配不同的参数 $v_{x,y}$（x：层，y：1，2，……Y^x）及节点参数 $\gamma_{x,y}$（x：层，y：1，2，……Y^x）；以及密钥计算功能，其识别从所述根延伸至所述树叶的路径，并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点或该树叶的父节点分配的参数 $v_{x,y}$ 和节点参数 $\gamma_{x,y}$ 来计算密钥。

[0056] 根据该配置，通过将计算机程序存储在计算机中提供的存储单元中并且由计算机中提供的 CPU 来读取和执行该计算机程序，该计算机程序促使计算机用作上述的密钥生成设备。另外，也可提供具有记录在其上的计算机程序的计算机可读记录介质。例如，该记录介质是磁盘、光盘、磁光盘、闪存等。另外，例如，可以经由网络传递上述计算机程序，而无需使用所述记录介质。

[0057] 为了取得上述目的，根据本发明的第八方面，提供用于促使计算机实现排除接收设备识别功能的程序，该排除接收设备识别功能识别 n 个接收设备之中的排除接收设备，并且确定非排除接收设备的组 S。

[0058] 根据该配置，通过将计算机程序存储在计算机中提供的存储单元中并且由计算机中提供的 CPU 来读取和执行该计算机程序，该计算机程序促使计算机用作上述的加密设备。另外，也可提供具有记录在其上的计算机程序的计 算机可读记录介质。例如，该记录介质是磁盘、光盘、磁光盘、闪存等。另外，例如，可以经由网络传递上述计算机程序，而无需使用所述记录介质。

[0059] 为了取得上述目的，根据本发明的第九方面，提供用于促使计算机实现接收通过如下处理得到的加密密钥的接收功能的程序，所述处理包含：分级地构造将 n 个接收设备分配给树叶并且由 $\log_Y n$ 表示高度的 Y 元树结构，形成由比树叶和根之间存在的中间节点更低的层中存在的多个树叶构成的子群，将叶密钥 g_y 分配给各树叶以及各中间节点，向所

述各中间节点及所述根分配不同的参数 $v_{x,y}$(x :层,y :1,2,……Y^x) 及节点参数 $Y_{x,y}$(x :层,y :1,2,……Y^x),识别从所述根延伸至所述树叶的路径,并且基于向所述路径中存在的中间节点或树叶分配的叶密钥 g_y 以及向该中间节点或该树叶的父节点分配的参数 $v_{x,y}$ 和节点参数 $Y_{x,y}$ 来计算密钥。

[0060] 根据该配置,通过将计算机程序存储在计算机中提供的存储单元中并且由计算机中提供的 CPU 来读取和执行该计算机程序,该计算机程序促使计算机用作上述接收设备。另外,也可提供具有记录在其上的计算机程序的计算机可读记录介质。例如,该记录介质是磁盘、光盘、磁光盘、闪存等。另外,例如,可以经由网络传递上述计算机程序,而无需使用所述记录介质。

[0061] 有益效果

[0062] 根据本发明,即使在排除客户的数量很小的情况下,也可以减小首标大小。

[0063] 附图说明

[0064] 图 1 是用于根据本发明的优选实施例说明加密密钥生成系统的说明图。

[0065] 图 2 是用于根据实施例说明密钥生成设备的硬件配置的框图。

[0066] 图 3 是用于根据本发明的基础技术的基本方法说明密钥生成的概况的说明图。

[0067] 图 4 是用于根据本发明的基础技术的一般化方法说明密钥生成的概况的流程图。

[0068] 图 5 是用于根据本发明的基础技术的一般化方法说明密钥生成阶段的流程图。

[0069] 图 6 是用于根据本发明的基础技术的一般化方法说明加密的概况的说明图。

[0070] 图 7 是用于根据本发明的基础技术的一般化方法说明加密阶段的说明图。

[0071] 图 8 是用于根据本发明的基础技术的一般化方法说明解密阶段的说明图。

[0072] 图 9 是用于根据本发明的优选实施例说明密钥生成设备的配置的框图。

[0073] 图 10 是用于根据实施例说明加密设备的配置的框图。

[0074] 图 11 是用于根据实施例说明接收设备的配置的框图。

[0075] 图 12 是用于根据实施例说明逻辑树的具体示例的说明图。

[0076] 图 13 是用于根据实施例说明密钥生成的概况的说明图。

[0077] 图 14 是用于根据实施例说明密钥生成阶段的流程图。

[0078] 图 15 是用于根据实施例说明密钥生成的具体示例的说明图。

[0079] 图 16 是用于根据实施例说明加密的概况的说明图。

[0080] 图 17 是用于根据实施例说明加密阶段的流程图。

[0081] 图 18 是用于根据实施例说明加密的具体示例的说明图。

[0082] 图 19 是用于根据实施例说明加密的具体示例的说明图。

[0083] 图 20 是用于根据实施例说明加密的具体示例的说明图。

[0084] 图 21 是用于根据实施例说明解密阶段的流程图。

[0085] 图 22 是用于根据实施例说明解密的具体示例的说明图。

[0086] 图 23 是执行传递给客户的首标的首标大小方面的比较的曲线图。

[0087] 图 24 是执行双线性群上的乘法的数量方面的比较的曲线图。

[0088] 图 25 是执行传递给客户的首标的首标大小方面的比较的曲线图。

[0089] 图 26 是执行双线性群上的乘法的数量方面的比较的曲线图。

具体实施方式

[0090] 在下文中，参考附图详细描述本发明的优选实施例。注意，在说明书和附图中，通过将相同的符号提供给具有基本上相同功能配置的组件，冗余说明将被省略。

[0091] （第一实施例）

[0092] 在下文中，详细描述根据本发明第一实施例的加密密钥传递系统。

[0093] 图 1 是示出根据本实施例的加密密钥传递系统 10 的说明图。例如，加密密钥传递系统 10 包含：通信网络 12、密钥生成设备 20、加密设备 30、接收设备 40A 以及接收设备 40B。

[0094] 通信网络 12 是用于连接密钥生成设备 20、加密设备 30 以及接收设备 40 以便于可以实现双向通信或单向通信的通信线网络。例如，该通信网络由公共线路网络（诸如因特网、电话网络、卫星通信网络或广播通信信道）、专用线路网络（诸如 WAN（广域网，Wide Area Network）、LAN（局域网，Local AreaNetwork）、IP-VPN（因特网协议虚拟专用网，Internet Protocol-Virtual PrivateNetwork）或无线 LAN）等构成。该通信网络可以是有线的或无线的。

[0095] 密钥生成设备 20 生成公钥 (public key) 以及对于多个接收设备中的每一个均唯一的保密密钥。密钥生成设备 20 公布公钥，并且将各保密密钥经由安全通信信道传递给相应接收设备。注意，执行公钥和保密密钥的生成及管理的中心拥有密钥生成设备 20。

[0096] 加密设备 30 通过使用密钥生成设备 20 生成并公布的公钥来对任何内容加密，并且将经加密的内容经由通信网络 12 传递给每个接收设备。加密设备 30 可由任意第三方拥有。另外，加密设备 30 可由密钥生成设备 20 的拥有者或接收设备 40 的拥有者拥有。

[0097] 每一个接收设备 40 均能够通过使用唯一的保密密钥来对从加密设备 30 传递的经加密内容进行解密，并且能够使用经解密的内容。注意，接收设备 40A 和接收设备 40B 可以经由通信网络 12 或线 (wire) 来彼此连接。注意，接收设备 40 由各客户拥有。

[0098] 注意，虽然在图解实施例中将诸如个人计算机 (Personal Computer：PC) 之类的计算机设备（无论是笔记本型设备或台式型设备）显示为接收设备 40，但是接收设备 40 并不限于本示例。只要接收设备 40 是具有经由网络的通信功能的设备，那么就可以将其配置为例如用于电视广播的信息装置（诸如 PDA（个人数字助理）、家用游戏机、DVD/HDD 记录器或电视接收器）、调谐器或解码器等。可替换地，接收设备 40 可以是客户可携带的便携式设备 (Portable Device)，诸如，例如便携式游戏机、便携式电话、便携式视频 / 音频播放器、PDA 或 PHS。

[0099] 接下来参考图 2 简要说明根据本实施例的密钥生成设备 20 的硬件配置。

[0100] 图 2 是示出密钥生成设备 20 的硬件配置的框图。例如，密钥生成设备 20 包含：CPU（中央处理单元）201、ROM（只读存储器）203、RAM（随机存取存储器）205、HDD（硬盘驱动器）207、加密处理单元 209 以及存储器（安全模块）211。

[0101] CPU 201 用作运算处理设备以及控制设备。CPU 201 根据各种程序控制密钥生成设备 20 内的一般运算。ROM 203 存储 CPU 201 使用的程序、运算参数等。RAM 205 临时存储 CPU 201 执行中使用的程序，在该程序的执行中适当变化的参数等。

[0102] HDD207 是用于被配置为根据本实施例的密钥生成设备 20 的存储单元的示例的数据存储的设备。HDD 207 驱动硬盘，并且存储 CPU 201 执行的程序以及各种数据。加

密处理单元 209 在 CPU 201 的控制下，执行根据本实施例的密钥生成设备 20 所执行的各种类型的加密处理。存储器（安全模块）211 主要用于安全地存储需要隐藏的信息，诸如私钥 (private secret key) 以及中心保密随机数。存储在存储器 211 内部的信息具有从外界不可查阅该信息的特性。另外，例如，存储器（安全模块）211 可由具有防止篡改 (tamper-resistant) 性质的存储设备构成。注意，虽然给出了指示安全模块为存储器的描述，但是，根据本发明的安全模块不限于存储器。例如，安全模块可以是磁盘、光盘或磁光盘。可替代地，安全模块可以是诸如半导体存储器之类的存储介质。

[0103] CPU 201、ROM 203、RAM 205、HDD 207、加密处理单元 209 以及存储器 211 通过由 CPU 总线等构成的总线 213 而相互连接。

[0104] 总线 213 通过桥接器与诸如 PCI（外围组件互连 / 接口）总线之类的输入 / 输出接口 215 相连接。

[0105] 输入单元 217 例如由用户操作的操作部件（诸如鼠标、键盘、触摸板、按钮、开关以及控制杆）、输入控制电路（用于基于用户的操作生成输入信号并且将该输入信号输出至 CPU 201）等构成。通过操作输入单元 217，密钥生成设备 20 的用户能够将各种数据输入至密钥生成设备 20，并且能够指令密钥生 成设备 20 执行处理操作。

[0106] 输出单元 219 例如由显示设备（诸如 CRT（阴极射线管）显示设备或液晶显示 (LCD) 设备以及灯）、音频输出设备（诸如扬声器和听筒）等构成。输出单元 219 例如能够输出再现内容。具体地，显示设备以文本或图像的形式显示诸如再现的视频数据之类的各种类型信息。同时，音频输出设备将再现的音乐数据等转换为声音，并且输出该声音。

[0107] 通信单元 221 是例如由用于允许与通信网络 12 的连接的通信设备等构成的通信接口。通信单元 221 经由通信网络 12，将诸如关于加密密钥的信息以及内容信息之类的各种数据传送至例如加密设备 30，以及从接收设备 40A 和 40B 接收诸如关于加密密钥的信息以及内容信息之类的各种数据。

[0108] 驱动器 223 是存储介质的读取器 / 写入器。驱动器 223 包含在密钥生成设备 20 中，或者外部地提供。驱动器 223 读取所加载的可拆卸记录介质 14（诸如磁盘、光盘、磁光盘或半导体存储器）上记录的信息，并且将该信息输出至 RAM 205。

[0109] 注意，由于加密设备 30 和接收设备 40 的硬件配置与密钥生成设备 20 的硬件配置基本相同，因此省略加密设备 30 和接收设备 40 的硬件配置的描述。

[0110] 以上已经描述了能够实施根据本实施例的密钥生成设备 20、加密设备 30 和接收设备 40 的功能的硬件配置的示例。每个上述组件可以由通用构件构成，或者可以由专用于该组件功能的硬件构成。因此，可以根据关于本实施例的每种实施场合的技术水平 (technical level)，以适当的方式改变将要使用的硬件配置。另外，显而易见，上述硬件配置仅是示例，并且本发明不限于此。例如，HDD 207 和存储器（安全模块）211 可以由相同的存储设备构成。另外，依据使用方式，省略了总线 213、输入 / 输出接口 215 等的配置是可用的。在下文中，详细描述通过上述硬件配置可以实现的加密密钥生成方法。

[0111] 关于基础技术的说明

[0112] 在提供本发明的优选实施例的详细描述之前，首先描述构成用于实现该实施例的基础的技术问题。注意，通过对于下面所述基础技术的改善，以可取得更显著效果的方式形成了本实施例。因此，与该改善有关的技术是形成本实施例特征的真正的部分。即，应该注

意，尽管本实施例遵循此处所述技术问题的基本构思，但是，本实施例真正的实质总结在改善部分中，本实施例的配置明显不同于基础技术的配置，另外，在本实施例与基础技术之间就 优点方面进行了划界。

[0113] 在使用公钥的传统内容传递方法中，中心判定内容传递系统的系统参数 k，并且基于该系统参数 k 形成 k 阶中心保密多项式。然后，通过使用该 k 阶保密多项式，中心生成公钥 PK 以及对于客户 i 唯一的保密密钥 d_i（在下文中，称为私钥）。中心公布公钥 PK，并且通过使用安全通信信道将私钥传递给客户 i。另外，在内容的传递时，中心传递加密文本 C 以及首标 h。由于首标 h 是通过使用公钥 PK 生成的，因此任何传递者均可以生成首标 h。在使用公钥的传统内容传递方法中，客户 i 应该仅持有一个保密密钥 d_i。另外，由于公布了公钥 PK，因此非中心传递者能够传递内容。

[0114] 然而，为了生成私钥，使用基于保密参数 k 的 k 阶多项式。在 k+1 或更多个客户相互合谋的情况下，存在不能保持系统的安全性的合谋问题。

[0115] 因此，上述非专利文献 1 中建议了公钥内容传递方法，其中，即使在任何数量的客户彼此合谋的情况下，也可以保持系统的安全性。

[0116] 在 Boneh、Gentry、Waters 等人的非专利文献 1 所述的方法中，通过使用称作双线性群的一种循环乘法群（而不使用 k 阶多项式）生成私钥，并且将对于群中客户 i 唯一的元素提供为私钥 d_i。另外，通过由每个客户使用用于首标 h 的生成以及会话密钥 s 的获取的、称作双线性映射的运算，可以解决使用公钥的传统内容传递系统中一直以来存在的巨大问题：合谋问题。

[0117] 在非专利文献 1 中，作为基本方法，首先描述用于将一组用户处理为一个群的方法。在下文中，参考图 3 描述该基本方法。在该基本方法中，中心 51 生成双线性群的生成元 g 与中心保密数 α，并且通过使用它们来向客户 i(i ＝ 1、……、n) 分配以下参数：

[0118] [算式 5]

[0119] $g_i = g^{\alpha^i}$

[0120] 另外，生成用于将一组客户 55 处理为一个群的参数 $\upsilon = g^{\gamma}$，并且将生成元 g 和参数 υ 公开为公钥 PK ＝ $(g、g_1、\cdots\cdots、g_n、g_{n+2}、\cdots\cdots、g_{2n}、\upsilon)$。此外，对于客户 i，通过使用分配给 i 的以下参数：

[0121] [算式 6]

[0122] $g_i = g^{\alpha^i}$

[0123] 经由安全一对一通信信道 53 预先提供以下私钥：

[0124] [算式 7]

[0125] $d_i = g_i^{\gamma}$

[0126] 传递者根据分配给所有非排除客户的以下参数：

[0127] [算式 8]

[0128] $g_i = g^{\alpha^i}$

[0129] 以及用于将一组客户处理为一个群的参数 $\upsilon = g^{\gamma}$，从公钥 PK ＝ $(g、g_1、\cdots\cdots、g_n、g_{n+2}、\cdots\cdots、g_{2n}、\upsilon)$ 创建与所有非排除客户相对应的公用首标元素。然后，传递者通过使用包含公用首标元素的首标元素以及在会话密钥生成时使用的随机数元素，生成首标 h，并且连同加密文本 C 一起传递该首标 h。

[0130] 如上所述，在基本方法中，通过将一组客户处理为一个群，并且形成与该群对应的首标元素，最小化了首标 h 的大小（在下文中，称为首标大小）。

[0131] 然而，由于将所有的客户处理为一个群，因此需要将不同的参数 g_1、……、g_n 分配给各客户。因此，公钥的大小等于或大于客户数量的两倍。另外，在每个客户均从首标 h 获取会话密钥 s 的情况下，需要计算与除了客户之外的所有非排除客户相对应的参数 g_1、……、g_n 的乘积。因此，如果表示客户的总数的值 n 非常大，那么强加给客户关于计算量方面的负担非常大。在实际的内容传递中，需要将内容经由付费广播、诸如 DVD、因特网之类的物理介质等传递至巨大数量的客户。因此，考虑到上述问题，可以说实际中不能使用该基本方法。

[0132] 作为用于解决上述问题的方法，在非专利文献 1 中建议了一般化方法，其中，可以通过将一组客户分组为多个子群来降低公钥的大小。在该一般化方法中，一组客户被分组为多个子群，并且对每个分组后的子群执行如在所述基本方法中那样的运算。因此，增加了需要为各个子群生成的不同首标元素以及首标大小。然而，可以降低公钥的大小。另外，每个客户需要计算分配给属于分组后子群的各客户的参数的乘积。然而，与所述基本方法相比，由于将一组客户分组为子群，因而可以降低需要计算的参数数量。因此，可以解决所述基本方法的问题。

[0133] 在下文中，参考图 4 ～ 8 详细描述非专利文献 1 中所述的一般化方法。首先定义说明上述一般化方法所需的符号，以及描述非专利文献 1 中使用的双线性群以及双线性映射。然后，通过利用这些定义，描述非专利文献 1 中所述一般化的细节、问题等。

[0134] < 符号的定义 >

[0135] 用于说明非专利文献 1 中所述一般化方法的每个符号如以下所列那样来定义。

[0136] n：客户的总数

[0137] A：当将客户群分组为多个子群时的分组数

[0138] B：属于分组后的子群的客户数

[0139] PK：系统的公钥

[0140] d_i：第 i 个客户的私钥

[0141] r：排除客户的总数

[0142] p：用作双线性群的阶的大素数

[0143] G、G_1：具有阶 p 的双线性群

[0144] g：G 的生成元

[0145] M：未加密的内容（纯文本）

[0146] s：会话密钥

[0147] C：通过使用会话密钥 s 对纯文本 M 加密得到的加密文本

[0148] $E_s(M)$：通过使用密钥 s 对纯文本 M 的加密

[0149] $D_s(C)$：通过使用密钥 s 对加密文本 C 的解密

[0150] e(u、v)：关于双线性群 G 的两个元素 u 和 v 的双线性映射。

[0151] < 双线性群的双线性映射 >

[0152] 现在描述非专利文献 1 中使用的双线性群的双线性映射。双线性映射 e(u、v) 是将循环乘法群 G 的两个元素 u 和 v 映射至循环乘法群 G_1 的元素并且满足以下所列性质的

映射。

[0153] 1. 双线性性质：对于任意 u、v ∈ G 以及 a、b ∈ Z，满足 $e(u^a, v^b) = e(u, v)^{ab}$。

[0154] 2. 非退化 (Non-degenerate) 性质：$e(g, g) \neq 1$。

[0155] 现在详细描述与非专利文献 1 中所述一般化方法有关的每个步骤。该一般化方法主要由三个阶段构成，即，密钥生成阶段、加密阶段以及解密阶段。密钥生成阶段仅由中心在系统的配置之时执行一次。加密阶段和解密阶段分别由传递者和客户每次进行传递时执行。在下文中描述每个阶段。

[0156] < 密钥生成阶段 >

[0157] 在下文中，参考图 4 和图 5 描述密钥生成阶段。图 4 是用于说明非专利文献 1 的一般化方法中的密钥生成阶段的说明图。图 5 是非专利文献 1 的一般化方法中的密钥生成阶段的流程图。

[0158] 中心 51 根据下面所述过程生成各客户 55 的私钥以及公钥。首先，中心 51 随机地选择大素数 p，并且判定将所选 p 作为其阶的双线性群 G（步骤 S11）。

[0159] 然后，中心 51 各自随机地选择在步骤 S11 中确定的双线性群 G 的生成元 g 以及中心保密随机数 α（α 是整数）（步骤 S13）。

[0160] 接下来，中心 51 判定属于分组后子群的客户数 B，并且使用以下表达式确定与计算相一致的分组数 A。然后，中心 51 将客户分组为 A 个子群（步骤 S15）。

[0161] [算式 9]

[0162] $$A = \left\lceil \frac{n}{B} \right\rceil \cdots\cdots \text{（表达式 1）}$$

[0163] 这里，上面表达式右侧指示的符号是表示“大于等于 (n/B) 的最小整数”的符号。

[0164] 然后，中心 51 如以下那样为 i(i ＝ 1、……、B、B+2、……、2B) 计算叶密钥 gi（步骤 S17）。

[0165] [算式 10]

[0166] $$g_i = g^{(\alpha)^i} \cdots\cdots \text{（表达式 2）}$$

[0167] 接下来，中心 51 随机选择与子群数 A 相对应的 A 个随机数 γ（γ_1、……、γ_A，γ 是整数）。然后，如以下那样计算属于双线性群 G 的 v_1……、v_A（步骤 S19）。

[0168] [算式 11]

[0169] $$v_i = g^{\gamma_i} \in G \quad (i=1、\ \cdots\cdots、\ A) \cdots\cdots \text{（表达式 3）}$$

[0170] 然后，中心 51 基于在上述步骤 S13 中选择的 g、在步骤 S17 中计算出的 g_i 以及在步骤 S19 中计算出的 v_i，确定下面所示的公钥 PK，并且公布该公钥 PK（步骤 S21）。

[0171] $$PK = (g、g_1、\cdots\cdots、g_B、g_{B+2}、\cdots\cdots、g_{2B}、v_1、\cdots\cdots、v_A) \cdots\cdots \text{（表达式 4）}$$

[0172] 然后，中心 51 选择与客户 i 属于的子群 S_a(a 是大于等于 i/B 的最小整数）以及作为子群中客户 i 的索引 (index) 的 b ＝ imodB（这里，i 是大于等于 1 并且小于等于 B 的整数）相对应的参数 g_b 和 γ_a，并且为下面表达式中计算出的客户 i 生成私钥 d_i（步骤 S23）。

[0173] [算式 12]

[0174] $$d_i = g_b^{\gamma_a} = v_a^{\alpha^b} \in G \cdots\cdots \text{（表达式 5）}$$

[0175] 然后，中心 51 经由安全的一对一通信信道 53 将如上述那样生成的私钥 d_i 秘密地传递至各客户 i（步骤 S23）。

[0176] 如上所述，在非专利文献 1 的密钥生成阶段中，在步骤 S15 中，中心 51 将由 n 个客户构成的一组客户分组为每一个均包含 B 个客户的 A 个子群。然后，在步骤 S11、步骤 S13、步骤 S17 以及步骤 S19 中，中心 51 设置内容传递系统管理所需的各种参数。

[0177] 另外，在步骤 S21 中，中心 51 通过使用已生成的参数来生成公钥 PK。在随后的步骤 S23 中，中心 51 基于表示在步骤 S15 中确定的子群分组数的 A 以及表示属于一个子群的客户数的 B，为各客户生成私钥。

[0178] 在这种场合下，对于每个客户，基于分配给该客户的客户唯一编号，确定该客户所属子群以及该子群中的索引。如上所述，由于在私钥生成中不使用 k 阶多项式，因此即使任意数量的客户相互合谋，也不可执行对于另一客户的私钥伪造 (fabrication) 以及允许排除用户从首标获取会话密钥的未授权密钥的形成。

[0179] < 加密阶段 >

[0180] 在下文中，参考图 6 和图 7 描述加密阶段。图 6 是用于说明非专利文献 1 一般化方法中的加密阶段的说明图。图 7 是非专利文献 1 的一般化方法中的加密阶段的流程图。

[0181] 传递者 57 根据以下所述过程对将要传递的内容加密，并且将经加密的内容经由广播通信信道 59 共同传递给非客户 61 以及客户 63。

[0182] 首先，传递者 57 随机选择整数 t，并且如下面那样计算会话密钥 s (步骤 S31)。

[0183] $s = e(g_{B+1}, g)^t = e(g_{B1}, g_1)^t$…… (表达式 6)

[0184] 然后，传递者 57 确定可对内容解密的用户组 S，并且对于 l = 1、……、A，如下面那样确定各子群 (步骤 S33)。

[0185] [算式 13]

[0186] $\hat{S}_l = S \cap \{(l-1)B+1、\ldots\ldots、lB\}$…… (表达式 7)

[0187] $S_l = \{x - lB + B \mid x \in \hat{S}_l\} \subseteq \{1、\ldots\ldots、B\}$…… (表达式 8)

[0188] 这里，下标 1 是表示子群的参数。以上表达式 7 表示的组是参数 1 表示的子群中所包含的客户和非客户的组。以上表达式 8 表示的组是表示参数 1 所表示的子群中的客户的位置的组。

[0189] 然后，传递者 57 如下面那样形成客户 63 计算会话密钥 s 所需的首标 h(步 骤 S35)。

[0190] [算式 14]

[0191] $h = (g^r, (v_1 \cdot \prod_{j \in S_1} g_{B+1-j})^r, \ldots, (v_A \cdot \prod_{j \in S_A} g_{B+1-j})^r) \in G^{A+1}$…… (表达式 9)

[0192] 接下来，传递者 57 基于步骤 S31 中计算出的会话密钥 s，如表达式 10 所示那样加密待传送的内容。然后，传递者 57 经由广播通信信道 59，连同关于在步骤 S33 中确定的组 S 信息以及在步骤 S35 中计算出的首标 h，传送经加密的内容 C，而不管是非客户 61 还是客户 63(步骤 S37)。

[0193] $C = E_S(M)$…… (表达式 10)

[0194] 如上所述，在传递之时，在加密阶段步骤 S31 中生成会话密钥之后，传递者 57 在步骤 S33 中确定可以对属于每个子群的内容进行解密的一组客户。然后，在步骤 S35 中，传递者 57 创建包含与各子群对应的元素的首标。这里，首标 h 的每个元素仅由与可在每个子群中执行解密的客户相对应的参数 g_b 形成，而不包含与排除客户对应的 g_b。因此，在稍后所

述解密之时，可以实现非客户 (non-customer) 的排除。

[0195] ＜解密阶段＞

[0196] 在下文中，参考图 8 描述解密阶段。图 8 是非专利文献 1 一般化方法中的解密阶段的流程图。

[0197] 接收到经加密内容等的传递的客户 i 根据下面所述过程，对经加密的内容执行解密处理。

[0198] 首先，客户 63 检查传递者传递的组 S 中是否包含其自身索引 i（步骤 S51）。在组 S 中不包含其自身索引 i 的情况下，客户 63 判定该客户 63 是被排除的，并且终止解密处理。在组 S 中包含其自身索引 i 的情况下，客户 63 继续执行以下所述处理。

[0199] 接下来，客户 63 从所传送的首标 h 中选择与客户 63 属于的子群 S_a 相对应的首标元素，并且计算会话密钥 s（步骤 S53）。即，如 h ＝ (C_0、C_1、……、C_A) 所表示，首标 h 由与各子群对应的首标元素构成。客户 63 基于该首标元素，如以下计算那样，选择与客户 63 属于的子群 S_a 相对应的元素 C_0 和 C_a，并且获取会话密钥 s。

[0200] [算式 15]

[0201] $$s=\frac{e(g_b,C_a)}{e(d_i\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},C_0)}\cdots\cdots\text{（表达式 11-1）}$$

[0202] $$=\frac{e(g_b,(v_a\cdot\prod_{j\in S_a}g_{B+1-j})^t)}{e({v_a}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)}\cdots\cdots\text{（表达式 11-2）}$$

[0203] $$=\frac{e(g_b,{g_{B+1-b}}^t)\cdot e(g_b,(v_a\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j})^t)}{e({v_a}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)}\cdots\cdots\text{（表达式 11-3）}$$

[0204] $$=\frac{e(g,g_{B+1})^t\cdot e(g^t,({v_a}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b})^t)}{e({v_a}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)}\cdots\cdots\text{（表达式 11-4）}$$

[0205] $$=e(g,g_{B+1})^t\cdots\cdots\text{（表达式 11-5）}$$

[0206] 从以上表达式 11-5 以及表达式 6 中可清楚地看到，通过使用从传递者 57 传送的首标 h、公钥 PK、以及客户 63 自己持有的私钥 d_i，客户 63 能够计算与传递者 57 为加密所使用的内容密钥 s 相同的一个。

[0207] 然后，客户 63 通过使用上面步骤 S53 中计算出的会话密钥 s，将已传递的经加密的内容 C 解密为纯文本 M（步骤 S55）。

[0208] $M = D_S(C)$……（表达式 12）

[0209] 如上所述，在解密的时候，客户 63 首先在步骤 S51 中检查该客户 63 是否是被排除的。在该客户 63 是否是被排除的情况下，由于客户 63 因为稍后描述的原因而不可获取会话密钥 s，因此客户 63 终止解密处理。根据步骤 S51 的判定知道其未被排除的客户从已传送的首标中提取与该客户所属子群相对应的首标元素，并且在步骤 S53 中，基于该首标元素、该客户的私钥以及公钥，通过使用表达式 11-1 ～ 11-5 所示的双线性映射来执行解密运算，从而可 以获取会话密钥。然后，通过使用计算出的会话密钥 s，客户执行加密文本的解密。

[0210] 这里，即使排除客户通过使用表达式 11-1 ～ 11-5 所示的双线性映射来执行解密运算，由于与其自身 g_b 对应的值 g_{B+1-b} 未包含在步骤 S53 中的表达式 11-2 的以下部分之中：

[0211] [算式 16]

[0212] $$(v_a \cdot \prod_{j \in S_a} g_{B+1-j})^t \cdots\cdots (\text{表达式 13})$$

[0213] 因此由于作为非专利文献 1 中安全性基础的 BDHEP(Bilinear Diffie-HellmanExponential Problem，双线性 Diffie-Hellman 指数问题）的困难，因而不可实现至表达式 11-3 的转换。因此，不能计算出正确的会话密钥 s。

[0214] 如上所述，非专利文献 1 的方法解决了使用 k 阶多项式的传统公钥内容传递方法中一直以来存在的问题：合谋问题。另外，由于中心在密钥加密阶段的步骤 S15 中预先将一组客户分组为 A 个子群，因此可以将传递者需要生成的首标配置为总具有 A+1 个元素。因此，无论排除客户的数量如何，均可以将首标大小保持恒定。

[0215] 如上所述，在非专利文献 1 的方法中，必须总是传送具有恒定大小的首标。因此，在不存在排除客户或存在少数排除客户的情况下，存在不可实现高效内容传递的问题。在实际的内容传递系统中，客户数量经常是很大的值。因此，相对于客户的总数，排除客户的数量经常是很小的值。另外，如果排除客户的数量很大，那么内容传递系统自身可能会崩溃。因此，作为内容传递系统，在不存在排除客户或排除客户的数量相对于客户的总数保持很小的情况下，需要高效地传递内容。

[0216] 然而，如上所述，非专利文献 1 中难于满足这种条件。此外，在非专利文献 1 中，为了在解密阶段的步骤 S53 中执行使用表达式 11-1 中双线性映射的运算，如以下表达式 14 中所示那样，需要预先计算分配给客户所属子群内存在的非排除客户的参数与该客户所持有的私钥的乘积。

[0217] [算式 17]

[0218] $$d_i \cdot \prod_{\substack{j \in S_a \\ j \neq b}} g_{B+1-j+b} \cdots\cdots (\text{表达式 14})$$

[0219] 这里，在由 PAIR 表示使用双线性映射的运算、由 INV 表示关于双线性群 G_1 的逆运算、由 MUL 表示关于双线性群 G 的乘法、而由 r_a 表示客户 i 所属子群 S_a 中排除客户的数量的情况下，可以将客户在解密阶段需要执行的运算的计算量表示为“2PAIR+INV+(B-1-r_a)MUL”。

[0220] 如据此清楚看到的那样，在属于分组后子群的客户的数量 B 很大的情况下或者客户所属子群中排除客户的数量 r_a 很小的情况下，存在每个客户在解密时需要执行的计算量增大的问题。

[0221] 如上所述，即使在使用非专利文献 1 的一般化方法的情况下，当一组客户的分组数增多时，也可以减小每个客户在内容解密时执行的计算量。然而，增大了首标大小。另外，相反，当一组客户的分组数减少时，可以减小首标大小。然而，存在计算量增大的问题。另外，即使在排除客户的数量很少的情况下，也总是需要传递具有恒定大小的首标 h。因此，在实际非常可能发生的情形下（诸如，不存在排除客户或排除客户的数量相对于客户的总数的百分比很小的情况下）存在不能减小首标大小以及内容传递时数据冗余度增大的问题。

[0222] 因此，为了解决上述问题，本申请的发明人在已专心致志于认真研究之后，开发了如下面所述那样的根据本发明实施例的加密密钥传递系统。在根据本实施例的密钥生成设备中，通过配置向非专利文献 1 的方法添加某些参数的逻辑树，即使在排除客户的数量很少的情况下，与专利文献 1 中所述的方法相比，也可以减小首标大小。另外，通过提供这种配置，可以将客户在解密时需要执行的运算的计算量降低至等效量或更低。因此，可以实现高效内容传递。

[0223] 本实施例的描述

[0224] 在下文中，根据上述基础技术，详细描述根据本实施例的密钥生成设备、加密设备和接收设备。根据本实施例的密钥生成设备 20 通过采用非专利文献 1 的方法构造逻辑树。与非专利文献 1 的方法相比，根据本实施例的密钥生成设备 20 通过逻辑树的使用实现了在不存在排除客户或排除客户的数量很少的情况下的高效内容传递。

[0225] 首先参考图 9 描述根据本实施例的密钥生成设备 20 的配置。图 9 是示出根据本实施例的密钥生成设备 20 的配置的框图。

[0226] 例如，密钥生成设备 20 包含树结构构造单元 231、随机数确定单元 233、叶密钥分配单元 235、参数分配单元 237、密钥计算单元 239、存储单元 241 以及传递单元 252。

[0227] 树结构构造单元 231 构造作为根据本实施例的密钥生成设备的重要元素的逻辑树。即，树结构构造单元 231 分级地构造 Y 元树，其中，将 n 个目标接收设备分配给树叶，并且由 $(\log_Y n)$ 表示高度。此外，形成每一个均具有 Y 元树的子群，在该 Y 元树中，将树叶和根之间存在的每个中间节点定义为父节点。即，通过树结构构造单元 231，Y 个分支总是从一个节点向下生成的 Y 元树结构分级地层叠。当浏览所构造的整个分级 Y 元树结构时，在最上层（在下文中，称为第 0 层）仅存在一个根，并且在该根的下面，将该根作为父节点的 Y 个子节点构造为第一层。另外，在第二层中，进一步存在将第一层中存在的 Y 个子节点作为父节点的 Y^2 个子节点。通过重复这种结构，在最底层（即，第 $\log_Y n$ 层）中总共存在 n 个树叶。

[0228] 这里，在一个分支从一个节点向下生长并且在该分支的末端存在一个节点的情况下，将上方节点相对地称作父节点，而将下方节点相对地称作子节点。关于父节点和子节点的这种概念是基于相对思想的。例如，在通过分支上下链接三个节点的情况下，如果将最上方的节点称为父节点，那么位于中间位置的节点称为子节点。另外，当关注于最下方节点时，对于位于用作父节点的中间位置的节点来说，最下方节点用作子节点。

[0229] 另外，在分级的树结构中，将最上层中存在的根与最下层中存在的 n 个树叶之间存在的每个节点称作中间节点。

[0230] 随机数确定单元 233 确定根据本实施例的密钥生成设备以及双线性群所使用的各种随机数。即，随机数确定单元 233 随机地选择素数 p，并且确定将素数 p 作为其阶的双

线性群 G。另外，随机数确定单元 233 随机地选择表示 G 的生成元的 g，并且随机地选择表示保密随机数的整数 α 。

[0231] 叶密钥分配单元 235 向树结构构造单元 231 构造的分级 Y 元树结构中的 n 个终端树叶以及不是树叶和根的所有中间节点分配叶密钥 g_y。

[0232] 参数分配单元 237 向树结构构造单元 231 构造的分级 Y 元树结构中的除了 n 个终端树叶之外的所有节点（即，最上层中的根以及在该根和树叶之间存在的所有中间节点）分配任意的参数 $v_{x,y}$。这里，每个 x 和 y 是表示节点位置的下标，x 表示层，而 y 表示该节点在层 x 中的位置。

[0233] 密钥计算单元 239 基于双线性群 G 以及随机数确定单元 233 确定的随机 数、叶密钥分配单元 235 分配的叶密钥、参数分配单元 237 分配的参数等来计算公钥和私钥。

[0234] 例如，存储单元 241 包含树结构存储部分 243、随机数存储部分 245、叶密钥存储部分 247、参数存储部分 249、密钥存储部分 251 等。在这些存储部分中存储着每个处理单元执行的、在处理的中间所需的变量和计算结果或者根据该处理获得的结果。诸如树结构构造单元 231、随机数确定单元 233、叶密钥分配单元 235、参数分配单元 237 以及密钥计算单元 239 之类的各处理单元能够自由地将数据写至存储单元 241 以及从存储单元 241 读取数据。

[0235] 另外，可以将存储单元 241 中的各种数据存储在不同于上述存储部分 243、245、247、249 以及 251 的部分中。注意，虽然图 9 中示出了各种存储部分独立地存在于存储单元 241 之内的状态，但是各种存储部分并不是必须单独存在，而是可以将各种数据作为一个整体存储在存储部分中。另外，可以使用配有安全模块的存储介质作为存储单元 241。

[0236] 根据本实施例的密钥生成设备中的传递单元 252 例如包括传输部分 253 和公钥公布部分 255。传输部分 253 向每个接收设备传送由密钥计算单元 239 计算出的且存储在密钥存储部分 251 中的私钥。另外，公钥公布部分 255 向每个接收设备公布由密钥计算单元 239 计算出的且存储在密钥存储部分 251 中的公钥。

[0237] 现在参考图 10 描述根据本实施例的加密设备 30 的配置。图 10 是示出根据本实施例的加密设备 30 的配置的框图。

[0238] 如图 10 中所示，加密设备 30 包括例如接收单元 301、存储单元 303、排除接收设备识别单元 305、会话密钥确定单元 307、内容存储单元 313、加密单元 315 以及内容传输单元 317。

[0239] 接收单元 301 接收密钥生成设备 20 生成并公布的公钥。另外，接收单元 301 能够进一步接收密钥生成设备 20 生成的素数 p 以及作为识别排除接收设备的信息的、关于非排除接收设备的组 S 的信息和公钥。

[0240] 存储单元 303 例如存储密钥生成设备 20 生成的公钥。另外，存储单元 303 能够存储关于素数 p 的信息、关于非排除接收设备的信息等和公钥。

[0241] 排除接收设备识别单元 305 在经由通信网络 12 连接至加密设备 30 的多 个接收设备 40 之中识别对其取消了内容的传递的排除接收设备，并且确定非排除接收设备的组 S。在确定组 S 的时候，排除接收设备识别单元 305 能够查阅存储单元 303 中存储的各种数据。

[0242] 会话密钥确定单元 307 确定用于待传递内容的加密的会话密钥。会话密钥确定单

元 307 可进一步包含例如首标元素计算部分 309 以及首标信息生成部分 311。

[0243] 在确定会话密钥 s 的时候，会话密钥确定单元 307 随机地选择整数 t，并且通过使用已公布的公钥来执行双线性映射的运算。

[0244] 首标元素计算部分 309 标记如下路径中存在的所有各节点，所述路径是：在密钥生成设备 20 构造的分级树结构中从对其分配了排除接收设备的树叶延伸至根的路径；并且首标元素计算部分 309 基于分配给已标记节点的参数以及分配给将所述已标识节点用作其父节点的中间节点的叶密钥来计算首标元素。

[0245] 首标信息生成部分 311 基于首标元素计算部分 309 得到的首标元素以及公钥来生成首标信息。

[0246] 内容存储单元 313 存储未加密的内容。另外，内容存储单元 313 可存储从诸如 CD（光盘）、DVD（数字多功能盘）或存储卡之类的介质获取的内容。这里，上述内容可以是任何内容数据，例如，通过移动图像或静态图像所构成的视频内容（诸如电影、电视节目、视频节目或图）、音频内容（诸如音乐、演讲或无线电节目）、游戏内容、文献内容或软件。视频内容可包含音频数据和视频数据。

[0247] 加密单元 315 从内容存储单元 313 选择待传递的内容，并且通过使用会话密钥确定单元 307 计算出的会话密钥 s 来对该内容加密。

[0248] 内容传输单元 317 经由通信网络 12 向每个接收设备传送加密单元 315 加密的已加密内容、首标信息生成部分 311 确定的首标以及排除接收设备识别单元 305 识别的组 S。

[0249] 现在，参考图 11 描述根据本实施例的接收设备 40 的配置。图 11 是示出接收设备 40 的配置的框图。

[0250] 如图 11 中所示，接收设备 40 例如包含接收单元 401、存储单元 403、确定单元 405 以及解密单元 407。

[0251] 接收单元 401 接收密钥生成设备 20 生成的私钥。另外，接收单元 401 能 够进一步接收密钥生成设备 20 生成的公钥以及作为识别排除接收设备的信息的、关于非排除接收设备的组 S 的信息和私钥。另外，接收单元 401 还能够接收加密设备 30 加密的内容。

[0252] 存储单元 403 例如存储密钥生成设备 20 生成的公钥以及私钥。另外，存储单元 403 能够存储关于非排除接收设备的组 S 的信息以及关于已传递的经加密内容、经解密内容等的内容信息和加密密钥。

[0253] 确定单元 405 确定接收到的组 S 中是否包含接收设备自身。根据确定单元 405 的确定结果，解密单元 407 对已加密的内容执行解密处理。

[0254] 解密单元 407 通过使用接收单元 401 接收到的首标 h 以及存储在存储单元 403 中的公钥和私钥，计算已加密内容的解密所需的会话密钥 s。在计算出会话密钥 s 之后，解密单元 407 继续执行已加密内容的解密。

[0255] 以上已经描述了根据本实施例的密钥生成设备 20、加密设备 30 以及接收设备 40 的功能的示例。上述每个组件均可以通过使用通用构件或电路来构成，或通过该组件功能所专用的硬件来构成。另外，各组件的所有功能均可由 CPU 等执行。因此，根据本实施例实施时的技术水平 (level)，可以以适当的方式改变将要使用的配置。

[0256] 如非专利文献中那样，根据本实施例的加密密钥传递系统 10 由三个阶段构成，即，密钥生成阶段、加密阶段和解密阶段。密钥生成阶段仅由中心在系统配置时执行一次。

另外，加密阶段和解密阶段分别由传递者和客户每次进行传递时执行。注意，如基础技术的描述中那样定义根据本实施例的加密密钥传递系统 10 的说明所使用的各符号及运算。在下文中，首先给出本实施例中配置的逻辑树的定义和描述。然后详细描述每个阶段。

[0257] 〈逻辑树的结构和定义〉

[0258] 首先给出对于根据本实施例的密钥生成设备 20 的说明所需的逻辑树的描述和定义。在根据本实施例的密钥生成设备 20 中，通过将每个客户分配给树叶并且将非专利文献 1 中客户的分组分配给逻辑树，实现了高效的内容传递。该逻辑树由根据本实施例的密钥生成设备 20 中的树结构构造单元 231 来构造。

[0259] 注意，为了简化，在本实施例中使用了 Y 元树。另外，由于需要将所有的客户都分配给树叶，因此假设客户的总数 n 是可表示为 Y 的幂的值。然而，在实际内客传递中经常发生不能将 n 表示为 Y 的幂的情况。尽管如此，通过 预先准备其数量（其远大于 n）可表示为 Y 的幂的树叶，可容易地处理这种情况。在下文中关于逻辑树的结构给出每个定义。

[0260] 对于本实施例中使用的 Y 元树，由 n 表示树叶的数量。因此，假设由 H 表示除了根之外的 Y 元树的高度，得到 $H = \log_Y n$。另外，假设由 N 表示除了树叶之外的节点的总数，得到 $N = (n-1)/(Y-1)$。因此，除了根之外，Y 元树中存在 H 层。这里，将这些层定义为 Layer（层）。即，以将根的一组子节点定义为 Layer1 以及将 Layer1 中所有节点的一组子节点（即，该根的孙节点）定义为 Layer2 的形式，将 Y 元树的各层定义为 Layer x(x = 0、……、H)。这里，x 是表示层的下标。另外，通过假设将包含在 Layer x 中的各个节点的索引表示为节点索引，给出定义 $(x, y)(y = 1、\cdots\cdots、Y^x)$。这里，根是 Layer0 中的节点，根的索引是 (0,1)。

[0261] 作为上述定义的 Y 元树的示例，在图 12 中示出客户数 n 为 9 且分支数 Y 为 3 的情况。

[0262] 由于客户数 n 为 9，因此将除了根之外的三叉树 (ternary tree) 的高度表示为 $\log_3 9 = 2$。因此在该三叉树中存在着包含该根的三层。即，将包含根的层 501 定义为 Layer0，并且将包含作为根的子节点的三个节点的层 503 定义为 Layer1。将 Layer1 中存在的三个节点单独地用作其父节点情况下的子节点的层 505 定义为 Layer2。由于根据 Layer1 中存在的三个节点中的每一个都形成三个子节点，因此在 Layer2 中总共存在 9 个树叶。

[0263] 另外，除了树叶之外的节点数 N（即，根的数量与中间节点的数量之和）被表示为 $(9-1)/(3-1) = 4$。

[0264] 例如，分配给包含树叶的各节点的节点索引是：对于根的 (0,1)，以及对于 Layer1 中从左端起的三个节点的 (1,1)、(1,2) 和 (1,3)。另外，将节点索引 (2,1)、(2,2)、……、(2,9) 提供给 Layer2 中从左端起单独的 9 个节点（即树叶）。

[0265] 另外，在根据本实施例的密钥生成设备 20 中，将接收设备 40（即，用于内容传递的客户 507）分配给树叶。即，分别将客户 1(507A)、客户 2(507B)、……、客户 9(507I) 分配给 Layer2 中的树叶 (2,1)、(2,2)、……、(2,9)。

[0266] 现在，在下文中通过使用逻辑树的上述定义给出根据本实施例的加密密钥传递系统的具体描述。

[0267] 〈密钥生成设备 20 的运算：加密密钥生成阶段〉

[0268] 中心操作该中心拥有的密钥生成设备 20，并且根据以下过程为各客户生成公钥和

私钥。在下文中，参考图 12、图 13 和图 14 详细描述根据本实施例的密钥生成设备 20 的操作。图 13 是用于说明密钥生成设备 20 的密钥生成的概况的说明图。图 14 是密钥生成设备 20 的加密密钥生成阶段的流程图。

[0269] 首先，密钥生成设备 20 的随机数确定单元 233 随机地选择素数 p（其为很大的值），并且确定将所选择的 p 作为其阶的双线性群 G（步骤 S101）。这里，很大值的素数 p 意味着具有很大数字的素数。通过选择具有对于其离散算法问题不易求解的大量数字的素数，随机数确定单元 233 确保了根据本实施例的加密密钥的安全。

[0270] 然后，随机数确定单元 233 随机地选择双线性群 G 的生成元 g，以及中心保密随机数 α（α 是整数）（步骤 S103）。

[0271] 与素数 p、双线性群 G、生成元 g 以及随机数 α 有关的数据被存储在例如存储单元 241 内的随机数存储单元 245 中，并且由叶密钥分配单元 235、参数分配单元 237、加密密钥计算单元 239 等查阅。

[0272] 然后，密钥生成设备 20 的树结构构造单元 231 确定属于分组后子群的客户数 Y。在根据以下计算确定了分组数 X 之后，树结构构造单元 231 将客户分组为 X 个子群。此外，树结构构造单元 231 构造将每一个客户都作为树叶来分配的 Y 元树（步骤 S105）。这里，以下表达式 101 内的 n 表示客户的总数。

[0273] [算式 18]

[0274] $$X = \left\lceil \frac{n}{Y} \right\rceil \cdots\cdots \text{（表达式 101）}$$

[0275] 例如，如图 12 中所示，在客户的总数 n 为 9 并且 Y = 3（即，构造三叉数）的情况下，根据表达式 101，分组数 X 为 3。

[0276] 树结构构造单元 231 使得将如上所述那样构造的 Y 元树结构存储在存储单元 241 内的树结构存储部分 243 中。

[0277] 接下来，密钥生成设备 20 的叶密钥分配单元 235 如以下那样对 i（i = 1、……、Y、Y+2、……、2Y）计算叶密钥 g_i（步骤 S107）。

[0278] [算式 19]

[0279] $$g_i = g^{(\alpha)^i} \cdots\cdots \text{（表达式 102）}$$

[0280] 从上面的表达式 102 可清楚地看到，对于叶密钥 g_i 的计算，使用了随机数确定单元 233 确定的生成元 g 以及中心保密随机数 α。因此，叶密钥分配单元 235 访问存储单元 241 内的随机数存储部分 245 以读取数据。在计算出叶密钥之后，叶密钥部分单元 235 将计算出的叶密钥 g_i 存储在存储单元 241 内的叶密钥存储部分 247 中。

[0281] 注意，在步骤 S107 中，不仅计算出了 Y 个叶密钥 g_i（其中，Y 表示属于子群的客户数），而且通过将 i 变化到 2Y（除了 Y+1）计算出了叶密钥 g_i。不执行 g_{Y+1} 的计算的原因是为了确保根据本实施例的加密密钥传递系统 10 的安全。另外，这是由于从 g_{Y+2} 至 g_{2Y} 的叶密钥 g_i 是在稍后所述解密阶段中执行解密所需要的。

[0282] 然后，加密密钥创建设备 20 的参数分配单元 237 随机地选择与除了树叶之外的所有节点 (x,y) 相对应的随机数 $Y_{x,y}$（$Y_{x,y}$ 是整数）。然后，参数分配单元 237 如下面那样计算参数 $v_{x,y}$，并且将参数 $v_{x,y}$ 分配给 Y 元树的除了树叶之外的各节点（步骤 S109）。这里，x

＝0、……、H-1(H是Y元树结构的高度)，而y＝1、……、Y^x。

[0283] [算式20]

[0284] $$v_{x,y} = g^{\gamma_{x,y}} \in G \cdots\cdots$$ (表达式103)

[0285] 例如，如图12中所示，在对九个客户构造三叉树结构的情况下，由于三叉树结构的高度H是2，因此x是0或1。另外，y是1、2或3。即，在图12的情况下，参数分配单元237一共分配了四个参数$v_{x,y}$：$v_{0,1}$、$v_{1,1}$、$v_{1,2}$和$v_{1,3}$。因此，对于$\gamma_{x,y}$，同样随机地选择了四个整数。基于如上述那样确定的值，根据表达式103将参数分配给各节点。

[0286] 另外，将参数分配单元237计算出的参数$v_{x,y}$、节点参数$\gamma_{x,y}$等存储在存储单元241内的参数存储部分249中。

[0287] 然后，叶密钥分配单元235将$g_{x,y}$分配给除了根之外的所有节点(步骤S111)。这里，y＝1、……、Y^x，而$g_{x,y}$表示由g_1、……、g_Y构成的组{g_1、……、g_Y}元素。如上所述，叶密钥分配单元235具有计算叶密钥g_y的功能以及将计 算出的叶密钥分配给除了根之外的所有节点的功能。分配结果与树结构相关联地存储在存储单元241内的叶密钥存储部分247中。

[0288] 作为示例，考虑图12中所示的情况。在这种情况下，在Layer1(503)中存在根用作其父节点的三个子节点以形成子群。因此，将g_1作为$g_{1,1}$分配给节点(1,1)，将g_2作为$g_{1,2}$分配给节点(1,2)，并且将g_3作为$g_{1,3}$分配给节点(1,3)。

[0289] 另外，当考虑Layer2(505)时，共存在三个子群：即，节点(1,1)用作其父节点的三个节点(2,1)、(2,2)和(2,3)所构成的子群，节点(1,2)用作其父节点的三个节点(2,4)、(2,5)和(2,6)所构成的子群，以及节点(1,3)用作其父节点的三个节点(2,7)、(2,8)和(2,9)所构成的子群。在这种情况下，将g_1作为$g_{2,1}$分配给节点(2,1)，将g_2作为$g_{2,2}$分配给节点(2,2)，并且将g_3作为$g_{2,3}$分配给节点(2,3)。类似地，将g_1作为$g_{2,4}$分配给节点(2,4)，将g_2作为$g_{2,5}$分配给节点(2,5)，并且将g_3作为$g_{2,6}$分配给节点(2,6)。另外，将g_1作为$g_{2,7}$分配给节点(2,7)，将g_2作为$g_{2,8}$分配给节点(2,8)，并且将g_3作为$g_{2,9}$分配给节点(2,9)。

[0290] 然后，密钥生成设备20的密钥计算单元239如以下那样形成公钥，并且经由公钥公布部分255公布公钥PK(步骤S113)。

[0291] PK＝(g、g_1、……、g_Y、g_{Y+2}，……、g_{2Y}、$v_{0,1}$、……、$v_{H-1,X}$)……(表达式104)

[0292] 从上面的表达式104可清楚地看到，公钥PK由随机数确定单元233确定的生成元g、叶密钥分配单元235计算出的叶密钥g_i以及参数分配单元237计算出的参数$v_{x,y}$构成。因此，叶密钥计算单元239通过查阅存储单元241内的每个存储部分245、247和249来形成公钥PK。密钥计算单元239将所形成的公钥PK存储在存储单元241内的密钥存储部分251中。公钥公布部分255查阅密钥存储部分251以公布公钥。注意，密钥计算单元239可直接将形成的公钥PK传送至公钥公布部分255。

[0293] 作为示例，考虑图12中所示的情况。在这种情况下，将(g、g_1、g_2、g_3、g_5、g_6、$v_{0,1}$、$v_{1,1}$、$v_{1,2}$、$v_{1,3}$)公布为公钥PK。

[0294] 然后，密钥计算单元239为客户i(i＝1、……、n)识别从根延伸至分配给客户i的树叶的路径，并且对于该路径中Layer x中的节点，将客户i的索引 设置为i_x。即，i_0＝

(0,1) 以及 i_H = (H, i)。中心为分配给客户 i 的除了根之外的所有节点 i_1、……、i_H 识别分配给这些节点的参数 g_{ix}。另外，中心识别分配给除了树叶之外的所有节点 i_0、……、i_{H-1} 的参数 γ_{ix}。并且如下面那样为客户 i 计算私钥 d_i。然后，传输部分 253 通过使用安全通信信道将私钥 d_i 传递至客户 i（步骤 S115）。

[0295] [算式 21]

[0296] $$d_i = \{g_{i_1}^{\gamma_{i_0}}, ..., g_{i_H}^{\gamma_{i_{H-1}}}\} = \{v_{i_0}^{\alpha^{i_1}}, ..., v_{i_{H-1}}^{\alpha^{i_H}}\} \in G^H \cdots\cdots$$ (表达式 105)

[0297] 从表达式 105 可清楚地看到，基于分配给已识别路径中的节点 i_x 的叶密钥 g_{ix} 以及分配给用作该节点 i_x 的父节点的节点的参数 γ_{ix-1} 来计算私钥 d_i 的各元素。即，可以说每个私钥 d_i 都是基于分配给每个节点的叶密钥而计算出的一组密钥。注意，在下文中参考图 15 详细描述上述步骤 S115 的具体示例。

[0298] 注意，当在密钥计算单元 239 中计算出对于各客户唯一的私钥 d_i 时，密钥计算单元 239 将这些私钥存储在存储单元 241 内的密钥存储部分 251 中。在传输部分 253 向每个客户传送私钥 d_i 的情况下，传输部分 253 通过查阅存储单元 241 内的密钥存储部分 251 来获取必要的信息。另外，密钥计算单元 239 可直接将生成的私钥传至传输部分 253。

[0299] 现在参考图 15 举例说明上述步骤 S115 的具体示例。在图 15 中，对九个客户构造了三叉树结构。这里，考虑向被分配给树叶 (2,3) 的客户 3 传送私钥 d_3 的情况。

[0300] 从根 (0,1) 延伸至表示客户 3 的树叶 (2,3) 的路径是从根 (0,1) 经由中间节点 (1,1) 延伸至树叶 (2,3) 的路径。在这种情况下，分别由 i_1 和 i_2 表示该路径中除了根 (0,1) 之外的节点 (1,1) 和 (2,3)。这里，考虑分配给各节点 (0,1)、(1,1) 和 (2,3) 的参数。对于节点 (0,1)，将 $\gamma_{0,1}$ 分配为 γ_{i0}。对于节点 (1,1)，将 $\gamma_{1,1}$ 分配为 γ_{i1}，并且将 $g_{1,1}$ 表示的 g_1 分配为 $g_{i,1}$。另外，对于树叶 (2,3)，将 $g_{2,3}$ 表示的 g_3 分配为 g_{i2}。

[0301] 根据表达式 105，待由客户 3 持有的私钥 d_3 是通过将分配给节点 (1,1) 的叶密钥 g1 提高至分配给作为节点 (1,1) 的父节点的根 (0,1) 的 $\gamma_{0,1}$ 的幂所得到的一组结果，以及通过将分配给树叶 (2,3) 的叶密钥 g3 提高至分配给作为树叶 (2,3) 的父节点的根 (1,1) 的 $\gamma_{1,1}$ 的幂所得到的一组结果。

[0302] 如上所述，如图 13 中所示，关于根据本实施例的密钥生成设备 20，中心 509 拥有的密钥生成设备 20 选择双线性群 G 以及各种参数，并且生成公钥 PK 以及对于客户唯一的私钥 d_i。然后，中心 509 公布公钥 PK 以及通过使用安全一对一通信信道 511 向每个客户 507 传递私钥 d_i。

[0303] < 加密设备 30 的运算 : 加密阶段 >

[0304] 现在参考图 16 和图 17 详细描述根据本实施例的加密设备 30 的运算（即，加密阶段）。图 16 是用于说明加密设备 30 的加密的概况的说明图。图 17 是加密设备 30 的加密的概况的流程图。注意，可以由拥有加密设备 30 的任意第三方执行下面所述的加密阶段。另外，只要密钥生成设备 20 的拥有者或接收设备 40 的拥有者是加密设备 30 的拥有者，那么即使密钥生成设备 20 的拥有者或接收设备 40 的拥有者也能够执行下面的加密阶段。

[0305] 在执行下面描述的加密阶段之前，加密设备 30 的接收单元 301 接收密钥生成设备 20 生成和公布的公钥、素数 p、关于树结构的信息以及关于非排除接收设备的组 S 的信息中的每一个。接收设备 301 接收到的这种信息存储在存储单元 303 中。存储在存储单元 303 中的这种信息可随意地由加密设备 30 的每个处理单元读取。

[0306] 首先，排除接收设备识别单元 305 标记从分配给期望将其排除的所有客户的树叶延伸至根的路径中的所有节点，并且将非排除客户所使用的、用于根据首标 h 识别分配给非排除客户的首标元素的节点索引的组 S 初始化为 S = Φ（Φ 表示空集）（步骤 S301）。

[0307] 然后，会话密钥确定单元 307 随机地选择任意的整数 t，并且如下面中那样计算会话密钥 s（步骤 S303）。

[0308] $s = e(g_{Y+1}, g)^t = e(g_Y, g_1)^t$ ……（表达式 106）

[0309] 然后，首标元素计算部分 309 将表示层的参数 x 设置为 -1（步骤 S305）。即，步骤 S305 是初始化表示层的参数 x 的步骤。

[0310] 然后，首标元素计算部分 309 将 x 替换为 x+1 以将 x 的值增大 1（步骤 S307）。

[0311] 接下来，首标元素计算部分 309 将 y 设置为 0 以初始化参数（步骤 S309）。

[0312] 然后，首标元素计算部分 309 将 y（其是表示每层中节点的位置的参数） 替换为 y+1 以将 y 的值增大 1（步骤 S311）。

[0313] 接下来，首标元素计算部分 309 将与节点 (x,y) 对应的首标元素 $c_{x,y}$ 初始化为 $c_{x,y} = 0$（步骤 S313）。

[0314] 根据下面所述的步骤，首标元素计算部分 309 执行用于计算首标元素的特定处理。

[0315] 然后，首标元素计算部分 309 判定是否标记了节点 (x，y) 的所有子节点（步骤 S315）。作为该判定的结果，在标记了所有子节点的情况下，首标元素计算部分 309 进入下面所述的步骤 S321。同时，在存在未标记子节点的情况下，首标元素计算部分 309 进入下面所述的步骤 S317。

[0316] 接下来，首标元素计算部分 309 将一组未标记子节点定义为 $S_{x,y}$ 并且如以下那样计算与属于 $S_{x,y}$ 的各元素用作根的子树（子群）的客户相对应的首标元素（步骤 S317）。

[0317] [算式 22]

[0318] $$c_{x,y} = (v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t \in G \cdots\cdots$$（表达式 107）

[0319] 另外，首标元素计算部分 309 如以下那样设置组 S（步骤 S317）。

[0320] [算式 23]

[0321] $S \cup S_{x,y}$……（表达式 108）

[0322] 接下来，首标元素计算部分 309 标记属于 $S_{x,y}$ 的各元素用作根的子树的所有节点（包含树叶）（步骤 S319）。

[0323] 然后，首标元素计算部分 309 判定当前关注的参数 y 是否对应于 Y^x（步骤 S321）。作为该判定的结果，在 y 是 Y^x 的情况下，首标元素计算部分 309 进入下述步骤 S323。同时，在 y 不是 Y^x 的情况下，首标元素计算部分 309 返回步骤 S311 以将参数 y 增大 1。

[0324] 接下来，首标元素计算部分 309 判定当前关注的参数 x 是否是 H-1（步骤 S323）。作为该判定的结果，在 x 是 H-1 的情况下，首标元素计算部分 309 进入下述步骤 S325。同时，在 x 不是 H-1 的情况下，首标元素计算部分 309 返回步骤 S307 以将参数 x 增大 1。

[0325] 如上所述，通过重复步骤 S307 ～ S323 直至满足了步骤 S321 和步骤 S323 两者的条件为止，首标元素计算部分 309 能够计算出首标的生成所需的所有首标元素。

[0326] 即，由于在对于首标元素的具体计算之前，在步骤 S313 中将与关注的节点 (x，y)

相对应的首标元素 $c_{x,y}$ 初始化为 0，因此在步骤 S315 中标记了关注的节点 (x，y) 的所有子节点的情况下，节点 (x，y) 的首标元素 $c_{x,y}$ 被保持为 0 并被存储。同时，在未标记关注的节点 (x，y) 的所有子节点的情况下，在步骤 S317 中将 $c_{x,y}$ 替换为新值。因此，$c_{x,y}$ 具有不为 0 的值。

[0327] 首标元素计算部分 309 将通过上述步骤的重复所获得的所有首标元素传给首标信息生成部分 311。另外，首标元素计算部分 309 可将计算出的首标元素存储在存储单元 303 中。

[0328] 然后，首标信息生成部分 311 通过使用生成元 g 和步骤 S303 中选择的 t 来计算 g^t。另外，首标信息生成部分 311 通过仅使用具有非 0 值的首标元素 $c_{x,y}$，如以下那样形成首标 h (步骤 S325)。

[0329] $h = (g^t、c_{0,1}、\cdots\cdots、c_{H-1,X})\ (c_{x,y} \neq 0)\cdots\cdots$ (表达式 109)

[0330] 在生成首标信息之后，首标信息生成部分 311 将生成的首标 h 传给加密单元 315。另外，首标信息生成部分 311 可将生成的 h 存储在存储单元 303 中。

[0331] 然后，加密单元 315 从存储单元 313 接收待传递的未加密内容 M，并且通过使用会话密钥确定单元 307 确定的会话密钥 s，如下面那样对内容 M 加密。然后，内容传输单元 317 将经加密的内容 C 连同首标信息生成部分 311 生成的首标 h 以及节点索引的组 S 传送至客户 (步骤 S327)。

[0332] $C = E_S(M)\cdots\cdots$ (表达式 110)

[0333] 现在参考图 18 ～图 20 具体描述根据本实施例的加密阶段。图 18 ～图 20 是用于具体说明根据本实施例的加密阶段的说明图。在图 18 ～图 20 中示出了构造三叉树结构并且将九个客户分配给树叶的情况。

[0334] 在下面的示例中描述期望排除的客户是客户 2 和客户 3 的情况。如图 18 中所示，将树叶 (2,2) 分配给客户 2，并且将树叶 (2,3) 分配给客户 3。在这种情况下，从期望排除的客户 2 延伸至根的路径是图 18 中虚线所示的、从树叶 (2,2) 经由节点 (1,1) 延伸至根 (0,1) 的路径。类似地，从期望排除的客户 3 延伸至根的路径是图 18 中虚线所示的、从树叶 (2,3) 经由节点 (1,1) 延伸至根 (0,1) 的路径。在这种情况下，排除接收设备识别单元 261 标记根 (0,1)、节点 (1,1)、树叶 (2,2) 和树叶 (2,3)。注意在图 18 中，以使用虚线环绕被标记节点的方式示出了被标记的节点。然后，通过会话密钥确定单元 307 执行步骤 S303，并且确定会话密钥 s。

[0335] 然后，首标元素计算部分 309 执行步骤 S305 ～ S311。作为结果，用 0 替换参数 x，并且用 1 替换参数 y。然后，首标元素计算部分 S309 执行步骤 S313。在这种情况下，将对应于节点 (0,1) 的首标元素 $c_{0,1}$ 初始化为 0。然后，首标元素计算部分 S309 执行步骤 S315 以确定是否标记了根 (0,1) 的所有子节点。从图 19 中可清楚的看到，存在根 (0,1) 的三个子节点 (1,1)、(1,2) 和 (1,3)，并且节点 (1,2) 和 (1,3) 未标记。因此，首标元素计算部分 309 执行步骤 S317。

[0336] 在图 19 的情况下，未标记子节点的组 $S_{0,1}$ 是 {(1,2)、(1,3)}。另外，由于分别将 g_2 和 g_3 分配给节点 (1,2) 和 (1,3)，因此将首标元素 $c_{0,1}$ 计算为 $(v_{0,1} \cdot g_2 \cdot g_1)^t$。

[0337] 然后，首标元素计算部分 309 执行步骤 S319。通过步骤 S319，标记了作为节点 (1,2) (其为 $S_{0,1}$ 的一元素) 用作根的子树的所有节点 : 节点 (1,2)、树叶 (2,4)、树叶 (2,5) 以

及树叶 (2,6)。类似地,对于作为 $S_{0,1}$ 的另一元素的节点 (1,3),标记了节点 (1,3)、树叶 (2,7)、树叶 (2,8) 以及树叶 (2,8)。

[0338] 由于首标元素计算部分 309 在步骤 S321 中的判定是 y = 1,因而满足了条件。因此,随后首标元素计算部分 309 执行步骤 S323 中的判定。在这种情况下,由于 x = 0 ≠ 1,因此不满足分支条件。因此,通过设置到 x = 1,首标元素计算部分 309 返回步骤 S307 以重复处理。

[0339] 从返回的步骤 S307 至 S311 的处理被顺序地再次执行。此时,已经用 1 替换了 x,并且用 1 替换了 y。因此,接下来对节点 (1,1) 执行类似的处理。

[0340] 在这种情况下,节点 (1,1) 的未标记子节点的组 $S_{1,1}$ 仅是 {(2,1)}。类似地,执行首标元素的计算,并且将 $(v_{1,1} \cdot g_3)^t$ 计算为首标元素 $c_{1,1}$。然后,由于标记了节点 (1,1) 用作根的子树的所有节点,因此现在标记了尚未被标记的树叶 (2,1)。

[0341] 结果,标记了包含根和树叶的三叉树结构的所有节点。因此,在步骤 S323 的判定中,满足了分支条件。

[0342] 通过上述处理,首标信息生成部分 311 通过使用具有非 0 值的首标元素 $c_{x,y}$(即,$c_{0,1}$ 和 $c_{1,1}$),形成了首标 h。因此,形成了 $(g^t, c_{0,1}, c_{1,1})$ 作为首标 h。另外,表示能够通过上述处理解密已传递内容的客户的组的 S 为 {(1,2),(1,3),(2,1)}。

[0343] 如上所述,在根据本实施例的加密内容传递块中,传递者 513 如图 16 中所示那样通过使用公钥 PK 以及传递者 513 选择的随机数 t 来计算会话密钥 s 和首标 h。同时,传递者 513 还判定能够解密内容的客户的组 S。然后,传递者 513 经由广播通信信道 515 传递经加密的内容 C、首标 h 以及组 S,而不管是客户 507 还是非客户 517。

[0344] < 接收设备 40 的运算 :解密阶段 >

[0345] 现在参考图 21 详细描述根据本实施例的接收设备 40 的运算(即,解密阶段)。图 21 是作为接收设备 40 的密钥处理方法的解密阶段的流程图。

[0346] 首先,由接收单元 401 接收经加密内容 C、首标 h 以及组 S 的接收设备 40 将信息临时地存在存储单元 403 中。然后,执行经加密内容 C 的解密处理。

[0347] 首先,接收设备 40 的判定单元 405 查阅存储在存储单元 403 中的组 S 以判定组 S 中包含的节点是否存在于从分配给接收设备 40 的树叶至根的各节点之中(步骤 S501)。作为判定的结果,在不存在组 S 中包含的节点的情况下,判定单元 405 判定接收设备 40 被排除,并且终止下面所述的解密处理。同时,作为判定的结果,在存在组 S 中包含的节点的情况下,接收设备 40 将组 S 中包含的节点的节点索引设置为 (x′,y′),并且执行下面的步骤 S503。

[0348] 接收设备 40 的解密单元 407 在接收单元 401 接收到的并且在存储单元 403 中存储的首标 h 的各元素之中选择与节点 (x′,y′) 的父节点 (x,y) 和 g^t 相对应的首标元素 $c_{x,y}$(步骤 S503)。这里,由下面的表达式表示节点 (x′,y′) 的父节点 (x,y)。

[0349] [算式 24]

[0350] $$(x, y) = (x' - 1, \left\lceil \frac{y'}{Y} \right\rceil) \cdots\cdots \text{(表达式 111)}$$

[0351] 另外,如下面那样,解密单元 407 通过使用公钥以及来自于接收设备 40 的私钥 d_i 的、与节点 (x′,y′) 相对应的元素来获取会话密钥 s(步骤 S503)。

[0352] [算式 25]

[0353] $$s=\frac{e(g_{i_x},c_{x,y})}{e(g_{i_x}^{\gamma_{|x|-1}}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j+i_x},g^t)}\cdots\cdots(\text{表达式 112-1})$$

[0354] $$=\frac{e(g_{i_x},(v_{x,y}\cdot\prod_{j\in S_{x,y}}g_{\gamma+1-j})^t)}{e(v_{i_x}^{(\alpha^{|x|})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j+i_x},g^t)}\cdots\cdots(\text{表达式 112-2})$$

[0355] $$=\frac{e(g_{i_x},g_{\gamma+1-i_x}^{\ t})\cdot e(g_{i_x},(v_{i_x}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j})^t)}{e(v_{i_x}^{(\alpha^{|x|})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j+i_x},g^t)}\cdots\cdots(\text{表达式 112-3})$$

[0356] $$=\frac{e(g,g_{\gamma+1})^t\cdot e(g^t,(v_{i_x}^{(\alpha^{|x|})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j+i_x})^t)}{e(v_{i_x}^{(\alpha^{|x|})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_x}}g_{\gamma+1-j+i_x},g^t)}\cdots\cdots(\text{表达式 112-4})$$

[0357] $$=e(g,g_{\gamma+1})^t\cdots\cdots(\text{表达式 112-5})$$

[0358] 然后，解密单元 407 通过使用所获取的会话密钥 s，对经加密的内容 C 解密以获得纯文本 M（步骤 S505）。

[0359] $M = Ds(C)\cdots\cdots$（表达式 113）

[0360] 然后，参考图 22 具体描述根据本实施例的解密阶段。图 22 是用于具体说明根据本实施例的解密阶段的说明图。在图 22 中，示出构造了三叉树结构并且向树叶分配九个客户的情况。

[0361] 在下面的示例中，假设如下的情况：期望排除的客户是客户 2 和客户 3，并且向客户 1 ～ 9 传递经加密的内容 C、首标 h 以及组 S。在下文中详细描述被分配给树叶 (2,4) 的客户 4 解密所传递内容的情况。

[0362] 在图 22 的情况下，从分配给客户 4 的树叶 (2,4) 延伸至根 (0,1) 的路径中包含的节点是上述的树叶 (2,4)、节点 (1,2) 以及根 (0,1)。这里，客户 4 使用的接收设备 40 的判定单元 405 判定接收单元 401 接收到的关于组 S 的信息中是否包含上述三个节点。

[0363] 在图 22 的情况下，由于客户 2 和客户 3 是期望排除的客户，因此组 S 是 {(1,2), (1,3), (2,1)}。如据此清楚看到的那样，组 S 中包含节点 (1,2)，该节点 (1,2) 是向其分配了客户 4 的树叶 (2,4) 的父节点。因此，判定单元 405 判定满足了步骤 S501 的分支条件。解密单元 407 继续执行解密处理。

[0364] 在这种情况下，步骤 S503 中的节点 (x′，y′) 对应于节点 (1,2)。因此，节点 (x′，y′) 的父节点 (x，y) 是根 (0,1)。解密单元 407 选择与节点 (0,1) 以及 g^t 相对应的首标元素 $c_{0,1}$。另外，解密单元 407 通过使用与 $v_{0,1}$ 有关的元素（其为来自于客户 4 的私钥 d_4 的、与节点 (0,1) 相对应的元素）以及公钥 PK 来计算会话密钥 s。具体地，由下面的表达式表示用于获得会话密钥 s 的双线性映射。

[0365] [算式 26]

[0366] $$s=\frac{e(g_{4_1},c_{0,1})}{e(g_{4_1}{}^{\gamma_{4_0}}\cdot\prod_{\substack{j\in S_{0,1}\\ j\neq 4_1}}g_{Y+1-j+4_1},g^r)}$$

[0367] 以上已详细描述了根据本实施例的加密密钥传递系统 10 中的三个阶段（密钥生成、加密以及解密）的示例。

[0368] 注意，可以创建用于促使计算机用作根据上述实施例的密钥生成设备 20、加密设备 30 以及接收设备 40 的计算机程序。通过将计算机程序存储在计算机中提供的存储单元中并且由计算机中提供的 CPU 来读取和执行该计算机程序，其促使计算机用作上述的密钥生成设备 20、加密设备 30 以及接收设备 40。另外，也可提供具有记录在其上的计算机程序的计算机可读记录介质。例如，该记录介质是磁盘、光盘、磁光盘、闪存等。另外，例如，可以经由网络传递上述计算机程序，而无需使用所述记录介质。

[0369] 现在，在下文中将根据本实施例的加密密钥传递系统 10 与作为基础技术的、非专利文献 1 中所述的内容传递系统相比较。

[0370] 作为基础技术的、非专利文献 1 的方法是在使用公钥的内容传递系统中通过使用双线性映射来解决合谋程序的方法。在该方法中，预先将客户分组为多个子群，并且在传递内容时，传递包含依据子群而不同的所有首标元素的首标。因此，即使在排除客户的数量增大的情况下，也可以将首标大小保持恒定。然而，即使在为实际内容传递系统所假设的情况下（诸如不存在排除客户的情况或者排除客户的数量很少的情况），也总是必须传递具有恒定大小的首标。因此，存在传递效率被降低的问题。

[0371] 另外，存在另一问题：在属于分组后子群的客户的数量 B 很大的情况下，或者客户所属子群中的排除客户的数量很少的情况下，客户在解密时需要执行的运算的计算量增大。

[0372] 同时，在根据本实施例的密钥生成设备中，通过使用基础技术的方法来构造逻辑树并且使得参数的数量略微增加，可以灵活地配置子群。具体地，在不存在排除客户或者排除客户的数量很少的情况下，可以减小所传递首标的大小，并且可以将客户需要执行的运算的计算量减小至小于等于基础技术中所述方法的计算量。在下文中描述基础技术和本实施例之间的主要差异，同时将注意力放在各阶段的差异中。另外，通过使用数值的具体示例，就解密所需的首标大小以及计算量进行比较。

[0373] ＜密钥生成阶段的差异＞

[0374] 首先描述密钥生成阶段的差异。在基础技术的方法中，在步骤 S11 和步骤 S13 中设置了各种参数之后，在步骤 S15 中，客户被分组为每一个均包含 B 个客户的 A 个子群。类似地，在本实施例中，在步骤 S101 和步骤 S103 中设置了各种参数，并且将客户分组为每一个均包含 Y 个客户的 X 个子群。

[0375] 然而，在本实施例中，在步骤 S105 中，进一步构造将客户分配给树叶的 Y 元树结构。因此，在基础技术中，在步骤 S19 中需要用于为每个子群合并 (intergrate) 首标元素的 A 个中心保密 γ_1、……、γ_A 以及与这些中心保密相对应的 A 个公共值 v_1、……、v_A（其中 A 表示子群的分组数），而在本实施例中，由于可以为步骤 S105 中构造的 Y 元树的除了树叶之外的所有节点形成子群，因此，需要 N 个值（其中，N 表示除了树叶之外的节点总数）。

[0376] 另外，在基础技术中，客户 i 仅属于由下面的表达式表示的子群 S_a。

[0377] [算式 27]

[0378]

$$S_a(a=\left\lceil \frac{i}{B} \right\rceil)$$

[0379] 因此，中心向客户 i 秘密地传递私钥：

[0380] [算式 28]

[0381] $$d_i = g_b^{\gamma_a} = v_a^{\alpha^b} \in G$$

[0382] 然而，在本实施例中，在步骤 S105 中构造了逻辑树之后，在步骤 S109 中，该逻辑树的每个节点均可用于子群的重构。因此，客户 i 需要属于由从分配 给客户 i 的树叶至根的所有节点所构成的多个子群。

[0383] 因此，在本实施例的步骤 S115 中，必须为客户 i 保留多个私钥。如上所述，在密钥生成阶段中，由于在本实施例中构造了逻辑树，因此与基础技术相比较，所需参数的数量略微增加。然而，在不存在排除客户的情况下或者排除客户的数量很少的情况下，与传统技术相比较，可以减小接下来所述的加密阶段中生成的首标的首标大小。

[0384] 〈加密阶段的差异〉

[0385] 接下来描述加密阶段。在基础技术中，在步骤 S31 中生成会话密钥。然后，在步骤 S33 中，为各子群选择非排除客户，并且确定分配给各客户的子群中客户索引的组 S1(1 = 1、……、A)。然后，在步骤 S35 中，计算仅各子群中非排除客户可通过其获得会话密钥的首标元素，并且配置首标。因此，除非排除了属于子群的所有客户，否则必须计算与所有子群相对应的首标元素。因此，无论排除客户的数量 r 很大或很小，都将首标大小保持恒定。

[0386] 同时，在本实施例中，在步骤 S301 中标记了从分配给排除客户的树叶至根的所有节点，并且将非排除客户通过其从首标 h 中识别分配给非排除客户的首标元素的一组节点索引设置为 S。然后，在步骤 S303 中，根据如基础技术中那样的过程在步骤 S303 中生成会话密钥 s。在步骤 S305 ～ S325 中，计算仅分配给未标记节点的客户可通过其获取会话密钥 s 的首标元素，并且配置首标 h。

[0387] 更详细地，在本实施例的步骤 S317 中，为属于 Layer x 的节点之中的未标记节点生成首标元素。这是与基础技术中步骤 S35 的运算相类似的运算。然而，由于已存在 A 个子群，因此在基础技术的步骤 S35 中必须生成 A 个首标元素，而在本实施例中，仅对特定节点的一组子节点执行步骤 S317，并且在步骤 S307 ～ S323 中重复该处理。

[0388] 这里，如步骤 S315 ～ S319 中所示，对于一旦已经生成其首标元素的节点来说，通过标记属于将该节点作为其顶点的子树的所有节点，不需要生成与这些节点相对应的首标元素。因此，出现如下优点：可以将用于包含节点的所有非排除客户的首标元素一起合并在路径中。因此，在排除客户的数量较少的情况下，可以将更大数量的节点合并在一起。因此，可以减小首标尺 寸。

[0389] 〈解密阶段的差异〉

[0390] 最后描述解密阶段。在基础技术中，非排除客户在步骤 S53 中获取与客户属于的子群相对应的首标元素，并且通过使用该首标元素、公钥和私钥来取得会话密钥。同时，在本实施例中，在步骤 S503 中，非排除客户在从分配给客户的树叶延伸至根的路径中存在的

节点之中获取与包含在 S 中的节点的父节点相对应的首标元素，并且通过使用该首标元素、公钥和私钥来取得会话密钥。

[0391] 其区别仅在于所使用的相应首标元素和私钥，并且执行如基础技术中那样的运算。然而，客户在基础技术的解密阶段中需要执行的运算的计算量是 2PAIR+INV+(B-1-r_a)MUL，而本实施例中的计算量是 2PAIR+INV+(Y-1-r_a)MUL。

[0392] ＜关于首标大小和计算量的比较＞

[0393] 在基础技术中，将一组客户分组为每一个均具有 B 个客户的 A 个子群。生成与各子群相对应的首标元素，并且作为首标共同地传递所有的首标元素。因此，无论排除客户的数量很大还是很小，首标大小总是 A+1。无论排除客户的数量多少，这均具有可将首标大小保持恒定的优点，然而这具有不可减小首标大小的缺点。在实际的内容传递系统中，在排除客户的数量相对于客户的总数的百分比很小的范围内需要高效传递内容的能力。因此，即使通过更加强调安全和便利来使用基础技术的方法，在内容传递时也存在增大了首标大小冗余度的问题。

[0394] 为了减小基础技术中的问题，可以设想通过减少一组客户的分组数 A 来减小其首标大小。然而，在这种情况下，存在如下问题：增大了表示属于分组后子群的客户数的 B 值，并且增大了表示每个客户需要执行的运算的计算量的值 2PAIR+INV+(B-1-r_a)MUL。

[0395] 同时，如在基础技术中那样，在本实施例中，将一组客户分组为每一个均包含 Y 个客户的 A 个子群。然而，此外通过添加一些参数构造了将分组后子群中的各客户设置为树叶的 Y 元树。因此，虽然无论是否存在排除客户，基础技术中的首标大小都是 A+1，但是在将根定义为最上层的情况下，可以 将属于不存在排除客户的子群的每个客户看作上层的成员。从而，可以将多个子群看作为一个子群，并且可以减小首标大小。另外，如上所述，虽然将每个客户需要执行的运算的计算量表示为 2PAIR+INV+(Y-1-r_a)MUL，但是通过将 Y 设置为 B 或更小，可以将计算量减小为小于等于基础技术方法中的计算量。

[0396] 如上所述，与基础技术相比较，本发明是使用公钥的内容传递方法中的一种。与基础技术相比，本发明具有下面所述的特征。

[0397] 第一，在本实施例中，通过向基础技术的方法添加参数构造了逻辑树，并且将所添加的参数分配给逻辑树的各节点。

[0398] 第二，用作中心的密钥生成设备预先向各客户传递与分配给逻辑树的参数有关的信息，作为附加私钥。

[0399] 第三，已加密内容的传递者操作加密设备。在排除了客户的情况下，如使用公共密钥的内容传递方法中那样，传递者生成已对每个节点执行了排除的首标 h。

[0400] 第四，每个客户操作接收设备以通过使用如基础技术中那样的方法，根据公钥 PK、首标 h 以及私钥 d_i 来计算会话密钥 s。

[0401] 第五，通过如上述第一至第四特征那样配置基础技术的方法，可以将客户解密所需的计算量减小至小于等于基础技术方法中的计算量。

[0402] 第六，通过如上述第一至第四特征那样配置基础技术的方法，在排除客户数量很少的情况下，与基础技术相比，可以减小首标大小。

[0403] 示例

[0404] 为了更详细地描述本实施例的优点，如图 23 ～ 26 中具体示例，示出在将参数 n、

A、B、X 和 Y 设置为很小的值的情况下，首标大小方面以及解密所需计算量方面的比较。

[0405] 在基础技术中，建议将与客户数 n 有关的分组后子群中包含的客户数 B 的值设置为 $B = (n)^{1/2}$。同时，在本实施例中，通过将逻辑树的分支数 Y（其为与基础技术中的 B 相对应的参数）设置为小于等于 B，可以增大首标大小和计算量方面的效率。

[0406] 因此，在下面为了比较，将客户数 n 设置为相同，并且设置 Y ＜ B。图 23 和图 24 中分别示出基础技术和本实施例之间就首标大小方面和解密所需运算的计算量方面的比较。另外，图 25 和 26 中分别示出在设置 Y ＝ B 的情况下的首标大小方面以及解密所需计算量方面的比较。

[0407] 在图 23 和 24 中，作为具体数值，将基础技术方法中的各参数设置为 n ＝ 64、A ＝ 8 且 B ＝ 8，而将本实施例中各参数设置为 n ＝ 64、X ＝ 16 且 Y ＝ 4。另外，在图 25 和 26 中，将各参数设置为 n ＝ 64、X ＝ 8 且 B ＝ Y ＝ 8。然而，为了简化，将所使用的双线性群以及双线性群的大小设置为相同。

[0408] （关于设置 Y ＜ B 的情况）

[0409] 首先说明图 23 和 24。在图 23 中，横坐标轴表示排除客户的数量，而纵坐标表示首标大小（首标元素的总数）。另外，在图 24 中，横坐标轴表示排除客户的数量，而纵坐标表示解密所需运算的计算量。然而，关于解密所需运算的计算量，由于仅有双线性群 G 上的乘法部分影响基础技术与本实施例之间的差异，因此图 24 中的纵坐标表示双线性群 G 上的乘法的数量。另外，在图 23 中，实线表示传统技术方法中的首标大小，而虚线表示本实施例中的首标大小。另外，在图 24 中，实线表示传统技术方法中的计算量，而虚线表示本实施例中的计算量。

[0410] 关于首标大小方面的比较，如从图 23 中可清楚看到的那样，在排除客户的数量 r 小于 4 的情况下，根据本实施例的方法中的首标大小小于基础技术的方法中的首标大小。即，这种情况表明：即使在大约上至 6％的总客户被排除的情况下，在根据本实施例的方法中也可以更高效地传递内容。

[0411] 关于解密所需计算量方面的比较，如从图 24 中可清楚看到的那样，在排除客户的数量 r 小于 60 的情况下，根据本实施例的方法中的计算量小于基础技术的方法中的计算量。这表明：在根据本实施例的方法中可以更高效地解密内容。另外，在排除客户的数量超过 60 的情况下，也可以看到：可以获得与基础技术方法中的计算量相等的计算量。因此，在如上述那样设置参数的情况下，当不存在排除客户或排除客户的数量很少的时候，根据本实施例的方法能够获得减小的首标大小并且获得每个客户在解密时需要执行运算的减小的计算量。所以，可以说：与根据基础技术的方法相比，根据本实施例的方法能够实现内容的高效传递。

[0412] （关于设置 Y ＝ B 的情况）

[0413] 接下来说明图 25 和 26。由于在图 25 和 26 中仅改变了上述图 23 和 24 中 X 和 Y 的值，因此图 25 和 26 中的横坐标轴和纵坐标轴、实线以及虚线表示与图 23 和 24 中的那些相同。

[0414] 在设置 X ＝ A ＝ 8 且 Y ＝ B ＝ 8 的情况下，关于首标大小方面的比较，如从图 25 中可清楚看到的那样，在排除客户的数量 r 小于 7 的情况下，根据本实施例的方法中的首标大小小于基础技术的方法中的首标大小。即，这种情况表明：即使在大约上至 9％的总客户

被排除的情况下，在根据本实施例的方法中也可以更高效地传递内容。此外，在排除客户的数量大于等于 7 的情况下，可以获得与基础技术的方法中的首标大小相等的首标大小。因此，无论排除客户的数量如何，均可以将首标大小减小至小于等于基础技术方法中的首标大小。

[0415] 另外，关于解密所需计算量方面的比较，如从图 26 中可清楚看到的那样，无论排除客户的数量 r 如何，均可以获得与基础技术的方法中的计算量相等的计算量。因此，在将各参数设置为 X ＝ A ＝ 8 且 y ＝ B ＝ 8 的情况下，可以看到，当不存在排除客户或排除客户的数量很少的时候，可以减小首标大小，并且解密仅需要与基础技术方法中的计算量相等的计算量。

[0416] 如从上面清楚看到的那样，通过应用本实施例，与基础技术相比，可以在更实际的内容传递系统中实现高效的内容传递，同时保持如基础技术中那样的便利和安全。

[0417] 如上所述，本发明是这样的方法：在用于通过使用公钥来安全传递内容的内容传递系统中，与传统方法相比，其用于实现待传递的数据量的减小以及解密所需的计算量的减小。通过本发明的实施，与使用公钥的传统内容传递方法相比，可以获得高效的内容传递。

[0418] 以上已经参考附图描述了本发明的优选实施例。然而，不用说，本发明并不限于这些实施例。显而易见，本领域的技术人员可在权利要求书中所述的范围之内构思各种变化或修改，应该明白，所述各种变化或修改都必然地落在本发明的技术范围内。

[0419] 例如，虽然上述树结构构造单元 231 假设了分支从顶部向底部生成的树 结构，但是三叉结构并不必然地受限于此。可以给出分支从底部向顶部、从左向右或从右向左生成的树结构。

[0420] 另外，本说明书每个流程图中的各步骤并不必然地以根据如流程图所述次序的时间顺序方式来处理。各步骤可包含并行或单独执行的处理（例如，并行处理或基于对象的处理）。

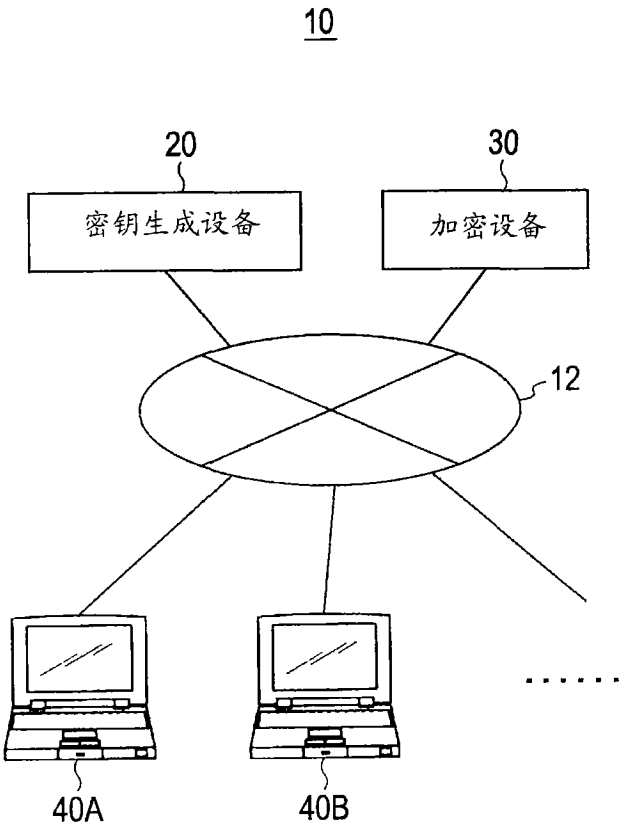


图 1

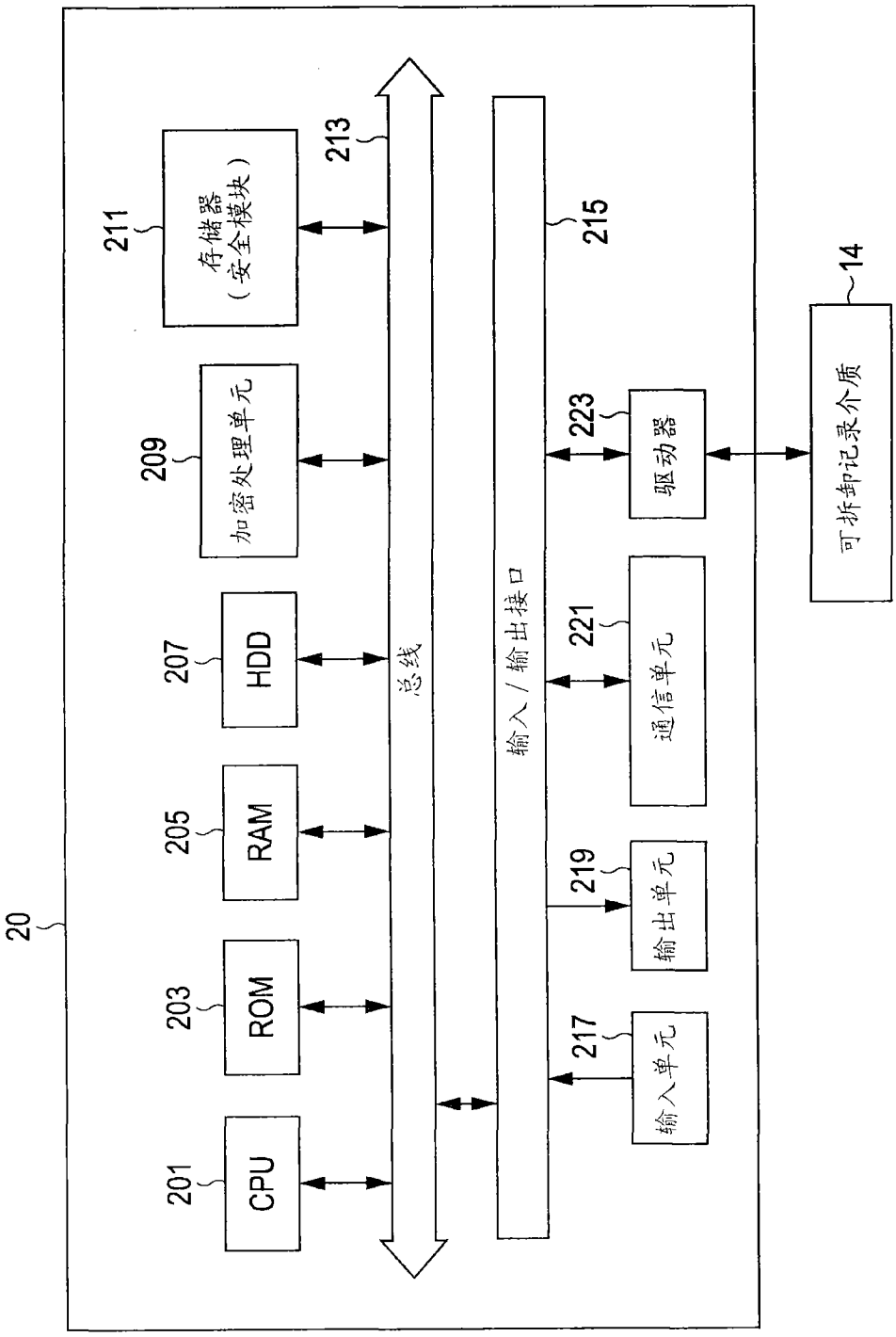

20
201
CPU
203
ROM
205
RAM
207
HDD
209
加密处理单元
211
存储器
（安全模块）
213
总线
215
输入/输出接口
217
输入单元
219
输出单元
221
通信单元
223
驱动器
14
可拆卸记录介质

图 2

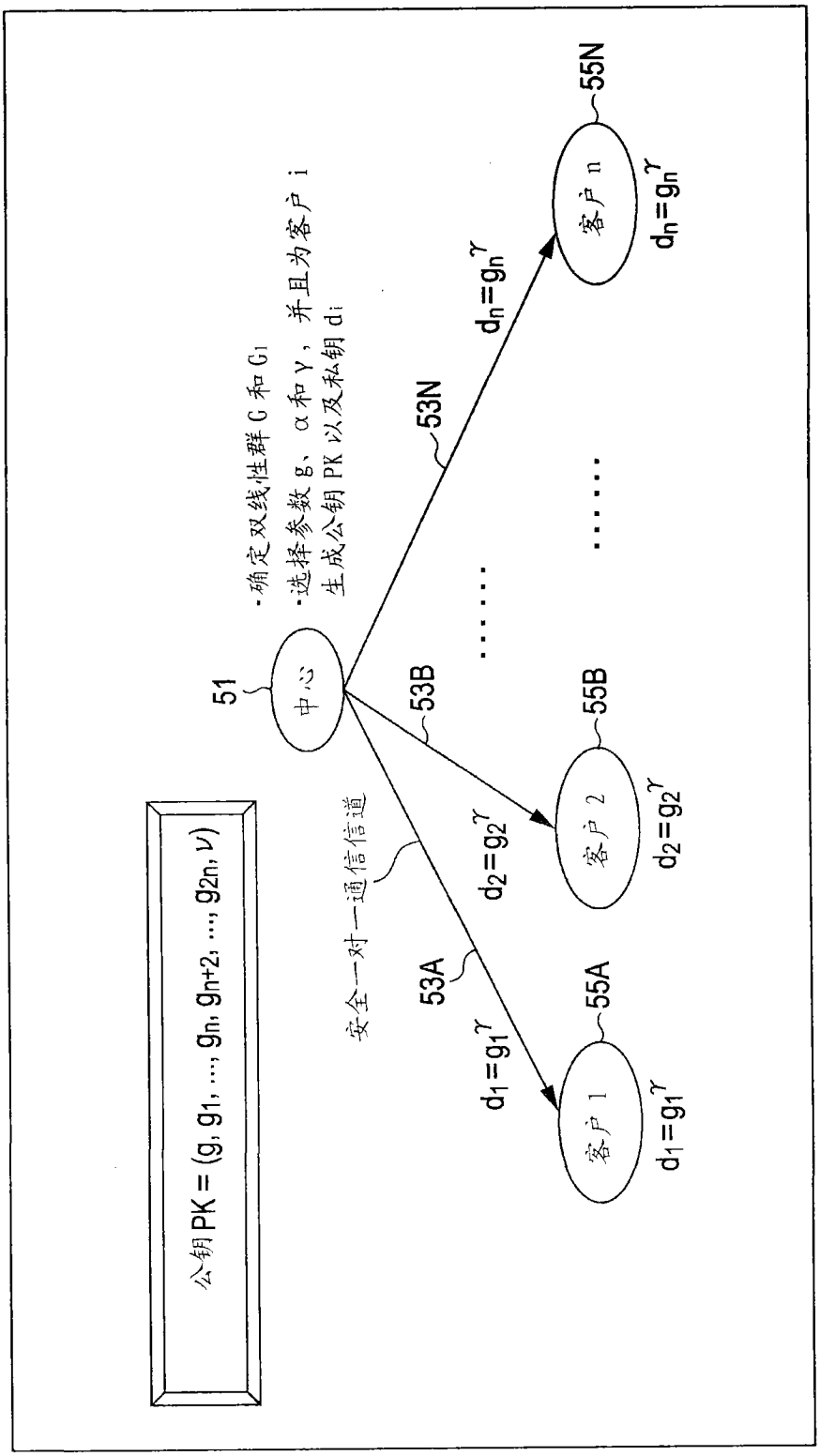

公钥 PK = (g, g1, ..., gn, gn+2, ..., g2n, v)
51
中心
·确定双线性群 G 和 G1
·选择参数 g、α和 γ，并且为客户 i 生成公钥 PK 以及私钥 di
安全一对一通信信道
53A
53B
53N
55A
55B
55N
客户 1
客户 2
客户 n
d1=g1^γ
d2=g2^γ
dn=gn^γ

图 3

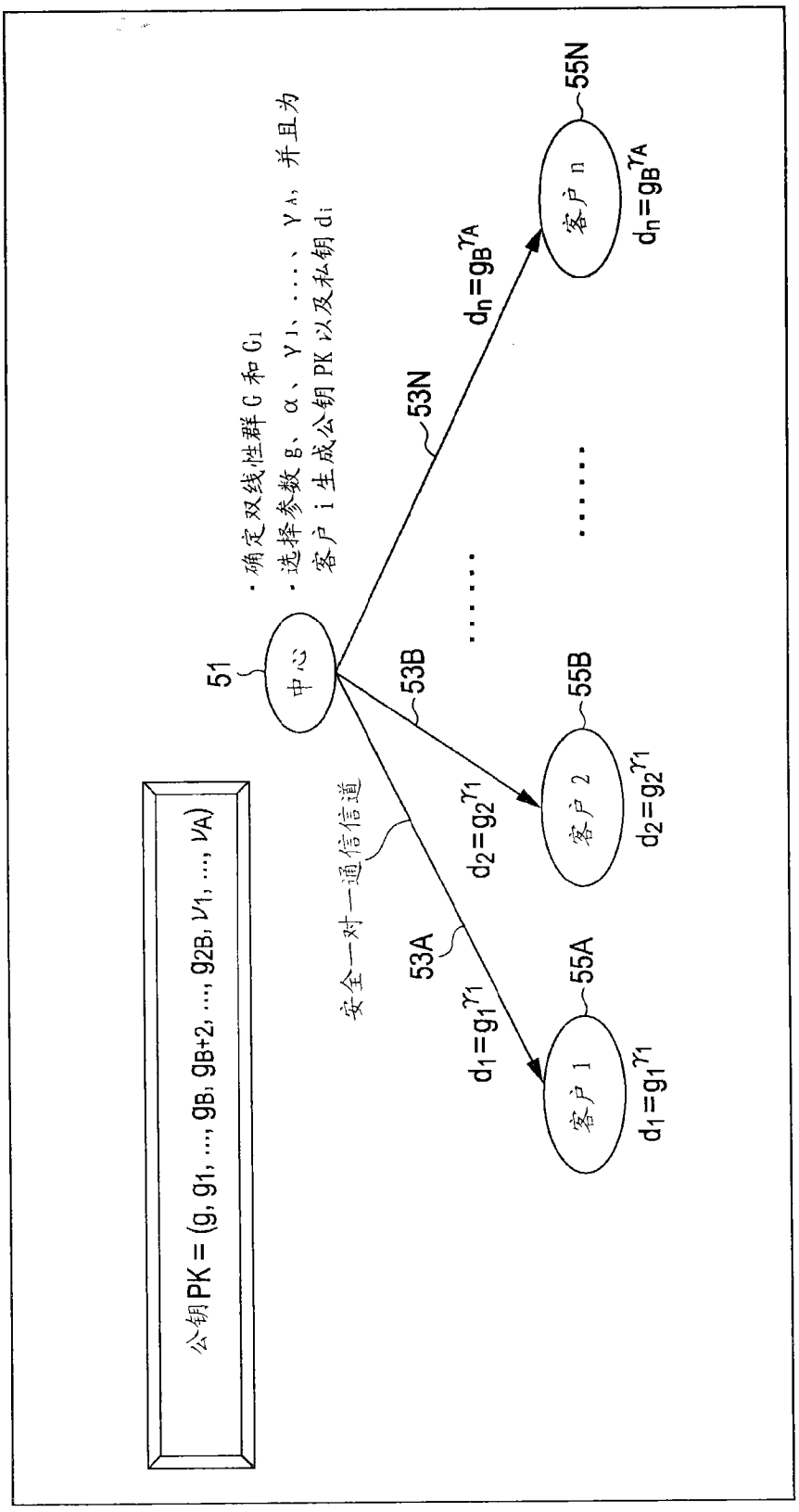

公钥PK = (g, g1, ..., gB, gB+2, ..., g2B, v1, ..., vA)
51
中心
• 确定双线性群 G 和 G1
• 选择参数 g、α、v1、...、vA，并且为客户 i 生成公钥 PK 以及私钥 di
安全一对一通信信道
53A
53B
53N
d1=g1^γ1
d2=g2^γ1
dn=gB^γA
55A
55B
55N
客户 1
客户 2
客户 n
d1=g1^γ1
d2=g2^γ1
dn=gB^γA

图 4

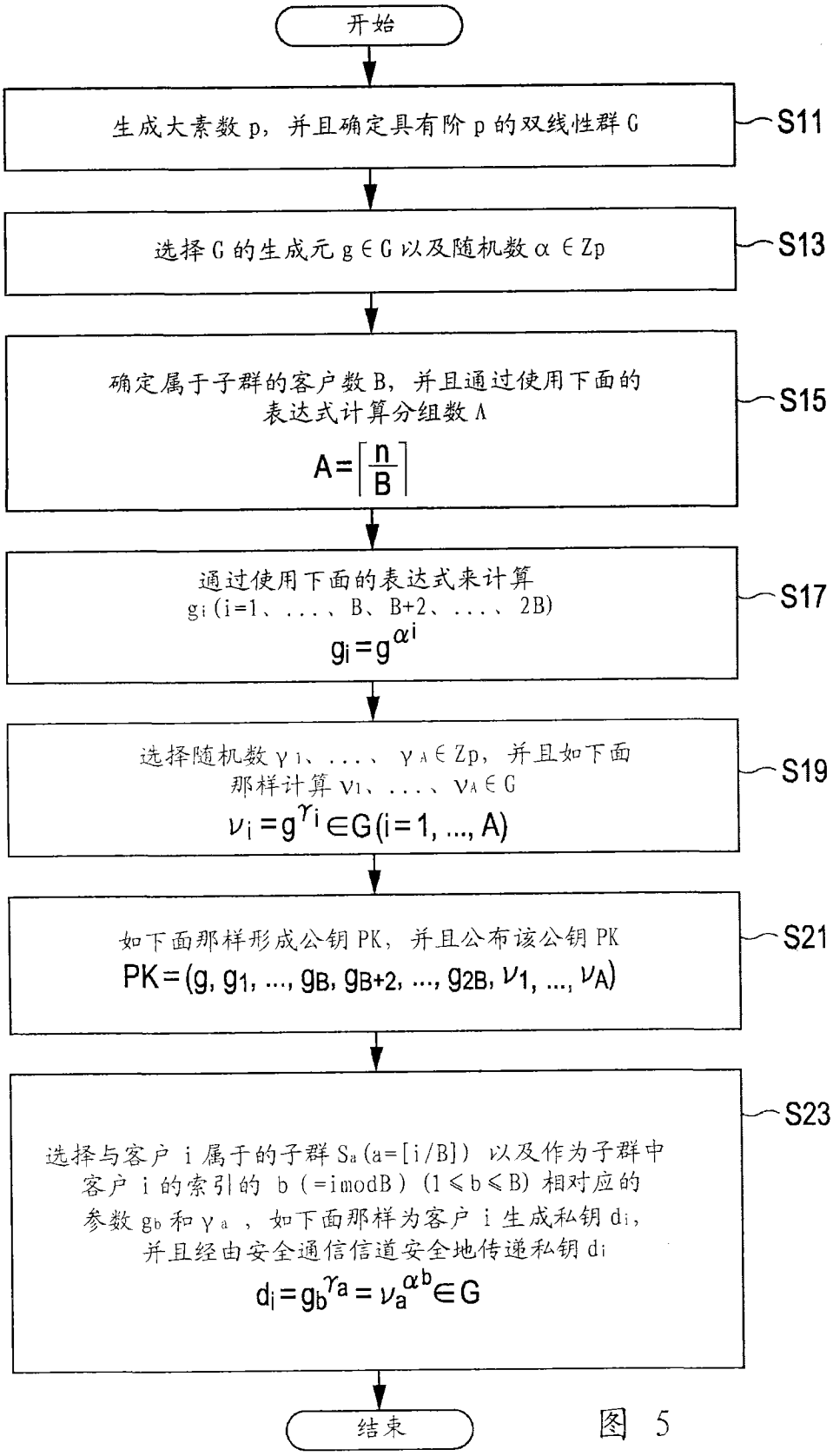

开始
生成大素数 p，并且确定具有阶 p 的双线性群 G
S11
选择 G 的生成元 g ∈ G 以及随机数 α ∈ Zp
S13
确定属于子群的客户数 B，并且通过使用下面的表达式计算分组数 A
$A=\lceil \frac{n}{B} \rceil$
S15
通过使用下面的表达式来计算 g_i (i=1、...、B、B+2、...、2B)
$g_i=g^{\alpha i}$
S17
选择随机数 γ_1、...、$\gamma_A \in Zp$，并且如下面那样计算 v_1、...、$v_A \in G$
$v_i=g^{\gamma i} \in G(i=1, ..., A)$
S19
如下面那样形成公钥 PK，并且公布该公钥 PK
$PK=(g, g_1, ..., g_B, g_{B+2}, ..., g_{2B}, v_1, ..., v_A)$
S21
选择与客户 i 属于的子群 S_a (a=[i/B]) 以及作为子群中客户 i 的索引的 b (=imodB) (1≤b≤B) 相对应的参数 g_b 和 γ_a，如下面那样为客户 i 生成私钥 d_i，并且经由安全通信信道安全地传递私钥 d_i
$d_i=g_b^{\gamma a}=v_a^{\alpha b} \in G$
S23
结束

图 5

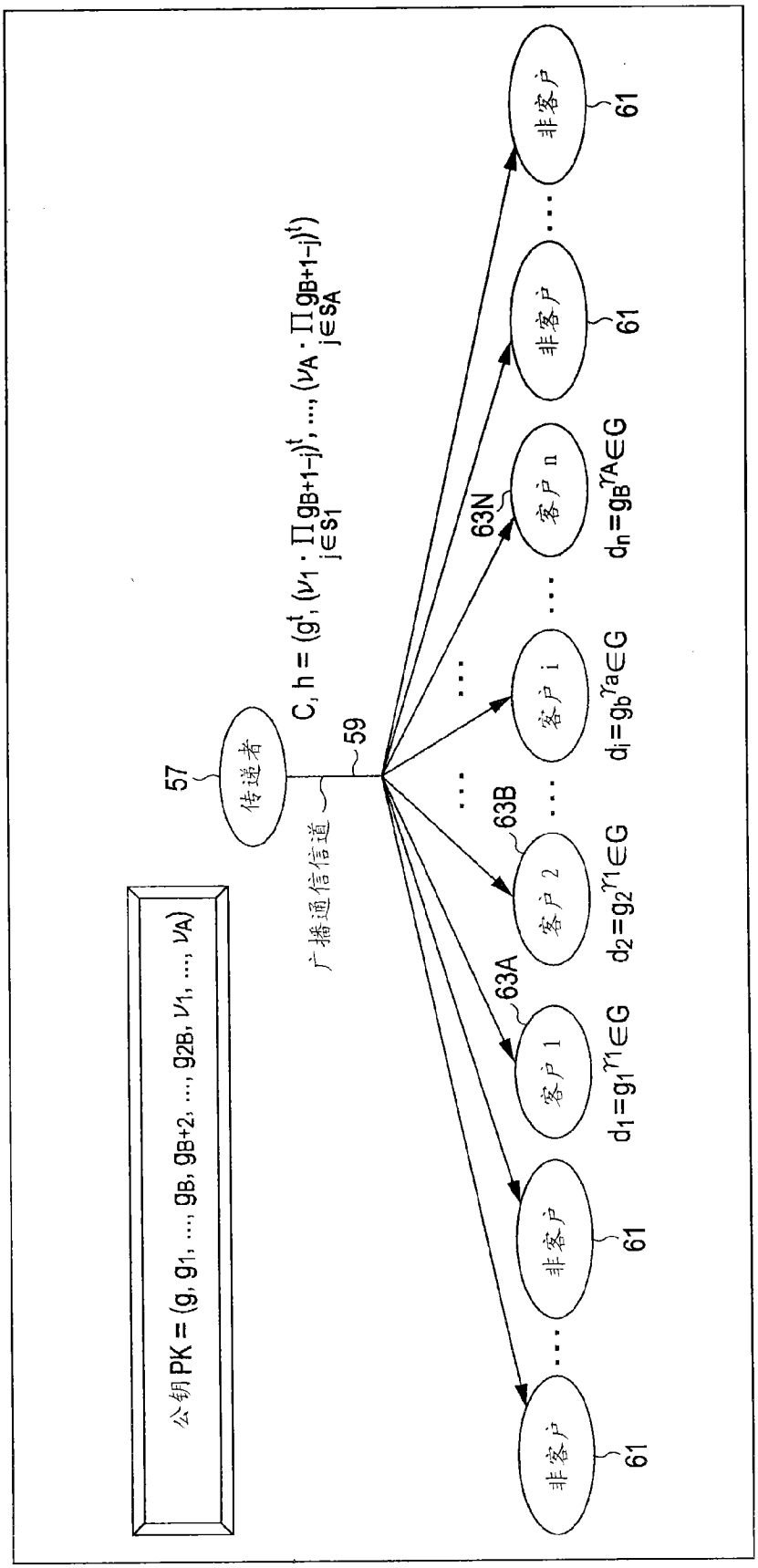

公钥 PK = (g, g1, ..., gB, gB+2, ..., g2B, v1, ..., vA)
57
传递者
C, h = (g^t, (v1 · ∏ gB+1-j)^t, ..., (vA · ∏ gB+1-j)^t)
59
广播通信信道
63A
63B
63N
客户 1
客户 2
客户 i
客户 n
非客户
61
d1=g1^γ1∈G
d2=g2^γ1∈G
di=gb^γa∈G
dn=gB^γA∈G

图 6

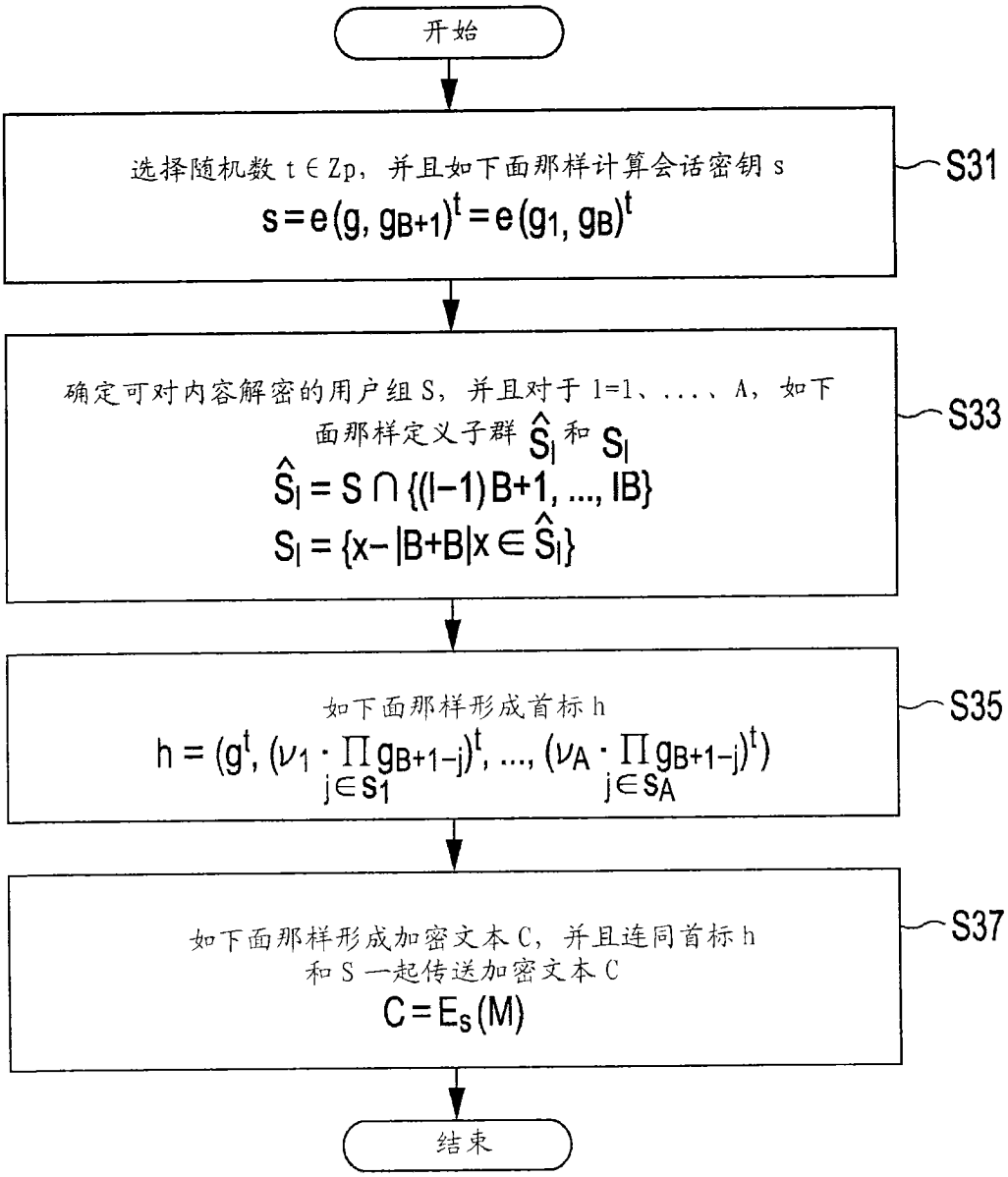

开始
选择随机数 t ∈ Zp，并且如下面那样计算会话密钥 s
$s = e(g, g_{B+1})^t = e(g_1, g_B)^t$
S31
确定可对内容解密的用户组 S，并且对于 l=1、...、A，如下面那样定义子群 $\hat{S}_l$ 和 S_l
$\hat{S}_l = S \cap \{(l-1)B+1, ..., lB\}$
$S_l = \{x - lB + B | x \in \hat{S}_l\}$
S33
如下面那样形成首标 h
$h = (g^t, (v_1 \cdot \prod_{j \in S_1} g_{B+1-j})^t, ..., (v_A \cdot \prod_{j \in S_A} g_{B+1-j})^t)$
S35
如下面那样形成加密文本 C，并且连同首标 h 和 S 一起传送加密文本 C
$C = E_s(M)$
S37
结束

图 7

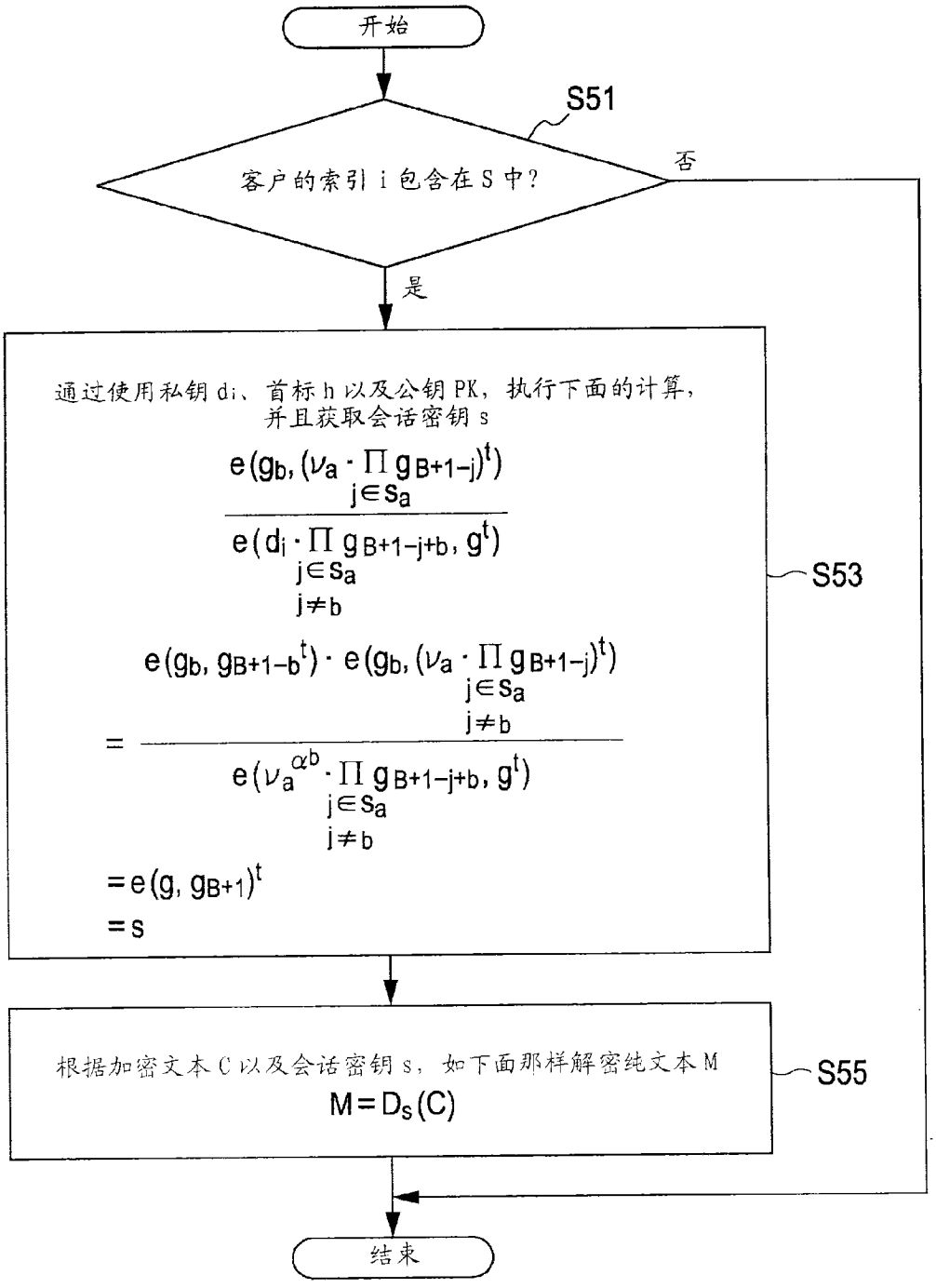

开始
S51
客户的索引 i 包含在 S 中？
否
是
通过使用私钥 d_i、首标 h 以及公钥 PK，执行下面的计算，并且获取会话密钥 s
$$\frac{e(g_b, (v_a \cdot \prod_{j \in S_a} g_{B+1-j})^t)}{e(d_i \cdot \prod_{\substack{j \in S_a \\ j \neq b}} g_{B+1-j+b}, g^t)}$$
$$= \frac{e(g_b, g_{B+1-b}^t) \cdot e(g_b, (v_a \cdot \prod_{\substack{j \in S_a \\ j \neq b}} g_{B+1-j})^t)}{e(v_a^{\alpha b} \cdot \prod_{\substack{j \in S_a \\ j \neq b}} g_{B+1-j+b}, g^t)}$$
$$= e(g, g_{B+1})^t$$
$$= s$$
S53
根据加密文本 C 以及会话密钥 s，如下面那样解密纯文本 M
$$M = D_s(C)$$
S55
结束

图 8

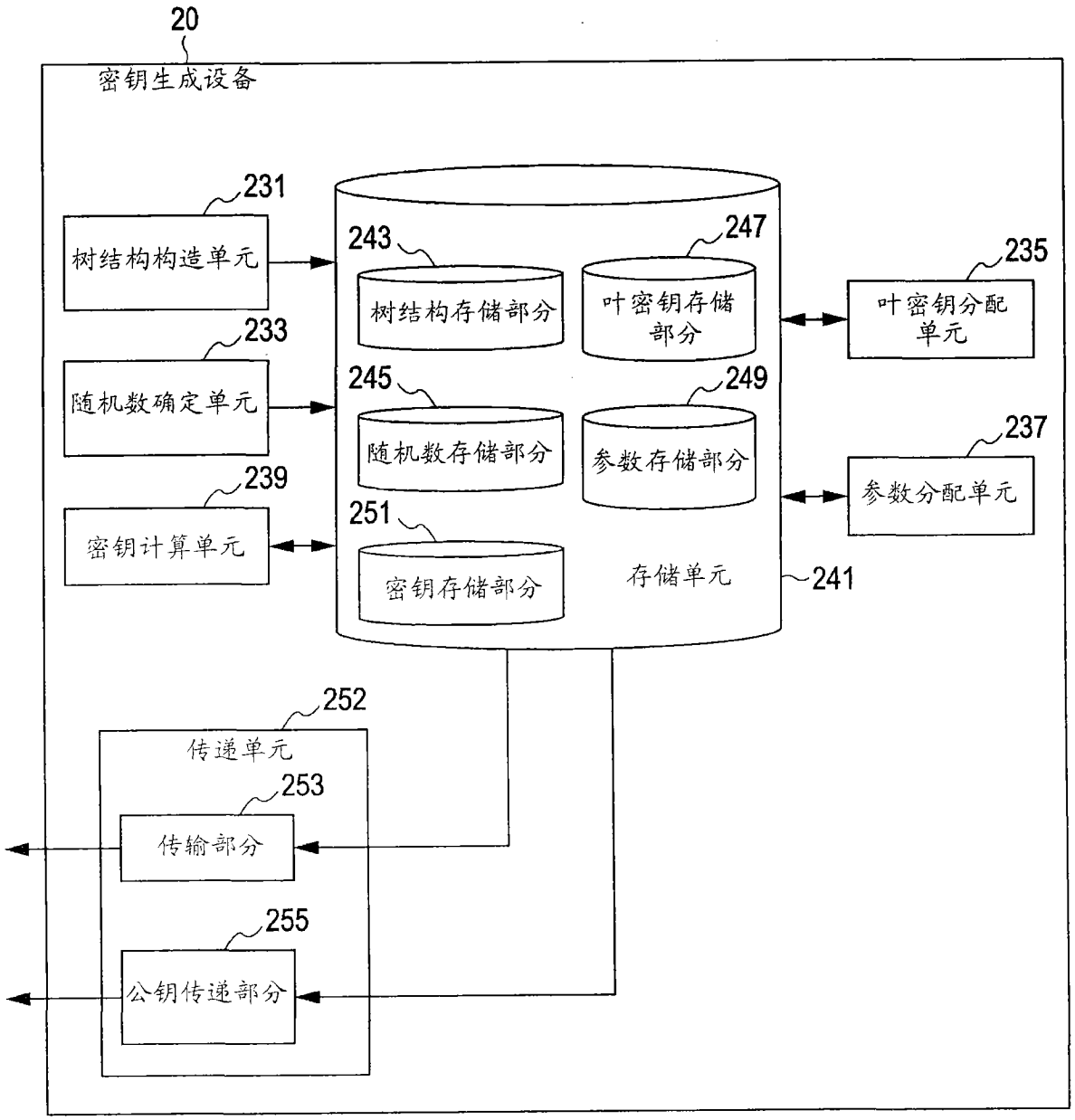

20
密钥生成设备
231
树结构构造单元
233
随机数确定单元
239
密钥计算单元
243
树结构存储部分
247
叶密钥存储部分
245
随机数存储部分
249
参数存储部分
251
密钥存储部分
存储单元
241
235
叶密钥分配单元
237
参数分配单元
252
传递单元
253
传输部分
255
公钥传递部分

图 9

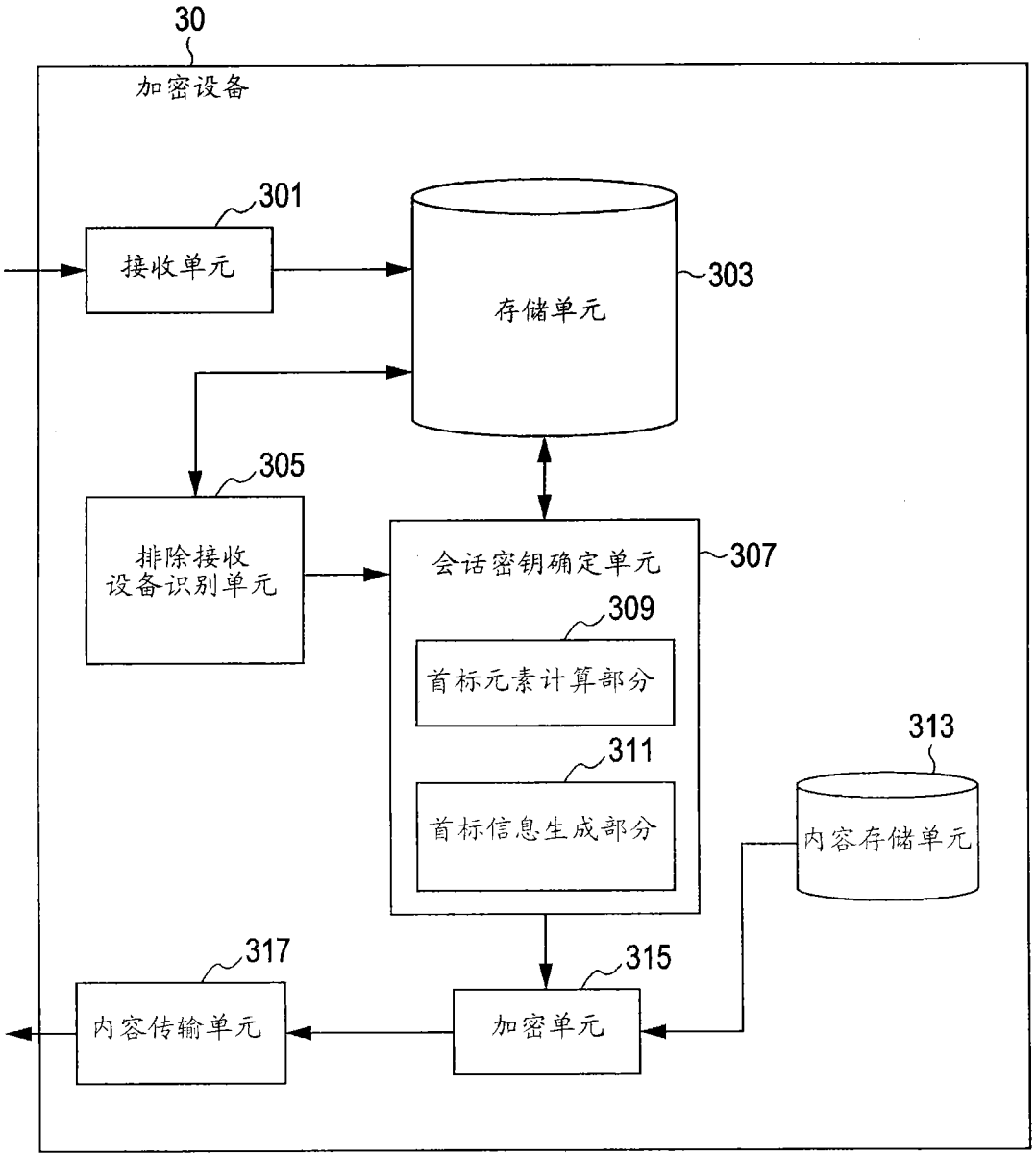

30
加密设备
301
接收单元
303
存储单元
305
排除接收
设备识别单元
307
会话密钥确定单元
309
首标元素计算部分
311
首标信息生成部分
313
内容存储单元
315
加密单元
317
内容传输单元

图 10

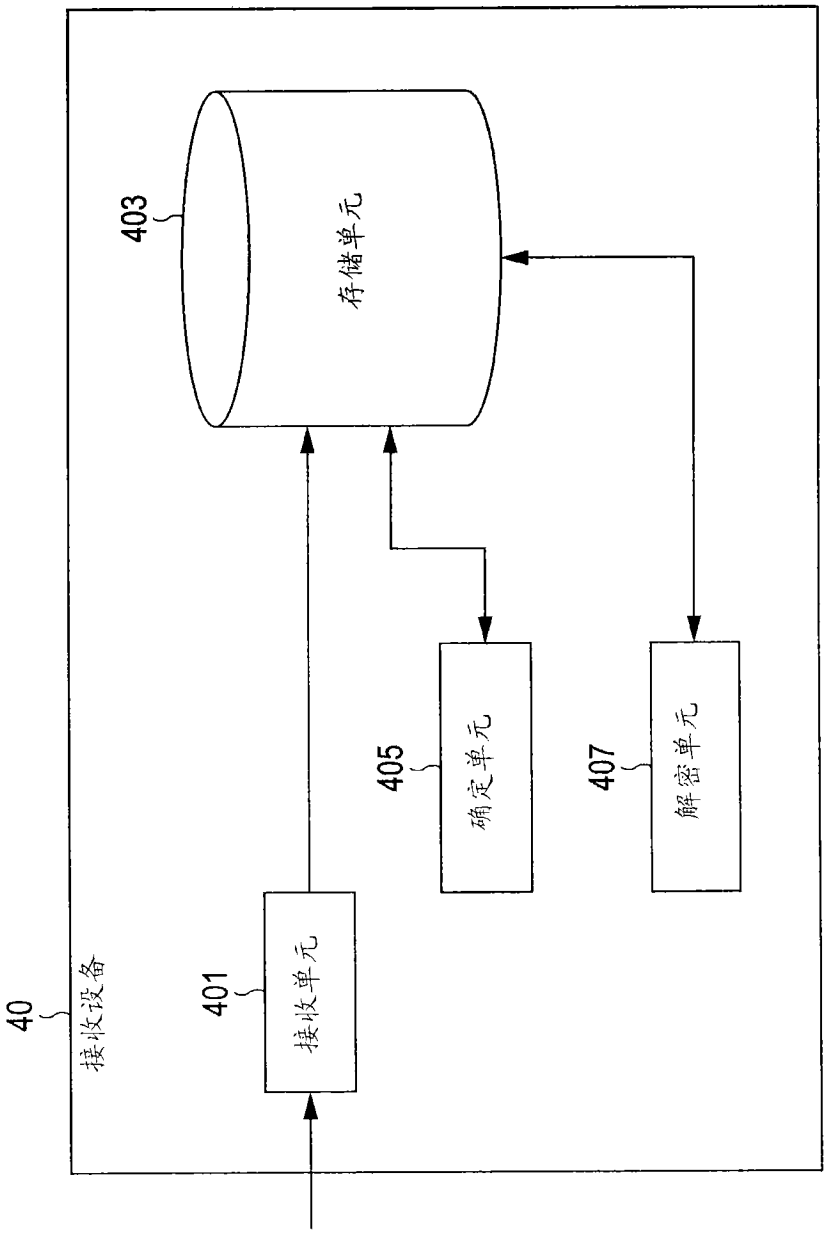


图 11

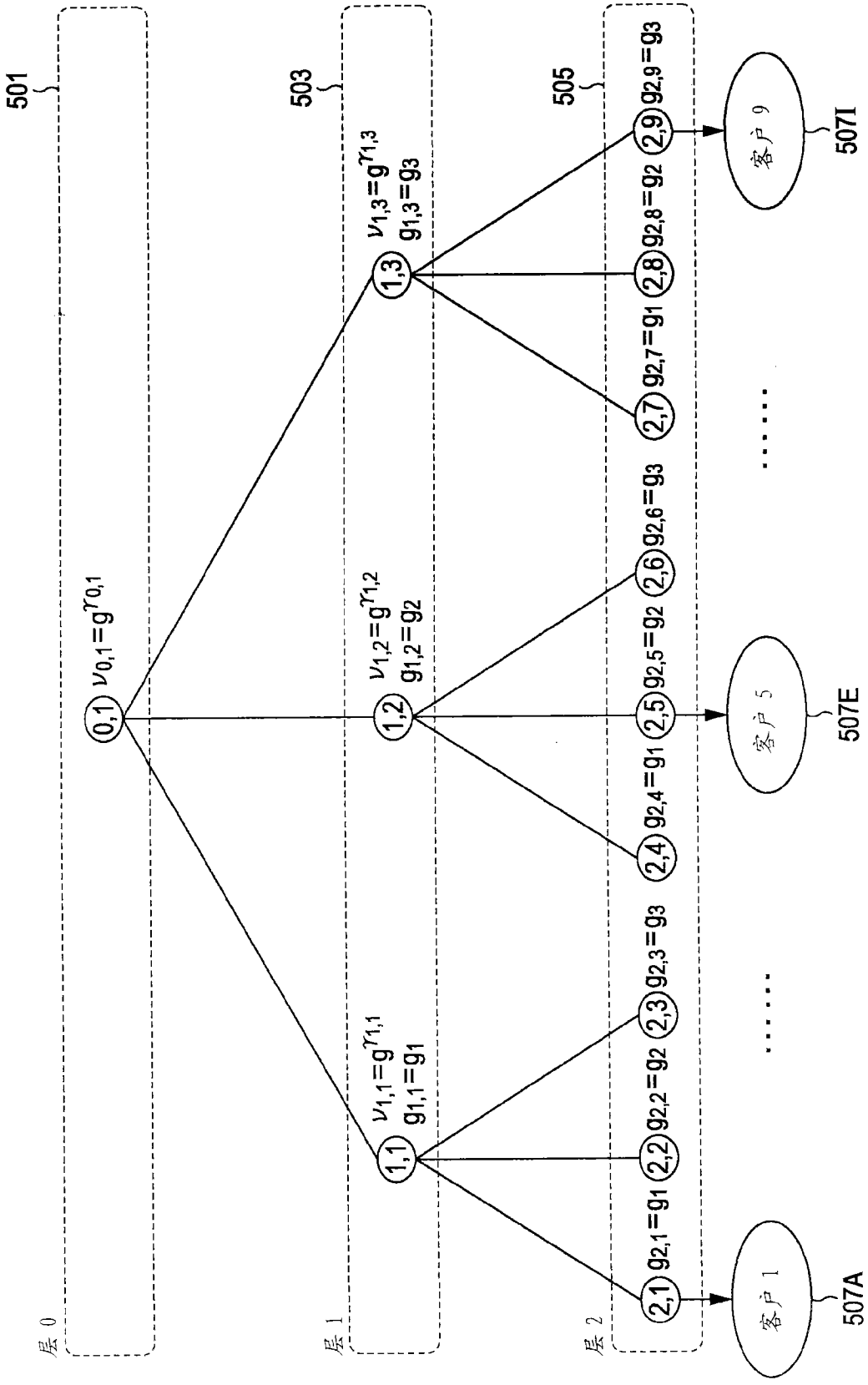

501
503
505
层 0
层 1
层 2
(0,1) $v_{0,1}=g^{\gamma_{0,1}}$
(1,1) $v_{1,1}=g^{\gamma_{1,1}}$ $g_{1,1}=g_1$
(1,2) $v_{1,2}=g^{\gamma_{1,2}}$ $g_{1,2}=g_2$
(1,3) $v_{1,3}=g^{\gamma_{1,3}}$ $g_{1,3}=g_3$
(2,1) $g_{2,1}=g_1$
(2,2) $g_{2,2}=g_2$
(2,3) $g_{2,3}=g_3$
(2,4) $g_{2,4}=g_1$
(2,5) $g_{2,5}=g_2$
(2,6) $g_{2,6}=g_3$
(2,7) $g_{2,7}=g_1$
(2,8) $g_{2,8}=g_2$
(2,9) $g_{2,9}=g_3$
客户 1
客户 5
客户 9
507A
507E
507I

图 12

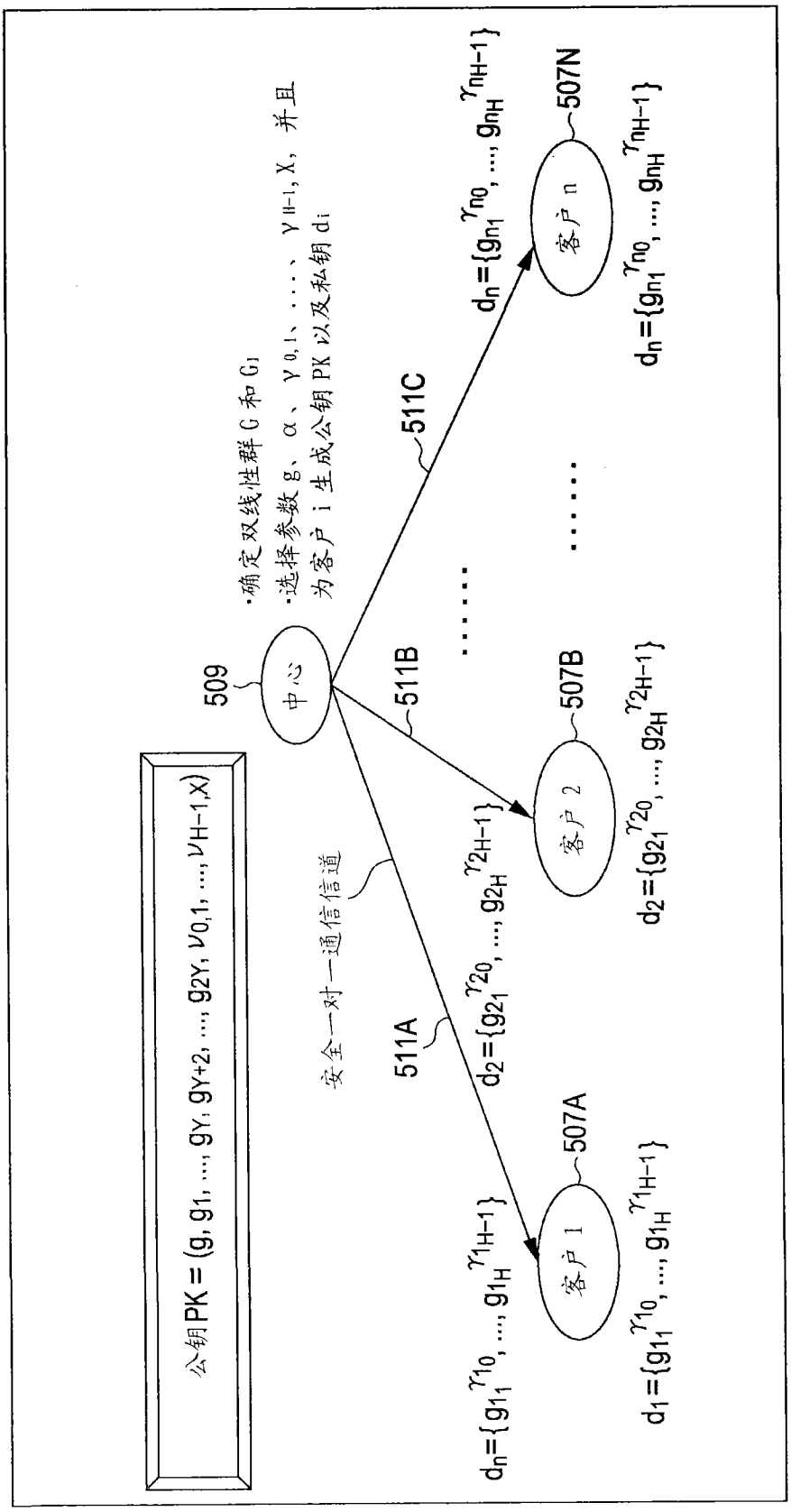

公钥PK = (g, g1, ..., gγ, gγ+2, ..., g2γ, ν0,1, ..., νH-1,X)
509
中心
·确定双线性群 G 和 G1
·选择参数 g、α、ν0,1、...、νH-1,X，并且为客户 i 生成公钥 PK 以及私钥 di
511A
511B
511C
安全一对一通信信道
客户 1
客户 2
客户 n
507A
507B
507N
dn={g1r10, ..., g1Hr1H-1}
d2={g21r20, ..., g2Hr2H-1}
dn={gn1rn0, ..., gnHrnH-1}
d1={g11r10, ..., g1Hr1H-1}
d2={g21r20, ..., g2Hr2H-1}
dn={gn1rn0, ..., gnHrnH-1}

图 13

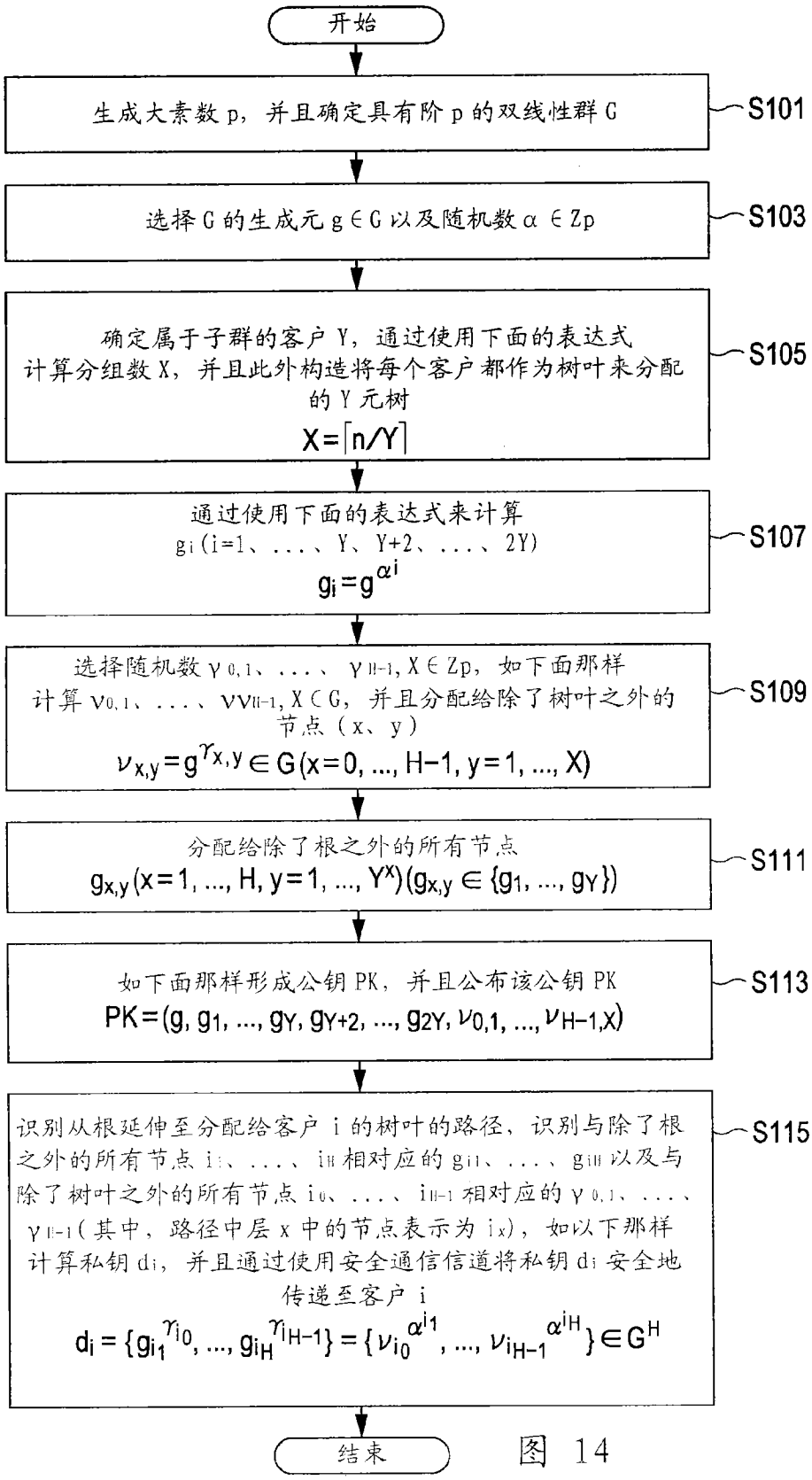

开始
生成大素数 p，并且确定具有阶 p 的双线性群 G
S101
选择 G 的生成元 g ∈ G 以及随机数 α ∈ Zp
S103
确定属于子群的客户 Y，通过使用下面的表达式计算分组数 X，并且此外构造将每个客户都作为树叶来分配的 Y 元树
X=⌈n/Y⌉
S105
通过使用下面的表达式来计算 gi (i=1、...、Y、Y+2、...、2Y)
gi=g^αi
S107
选择随机数 γ0,1、...、γH-1,X ∈ Zp，如下面那样计算 v0,1、...、vvH-1,X ∈ G，并且分配给除了树叶之外的节点（x、y）
vx,y=g^γx,y ∈ G(x=0, ..., H-1, y=1, ..., X)
S109
分配给除了根之外的所有节点
gx,y(x=1, ..., H, y=1, ..., Yx)(gx,y ∈ {g1, ..., gY})
S111
如下面那样形成公钥 PK，并且公布该公钥 PK
PK=(g, g1, ..., gY, gY+2, ..., g2Y, v0,1, ..., vH-1,X)
S113
识别从根延伸至分配给客户 i 的树叶的路径，识别与除了根之外的所有节点 i1、...、iH 相对应的 gi1、...、giH 以及与除了树叶之外的所有节点 i0、...、iH-1 相对应的 γ0,1、...、γH-1（其中，路径中层 x 中的节点表示为 ix），如以下那样计算私钥 di，并且通过使用安全通信信道将私钥 di 安全地传递至客户 i
di = {gi1^γi0, ..., giH^γiH-1} = {vi0^αi1, ..., viH-1^αiH} ∈ G^H
S115
结束

图 14

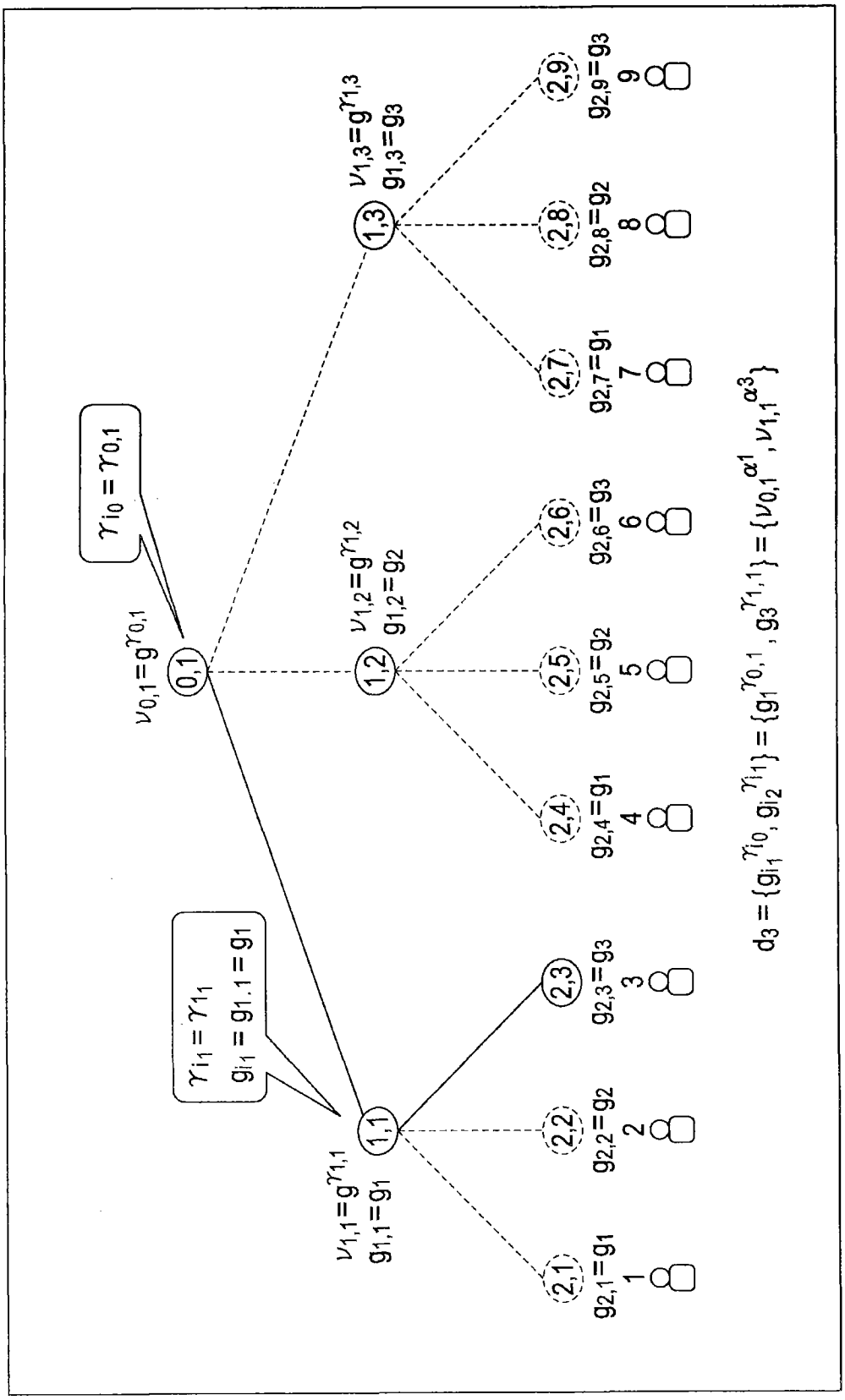

$\gamma_{i_0} = \gamma_{0,1}$
$\nu_{0,1}=g^{\gamma_{0,1}}$
(0,1)
$\gamma_{i_1} = \gamma_{1,1}$
$g_{i_1} = g_{1.1} = g_1$
$\nu_{1,1}=g^{\gamma_{1,1}}$
$g_{1,1}=g_1$
(1,1)
$\nu_{1,2}=g^{\gamma_{1,2}}$
$g_{1,2}=g_2$
(1,2)
$\nu_{1,3}=g^{\gamma_{1,3}}$
$g_{1,3}=g_3$
(1,3)
(2,1) $g_{2,1}=g_1$ 1
(2,2) $g_{2,2}=g_2$ 2
(2,3) $g_{2,3}=g_3$ 3
(2,4) $g_{2,4}=g_1$ 4
(2,5) $g_{2,5}=g_2$ 5
(2,6) $g_{2,6}=g_3$ 6
(2,7) $g_{2,7}=g_1$ 7
(2,8) $g_{2,8}=g_2$ 8
(2,9) $g_{2,9}=g_3$ 9
$d_3 = \{g_{i_1}{}^{\gamma_{i_0}}, g_{i_2}{}^{\gamma_{i_1}}\} = \{g_1{}^{\gamma_{0,1}}, g_3{}^{\gamma_{1,1}}\} = \{\nu_{0,1}{}^{\alpha^1}, \nu_{1,1}{}^{\alpha^3}\}$

图 15

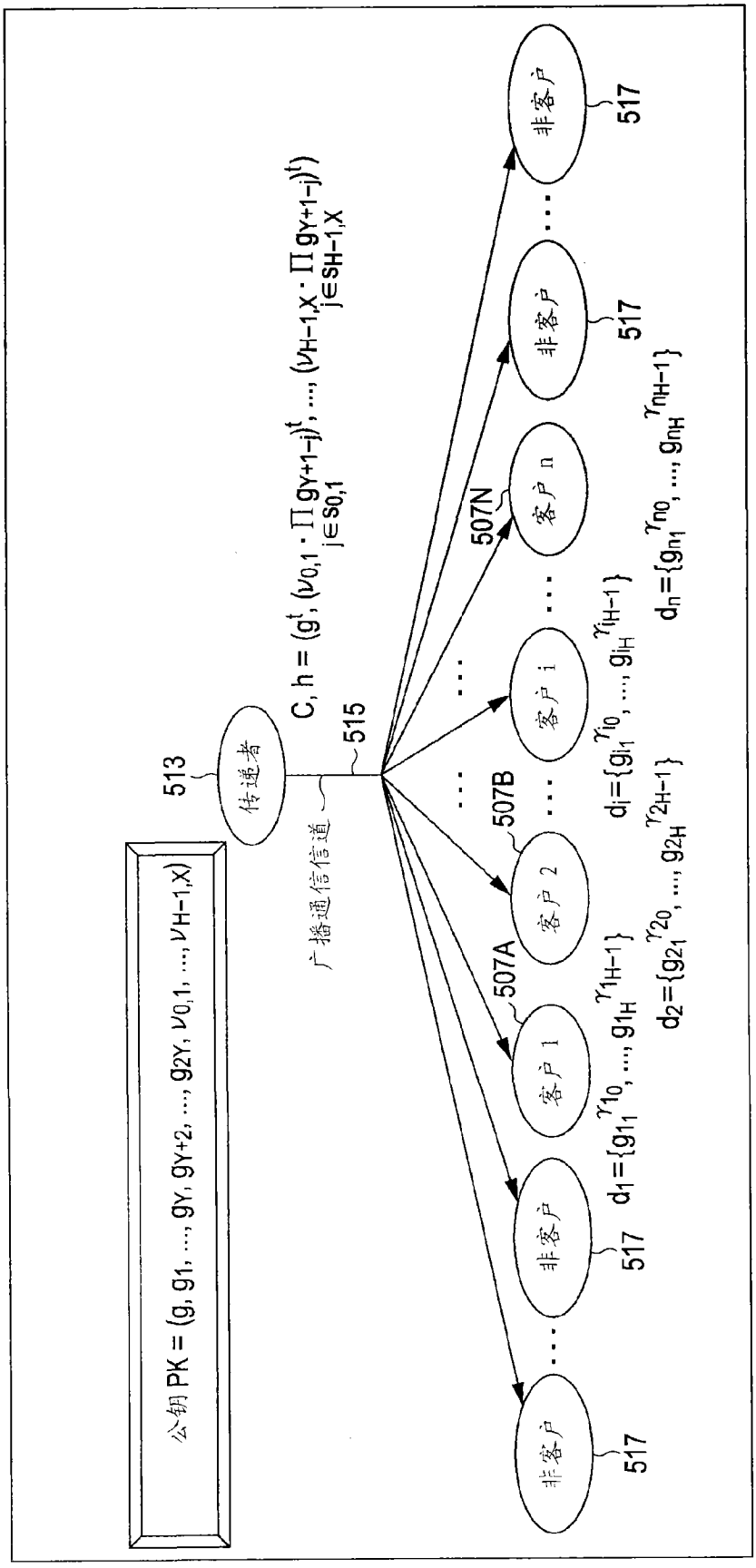

公钥 PK = (g, g1, ..., gY, gY+2, ..., g2Y, v0,1, ..., vH-1,X)
513
传送者
广播通信信道
C, h = (g^t, (v0,1 · ∏ gY+1-j)^t, ..., (vH-1,X · ∏ gY+1-j)^t)
j∈S0,1
j∈SH-1,X
515
507A
507B
507N
客户 1
客户 2
客户 i
客户 n
非客户
517
d1={g11^γ10, ..., g1H^γ1H-1}
d2={g21^γ20, ..., g2H^γ2H-1}
di={gi1^γi0, ..., giH^γiH-1}
dn={gn1^γn0, ..., gnH^γnH-1}

图 16

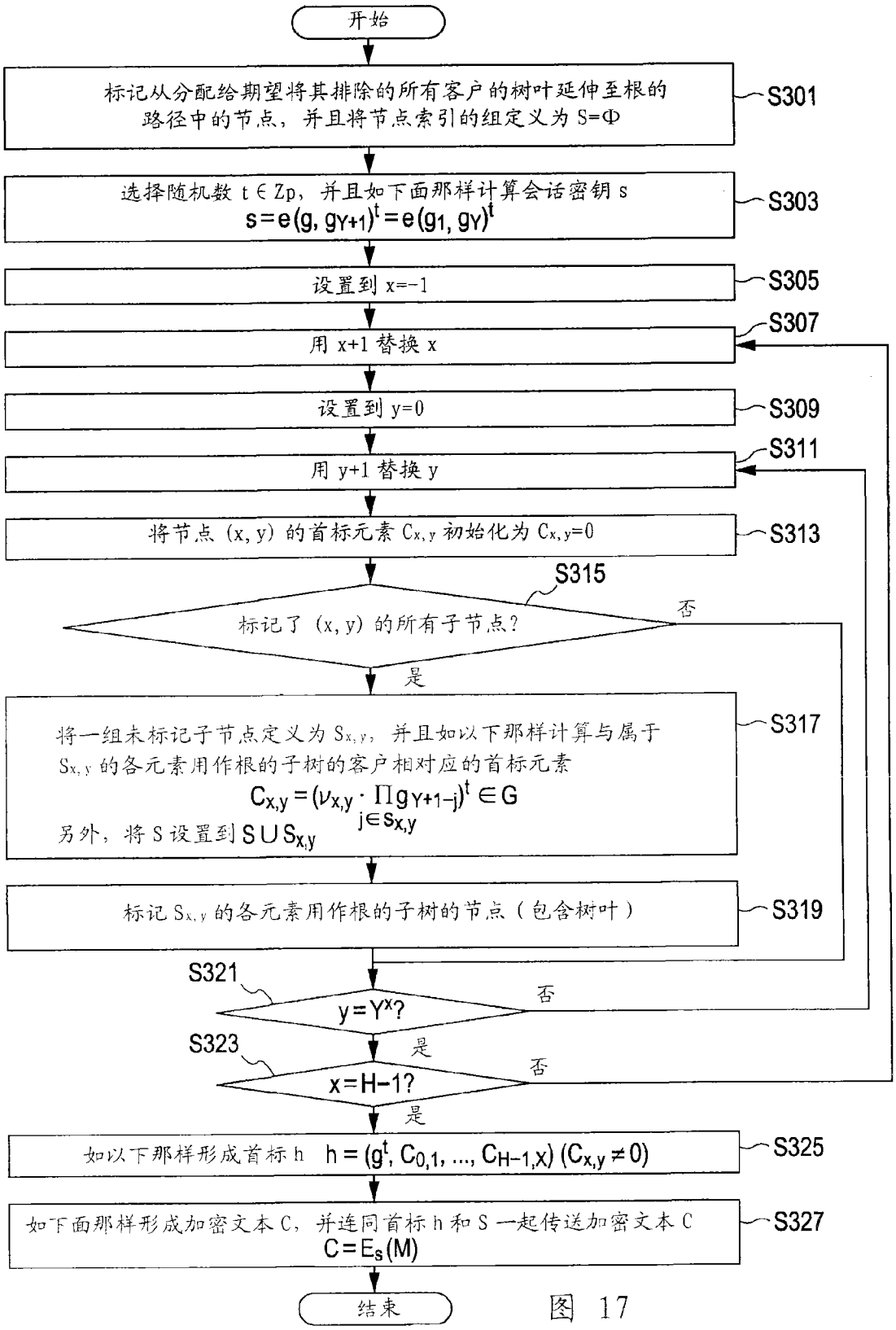

开始
标记从分配给期望将其排除的所有客户的树叶延伸至根的路径中的节点，并且将节点索引的组定义为 S=Φ
S301
选择随机数 t ∈ Zp，并且如下面那样计算会话密钥 s
$s=e(g, g_{Y+1})^t=e(g_1, g_Y)^t$
S303
设置到 x=-1
S305
用 x+1 替换 x
S307
设置到 y=0
S309
用 y+1 替换 y
S311
将节点 (x, y) 的首标元素 $C_{x,y}$ 初始化为 $C_{x,y}=0$
S313
S315
标记了 (x, y) 的所有子节点？
否
是
将一组未标记子节点定义为 $S_{x,y}$，并且如以下那样计算与属于 $S_{x,y}$ 的各元素用作根的子树的客户相对应的首标元素
$C_{x,y}=(\nu_{x,y}\cdot\prod_{j\in S_{x,y}} g_{Y+1-j})^t \in G$
另外，将 S 设置到 $S \cup S_{x,y}$
S317
标记 $S_{x,y}$ 的各元素用作根的子树的节点（包含树叶）
S319
S321
$y=Y^x$?
否
是
S323
x=H-1?
否
是
如以下那样形成首标 h $h=(g^t, C_{0,1}, \ldots, C_{H-1,X})\ (C_{x,y}\neq 0)$
S325
如下面那样形成加密文本 C，并连同首标 h 和 S 一起传送加密文本 C
$C=E_S(M)$
S327
结束

图 17

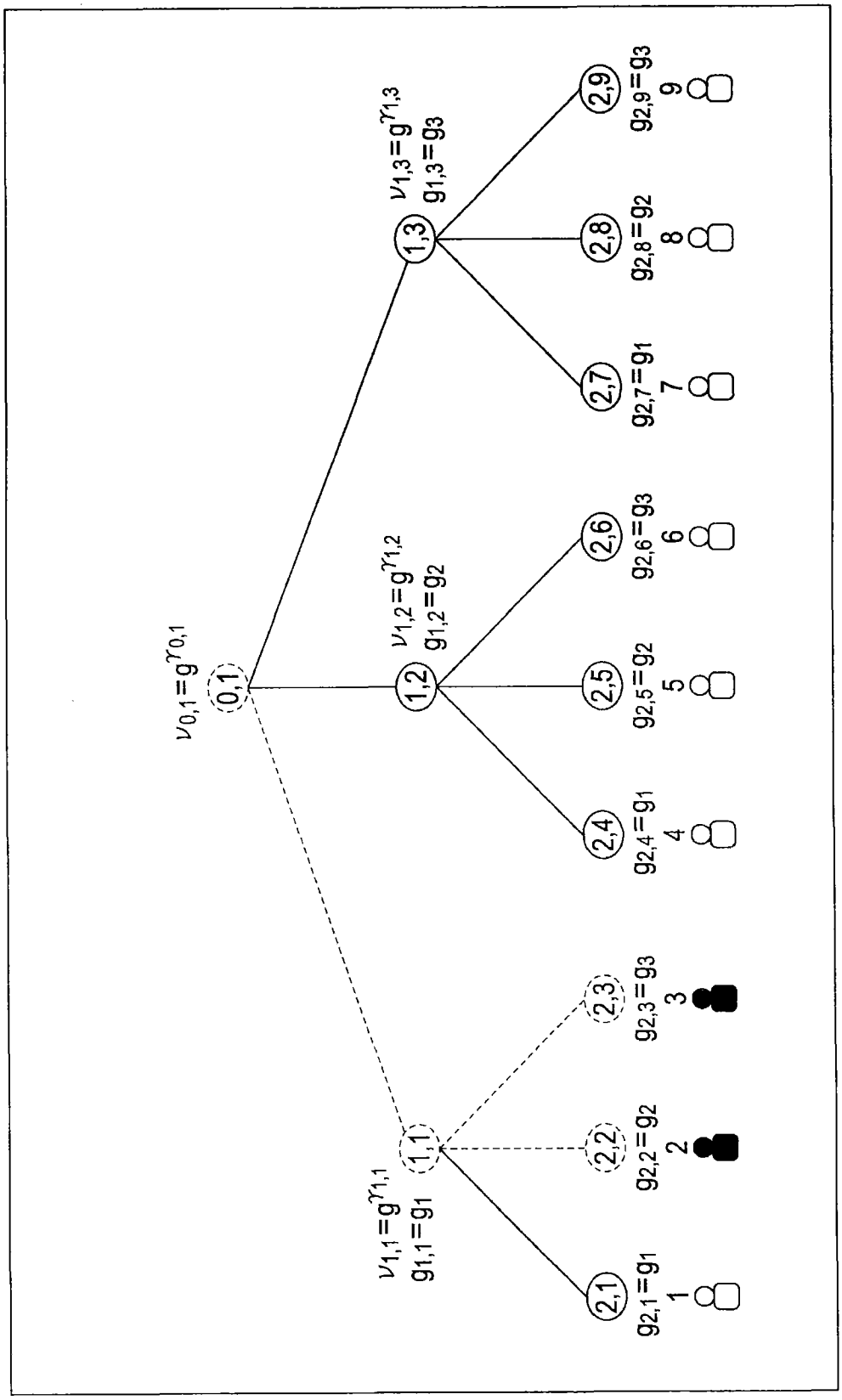

$v_{0,1}=g^{\gamma_{0,1}}$
(0,1)
$v_{1,1}=g^{\gamma_{1,1}}$
$g_{1,1}=g_1$
(1,1)
$v_{1,2}=g^{\gamma_{1,2}}$
$g_{1,2}=g_2$
(1,2)
$v_{1,3}=g^{\gamma_{1,3}}$
$g_{1,3}=g_3$
(1,3)
(2,1) $g_{2,1}=g_1$ 1
(2,2) $g_{2,2}=g_2$ 2
(2,3) $g_{2,3}=g_3$ 3
(2,4) $g_{2,4}=g_1$ 4
(2,5) $g_{2,5}=g_2$ 5
(2,6) $g_{2,6}=g_3$ 6
(2,7) $g_{2,7}=g_1$ 7
(2,8) $g_{2,8}=g_2$ 8
(2,9) $g_{2,9}=g_3$ 9

图 18

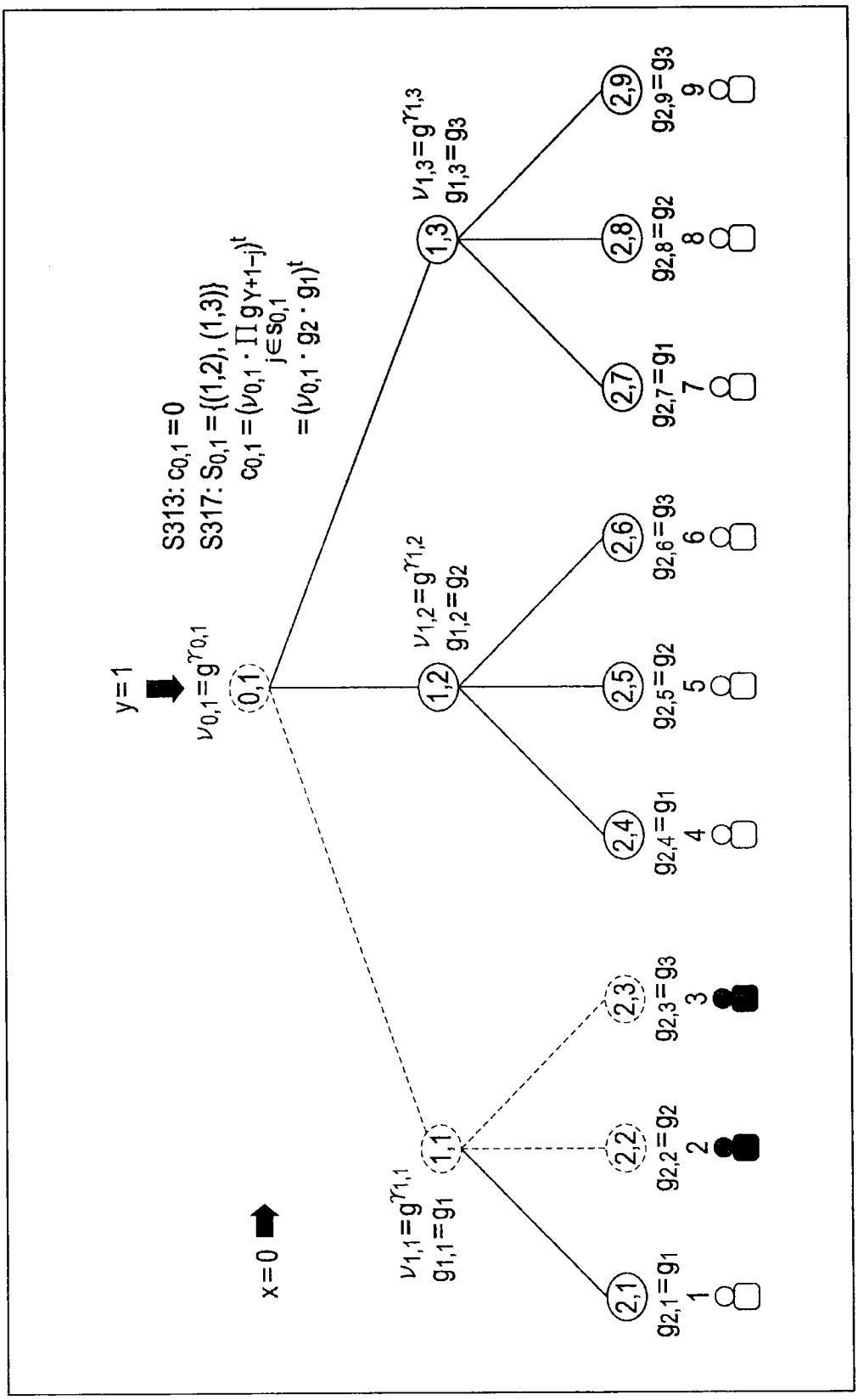

y=1
$v_{0,1}=g^{\gamma_{0,1}}$
(0,1)
S313: $c_{0,1}=0$
S317: $S_{0,1}=\{(1,2),(1,3)\}$
$c_{0,1}=(v_{0,1}\cdot\prod_{j\in S_{0,1}} g_{Y+1-j})^t$
$=(v_{0,1}\cdot g_2\cdot g_1)^t$
x=0
(1,1) $v_{1,1}=g^{\gamma_{1,1}}$ $g_{1,1}=g_1$
(1,2) $v_{1,2}=g^{\gamma_{1,2}}$ $g_{1,2}=g_2$
(1,3) $v_{1,3}=g^{\gamma_{1,3}}$ $g_{1,3}=g_3$
(2,1) $g_{2,1}=g_1$ 1
(2,2) $g_{2,2}=g_2$ 2
(2,3) $g_{2,3}=g_3$ 3
(2,4) $g_{2,4}=g_1$ 4
(2,5) $g_{2,5}=g_2$ 5
(2,6) $g_{2,6}=g_3$ 6
(2,7) $g_{2,7}=g_1$ 7
(2,8) $g_{2,8}=g_2$ 8
(2,9) $g_{2,9}=g_3$ 9

图 19

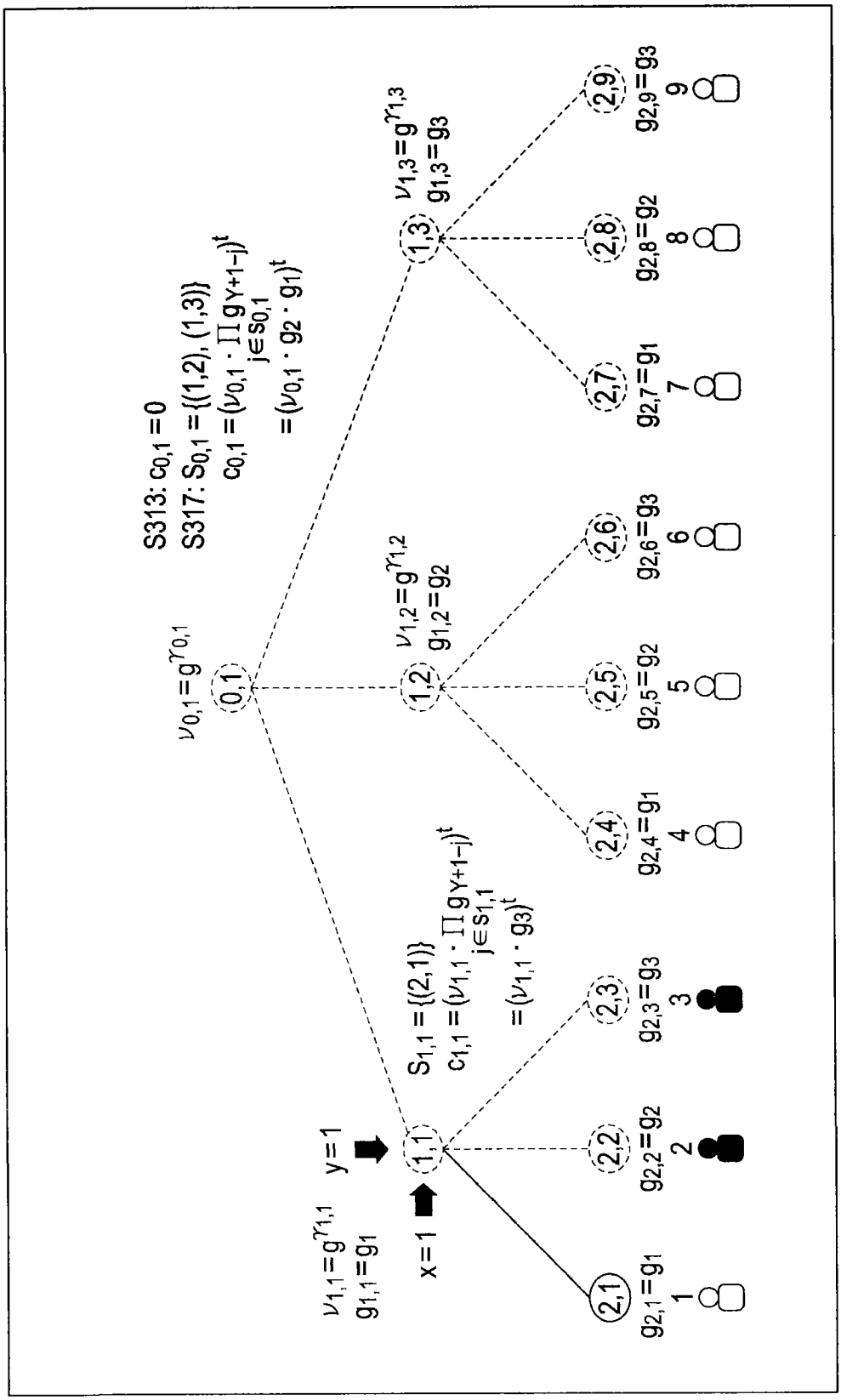

S313: $c_{0,1}=0$
S317: $S_{0,1}=\{(1,2),(1,3)\}$
$c_{0,1}=(\nu_{0,1}\cdot\prod_{j\in s_{0,1}} g_{\gamma+1-j})^t$
$=(\nu_{0,1}\cdot g_2\cdot g_1)^t$
$\nu_{0,1}=g^{\gamma_{0,1}}$
$\nu_{1,1}=g^{\gamma_{1,1}}$
$g_{1,1}=g_1$
x=1
y=1
$S_{1,1}=\{(2,1)\}$
$c_{1,1}=(\nu_{1,1}\cdot\prod_{j\in s_{1,1}} g_{\gamma+1-j})^t$
$=(\nu_{1,1}\cdot g_3)^t$
$\nu_{1,2}=g^{\gamma_{1,2}}$
$g_{1,2}=g_2$
$\nu_{1,3}=g^{\gamma_{1,3}}$
$g_{1,3}=g_3$
(0,1)
(1,1)
(1,2)
(1,3)
(2,1) $g_{2,1}=g_1$ 1
(2,2) $g_{2,2}=g_2$ 2
(2,3) $g_{2,3}=g_3$ 3
(2,4) $g_{2,4}=g_1$ 4
(2,5) $g_{2,5}=g_2$ 5
(2,6) $g_{2,6}=g_3$ 6
(2,7) $g_{2,7}=g_1$ 7
(2,8) $g_{2,8}=g_2$ 8
(2,9) $g_{2,9}=g_3$ 9

图 20

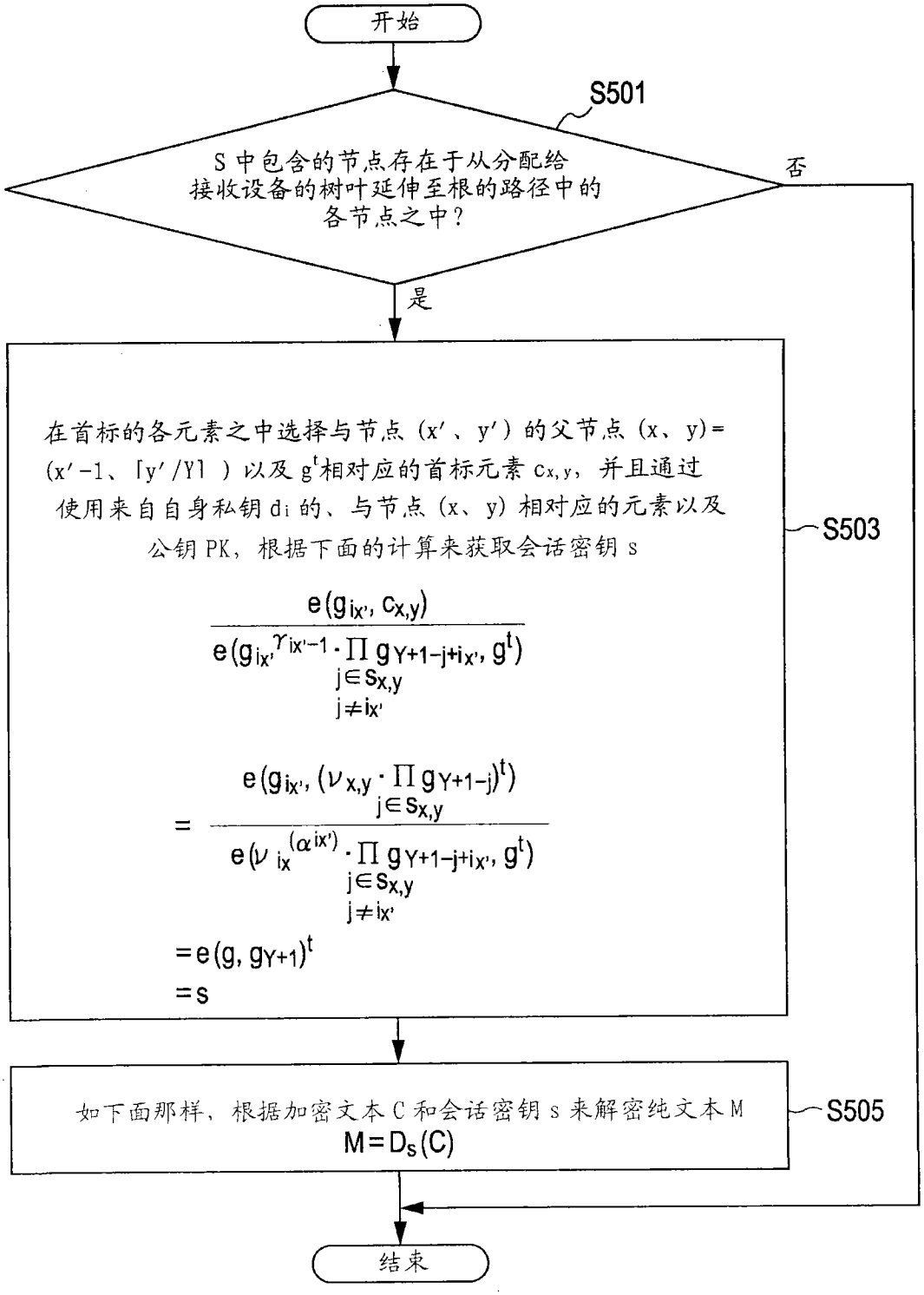

开始
S501
S 中包含的节点存在于从分配给接收设备的树叶延伸至根的路径中的各节点之中？
否
是
在首标的各元素之中选择与节点（x′、y′）的父节点（x、y）=（x′-1、⌈y′/Y⌉）以及 g^t 相对应的首标元素 $c_{x,y}$，并且通过使用来自自身私钥 d_i 的、与节点（x、y）相对应的元素以及公钥 PK，根据下面的计算来获取会话密钥 s
$$\frac{e(g_{ix'}, c_{x,y})}{e(g_{ix'}^{\gamma_{ix'-1}} \cdot \prod_{\substack{j \in S_{x,y} \\ j \neq ix'}} g_{Y+1-j+ix'}, g^t)}$$
$$= \frac{e(g_{ix'}, (\nu_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t)}{e(\nu_{ix}^{(\alpha ix')} \cdot \prod_{\substack{j \in S_{x,y} \\ j \neq ix'}} g_{Y+1-j+ix'}, g^t)}$$
$$= e(g, g_{Y+1})^t$$
$$= s$$
S503
如下面那样，根据加密文本 C 和会话密钥 s 来解密纯文本 M
$M = D_s(C)$
S505
结束

图 21

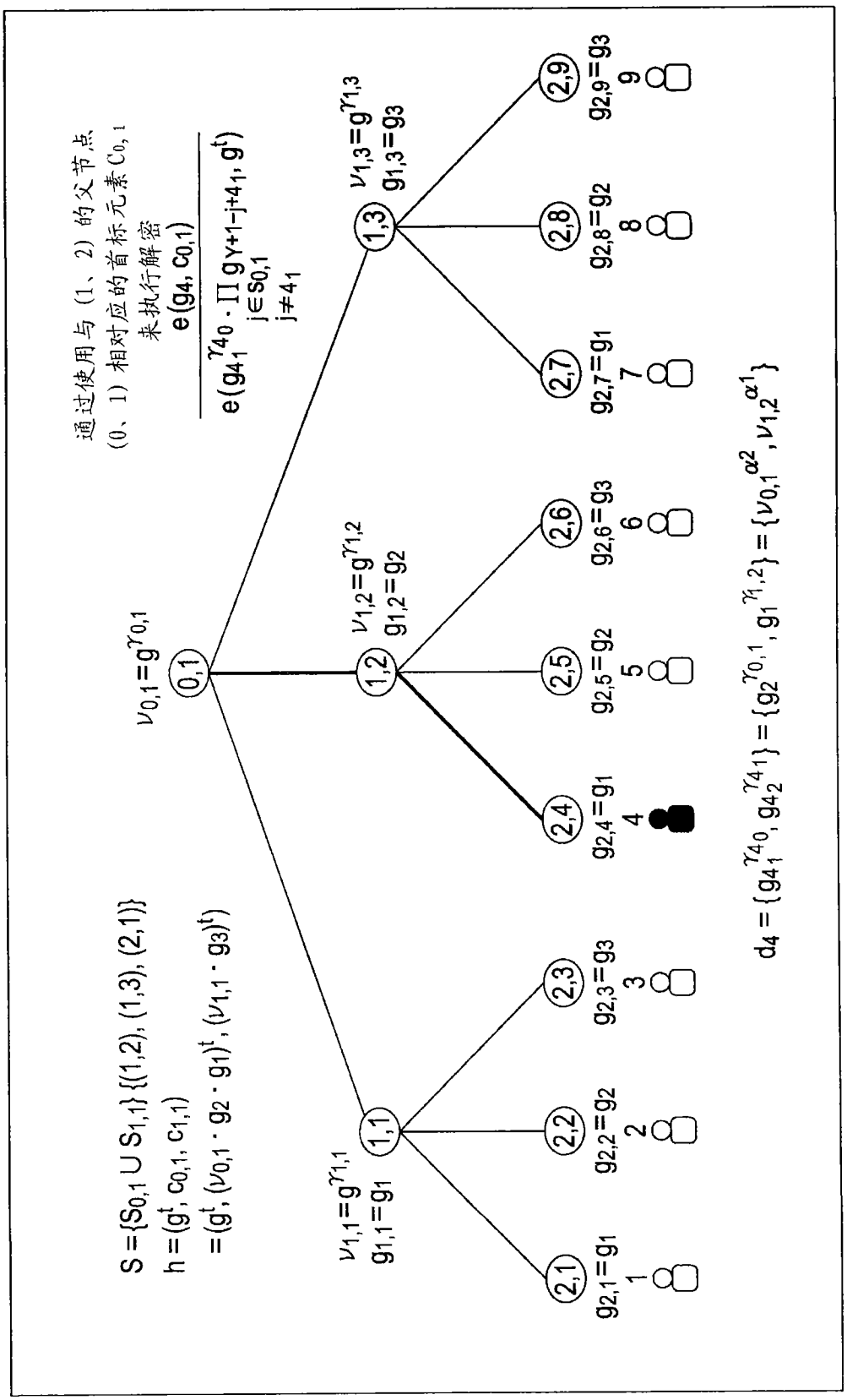

通过使用与（1、2）的父节点
(0、1) 相对应的首标元素 $c_{0,1}$
来执行解密
$e(g_4, c_{0,1})$
$e(g_4{}^{\gamma_{4_0}} \cdot \prod_{j \in s_{0,1}, j \neq 4_1} g_{Y+1-j+4_1}, g^t)$
$S = \{S_{0,1} \cup S_{1,1}\}\ \{(1,2), (1,3), (2,1)\}$
$h = (g^t, c_{0,1}, c_{1,1})$
$= (g^t, (v_{0,1} \cdot g_2 \cdot g_1)^t, (v_{1,1} \cdot g_3)^t)$
$v_{0,1} = g^{\gamma_{0,1}}$
$v_{1,1} = g^{\gamma_{1,1}}$
$g_{1,1} = g_1$
$v_{1,2} = g^{\gamma_{1,2}}$
$g_{1,2} = g_2$
$v_{1,3} = g^{\gamma_{1,3}}$
$g_{1,3} = g_3$
$g_{2,1} = g_1$
$g_{2,2} = g_2$
$g_{2,3} = g_3$
$g_{2,4} = g_1$
$g_{2,5} = g_2$
$g_{2,6} = g_3$
$g_{2,7} = g_1$
$g_{2,8} = g_2$
$g_{2,9} = g_3$
$d_4 = \{g_4{}^{\gamma_{4_0}}, g_{4_2}{}^{\gamma_{4_1}}\} = \{g_2{}^{\gamma_{0,1}}, g_1{}^{\gamma_{1,2}}\} = \{v_{0,1}{}^{\alpha^2}, v_{1,2}{}^{\alpha^1}\}$

图 22

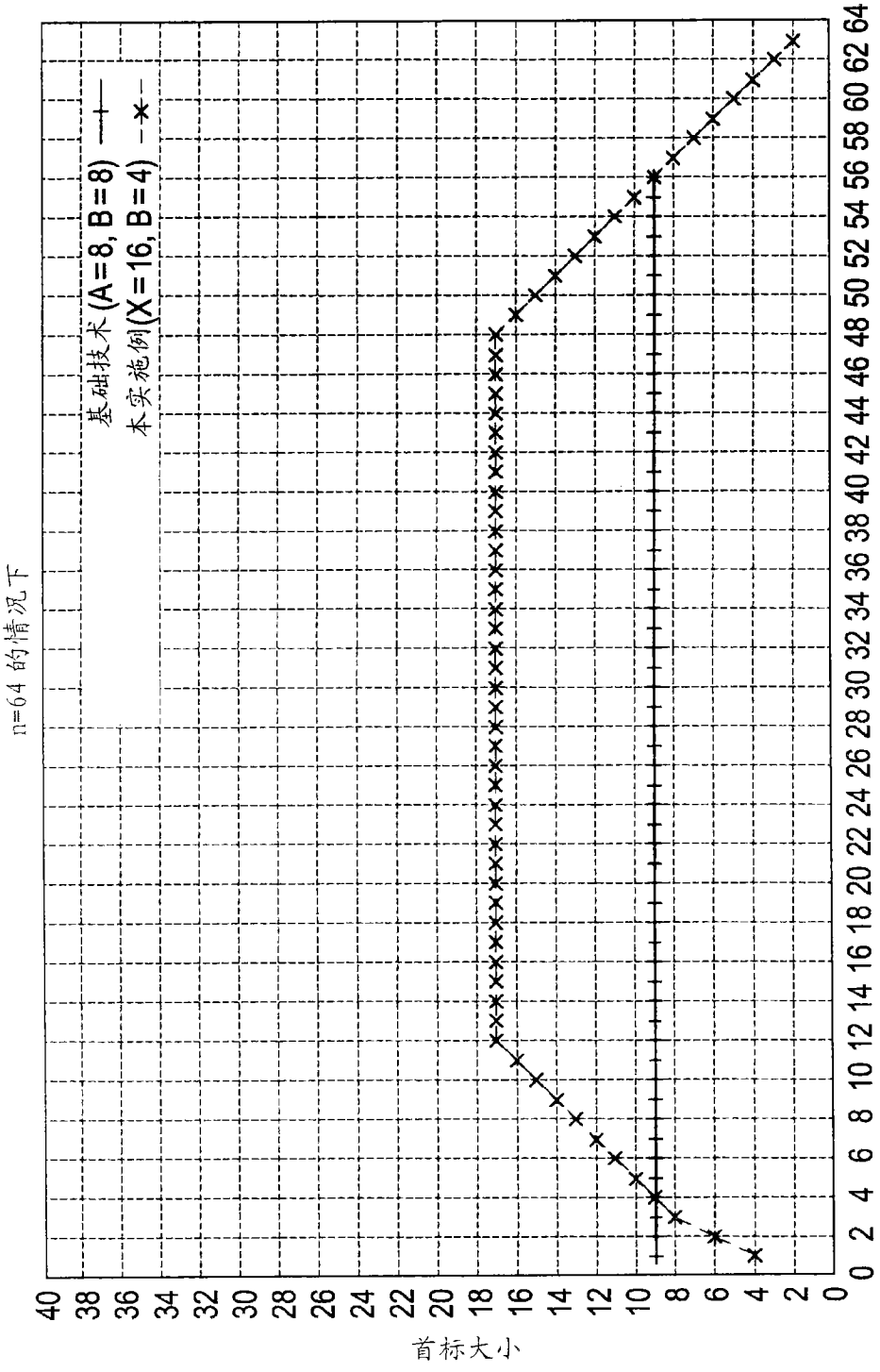

n=64 的情况下
基础技术 (A=8, B=8)
本实施例(X=16, B=4)
首标大小
r: 排除客户的数量
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40

图 23

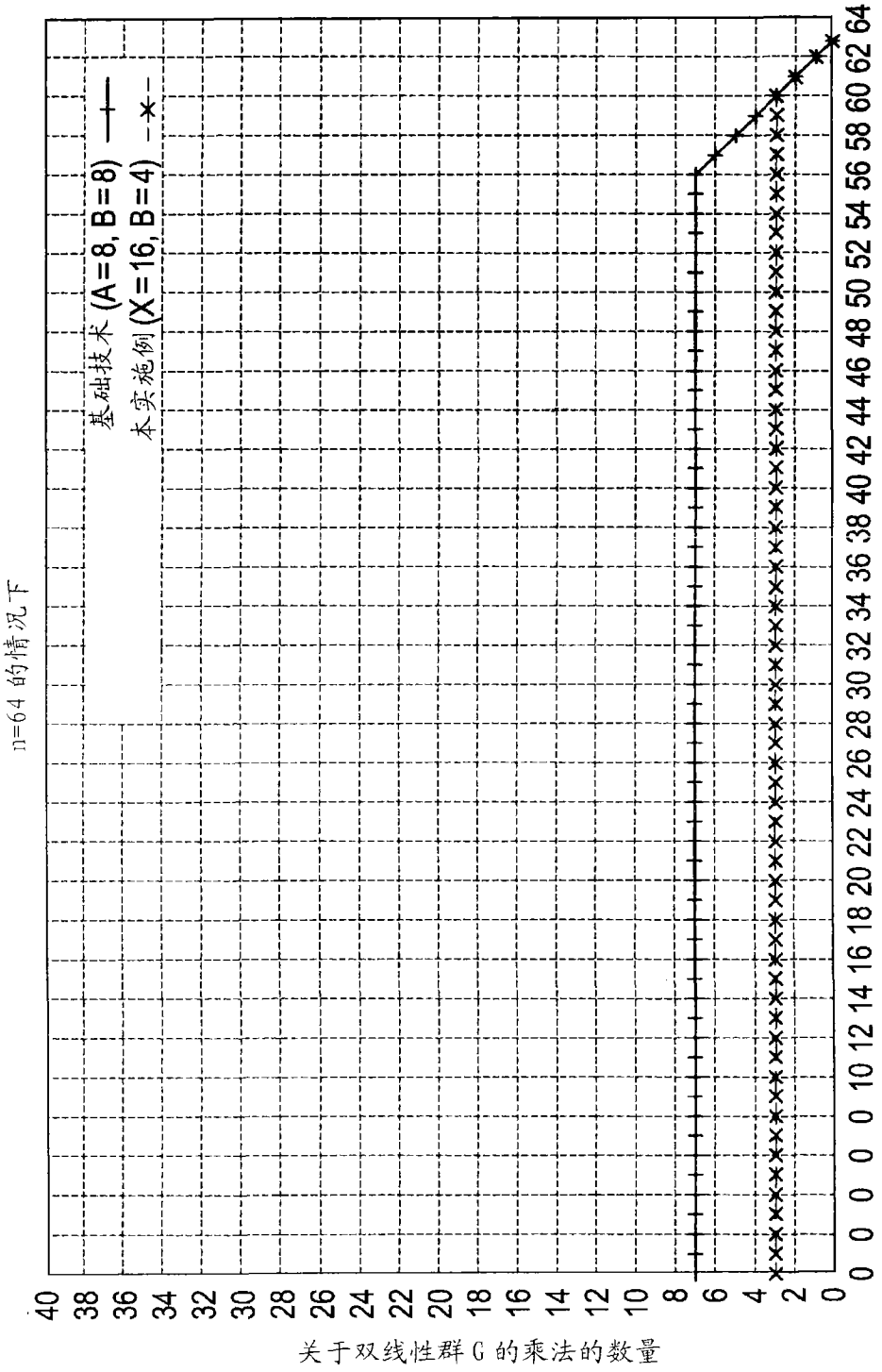


图 24

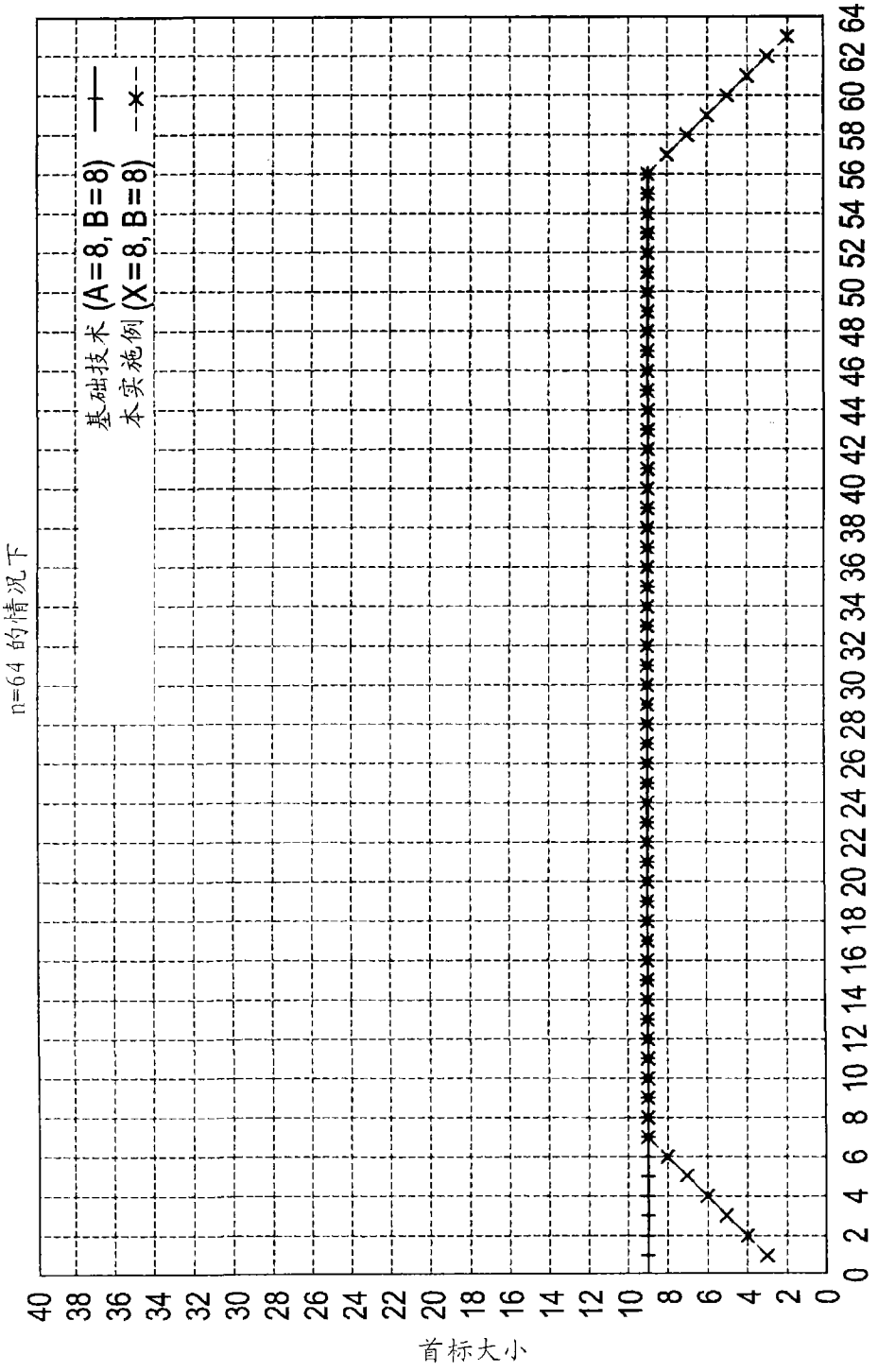

n=64 的情况下
基础技术 (A=8, B=8)
本实施例 (X=8, B=8)
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64
40 38 36 34 32 30 28 26 24 22 20 18 16 14 12 10 8 6 4 2 0
r: 排除客户的数量
首标大小

图 25

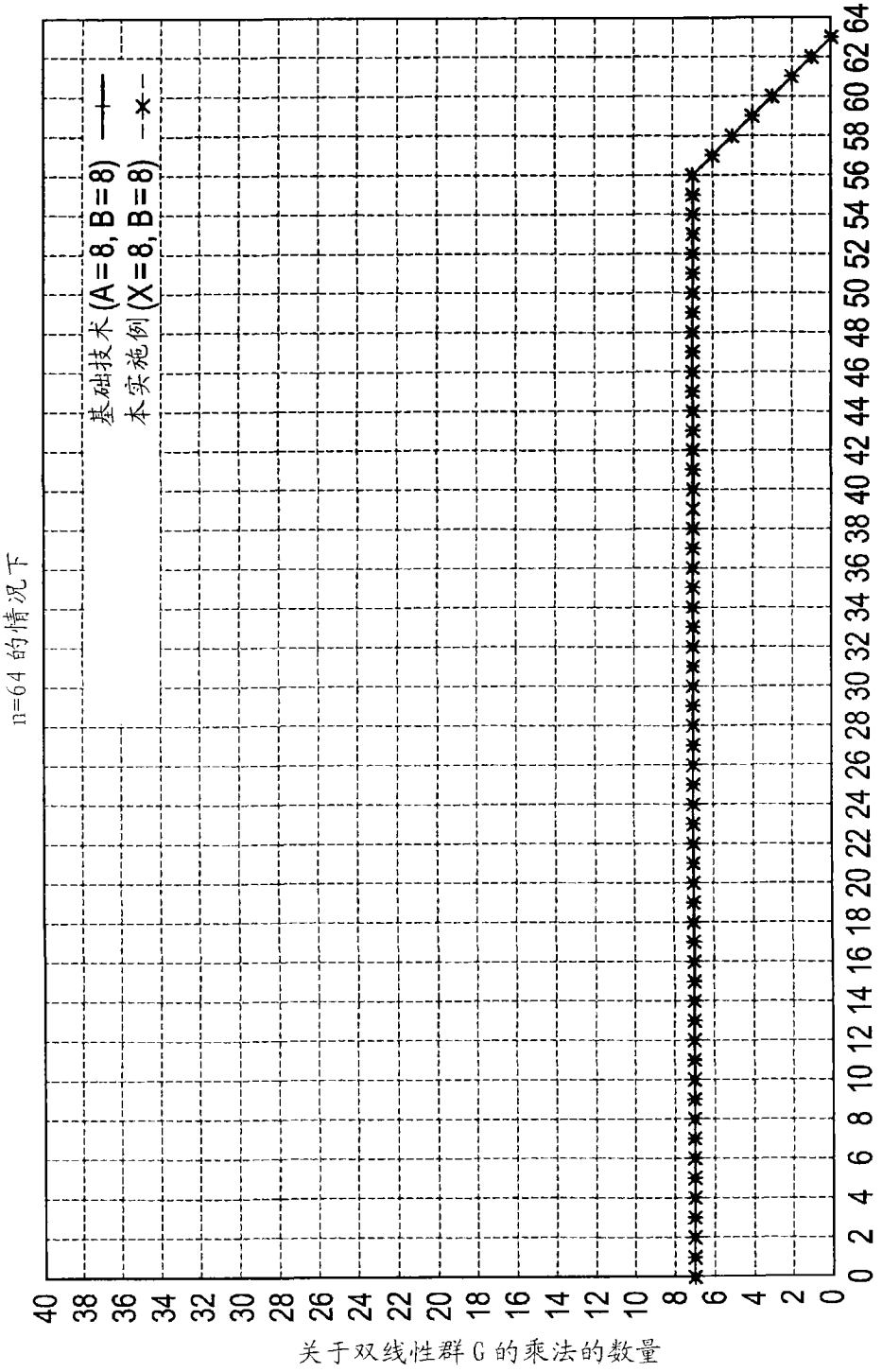

n=64 的情况下
基础技术 (A=8, B=8)
本实施例 (X=8, B=8)
关于双线性群 G 的乘法的数量
r: 排除客户的数量
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40

图 26