(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 101689993 B
(45)授权公告日 2013.02.27

(21)申请号 200780053725.5
(22)申请日 2007.07.11
(85)PCT申请进入国家阶段日
2010.01.11
(86)PCT申请的申请数据
PCT/JP2007/063824 2007.07.11
(87)PCT申请的公布数据
WO2009/008069 JA 2009.01.15
(73)专利权人 株式会社东芝
地址 日本东京都
专利权人 东芝解决方案株式会社
(72)发明人 吉田琢也 冈田光司
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 许海兰
(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 1864386 A,2006.11.15,
JP 2005210638 A,2005.08.04,
审查员 李俊洁

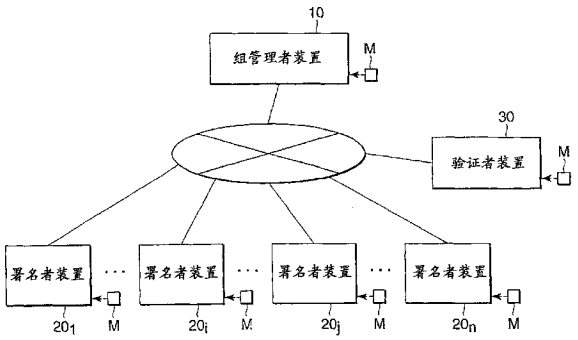
权利要求书 5 页 说明书 18 页 附图 12 页

(54)发明名称

组署名系统、装置和方法

(57)摘要

本发明的一个实施例的组署名系统具备能够相互进行通信的组管理者装置(10)、署名者装置(20_1～20_n)和验证者装置(30)。在此,各装置(10、20_1～20_n、30)所使用的组署名方式是完全不使用RSA那样位数未知的乘法巡回群而只使用素数位数(q)的乘法巡回群(G)的方式,并且将继承(k_{i1}、k_{i2})作为成员秘密密钥。利用$T_i=g_1\hat{}\{k_{i1}\}$作为用于确定署名者的信息。因此,与现有的[CG04]方式相比,能够减少计算量而提高计算速度。



CN 101689993 B

1. 一种组署名系统，其特征在于包括：能够相互进行通信的组管理者装置 (10)、署名者装置 (20i) 和验证者装置 (30)，各装置使用组署名方式，

上述组管理者装置具备：

管理者用存储部件 (11)，存储包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数；

组密钥生成部件 (14)，根据上述管理者用存储部件内的公开参数，生成包含值 a，b $\in Z_q$ 的组秘密密钥、包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2，f 和上述生成元 g_1 的组公开密钥；以及

成员秘密密钥生成部件 (15)，根据上述组秘密密钥、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$，计算出由满足第四关系式 $f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$ 的继承 k_{i1}、k_{i2} 构成的成员秘密密钥，并根据上述成员秘密密钥和上述生成元 g_1，计算出署名者确定信息 $T_i = g_1\hat{}\{k_{i1}\}$，

上述署名者装置具备：

署名者用存储部件 (21)，存储包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、上述组公开密钥、上述成员秘密密钥、上述署名者确定信息 T_i 和消息；

组署名生成部件 (25)，根据上述署名者用存储部件内的公开参数和组公开密钥，对上述署名者确定信息 T_i 进行加密，生成该署名者确定信息 T_i 的密码数据，并根据上述署名者用存储部件内的公开参数、上述组公开密钥、上述成员秘密密钥和上述消息、上述署名者确定信息 T_i 的密码数据，生成表示知道了该成员秘密密钥且基于该署名者确定信息 T_i 正确地生成了上述密码数据的零知识证明；以及

通信部件 (23)，将由上述密码数据和上述零知识证明构成的组署名和上述消息发送到上述验证者装置，

其中 ^ 是表示幂的记号，

上述验证者装置具备：

验证者用存储部件 (31)，存储包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、上述组公开密钥；

通信部件 (33)，从上述署名者装置接收上述组署名和消息；以及

署名验证部件 (34)，根据上述接收到的组署名和消息、上述验证者用存储部件内的公开参数和组公开密钥，对该组署名的正当性进行验证，

上述通信部件 (33) 将上述验证了的结果发送到上述署名者装置。

2. 一种组管理者装置 (10)，能够与使用组署名方式的署名者装置 (20_i) 和验证者装置 (30) 进行通信，其特征在于包括：

管理者用存储部件 (11)，存储包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数；

组密钥生成部件 (14)，根据上述管理者用存储部件内的公开参数，生成包含值 a，b $\in Z_q$ 的组秘密密钥、包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2，f 和上述生成元 g_1 的组公开密钥；

成员秘密密钥生成部件 (15)，根据上述组秘密密钥、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$，计算出由满足第四关系式 $f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$ 的继承 k_{i1}、k_{i2} 构成的成员

秘密密钥，根据上述成员秘密密钥和上述生成元 g_1，计算出署名者确定信息 $T_i = g_1 \hat{} \{k_{i1}\}$；以及

通信部件 (13)，将用于生成上述组署名方式中的组署名的上述公开参数、上述组公开密钥、上述成员秘密密钥和上述署名者确定信息 T_i 发送到上述署名者装置，将用于对上述组署名方式中的组署名进行验证的上述公开参数和上述组公开密钥发送到上述验证者装置，

其中 ^ 是表示幂的记号。

3. 根据权利要求 2 所述的组管理者装置，其特征在于：

上述管理者用存储部件 (11)，相互关联地存储上述署名者确定信息 T_i 和用户识别信息 ID(i)；

上述通信部件 (13) 从上述署名者装置接收组署名和消息，其中该组署名由针对上述署名者确定信息 $T_i = g_1 \hat{} \{k_{i1}\}$ 表示知道了上述成员秘密密钥并且基于上述署名者确定信息 T_i 正确地生成了密码数据的零知识证明、上述署名者确定信息 T_i 的密码数据构成；

上述组管理者装置还具备：

署名验证部件 (16)，根据上述接收到的组署名和消息、上述管理者用存储部件内的公开参数、上述生成的组秘密密钥和组公开密钥，对该组署名的正当性进行验证；以及

署名者确定部件 (17)，在上述验证的结果表示正当性时，根据上述组秘密密钥从上述密码数据计算署名者确定信息 T_i，从上述管理者用存储部件确定与所得到的署名者确定信息 T_i 对应的用户识别信息 ID(i)，

上述密码数据是由上述署名者装置根据上述公开参数和组公开密钥对上述署名者确定信息 T_i 进行了加密的数据，

上述零知识证明是由上述署名者装置根据上述公开参数、上述组公开密钥、上述成员秘密密钥和消息、上述署名者确定信息 T_i 的密码数据生成的数据。

4. 一种署名者装置 (20_i)，能够与使用组署名方式的组管理者装置 (10) 和验证者装置 (30) 进行通信，其特征在于包括：

通信部件 (23)，从上述组管理者装置接收包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、包含根据上述公开参数使得满足值 $a, b \in Z_q$、第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 那样地生成的值 g_2、f 和上述生成元 g_1 的组公开密钥、由根据上述 $a, b \in Z_q$、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$ 而使得满足第四关系式 $f = g_1 \hat{} \{k_{i1}\} g_2 \hat{} \{k_{i2}\}$ 那样地生成的继承 k_{i1}、k_{i2} 构成的成员秘密密钥、根据上述成员秘密密钥和上述生成元 g_1 生成的署名者确定信息 $T_i = g_1 \hat{} \{k_{i1}\}$；

署名者用存储部件 (21)，存储上述接收到的公开参数、上述组公开密钥、上述成员秘密密钥、上述署名者确定信息 T_i 和消息；

消息生成部件 (24)，生成上述消息并写入到上述署名者用存储部件；

组署名生成部件 (25)，根据上述署名者用存储部件内的公开参数和组公开密钥，对上述署名者确定信息 T_i 进行加密，生成该署名者确定信息 T_i 的密码数据，并根据上述署名者用存储部件内的公开参数、上述组公开密钥、上述成员秘密密钥和上述消息、上述署名者确定信息 T_i 的密码数据，生成表示知道了该成员秘密密钥和基于该署名者确定信息 T_i 正确地生成了上述密码数据的零知识证明，

其中，^ 是表示幂的记号，

上述通信部件 (23) 将由上述密码数据和上述零知识证明构成的组署名和上述消息发送到上述验证者装置。

5. 一种验证者装置 (30)，能够与使用组署名方式的组管理者装置 (10) 和署名者装置 (20_i) 进行通信，其特征在于包括：

通信部件 (33)，从上述组管理者装置接收包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、包含根据上述公开参数使得满足值 a，$b \in Z_q$、第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 那样地生成的值 g_2、f 和上述生成元 g_1 的组公开密钥，从上述署名者装置接收组署名和消息，其中该组署名由以下部分构成：由根据上述值 a，$b \in Z_q$、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$ 而使得满足第四关系式 $f = g_1\hat{}\{k_{i1}\} g_2\hat{}\{k_{i2}\}$ 那样地生成的继承 k_{i1}、k_{i2} 构成的成员秘密密钥、针对根据上述成员秘密密钥和上述生成元 g_1 生成的署名者确定信息 $T_i = g_1\hat{}\{k_{i1}\}$ 而表示知道了上述成员秘密密钥并且基于上述署名者确定信息 T_i 而正确地生成了密码数据的零知识证明、上述署名者确定信息 T_i 的密码数据；

验证者用存储部件 (31)，存储上述接收到的公开参数和上述组公开密钥；

署名验证部件 (34)，根据上述接收到的组署名和消息、上述验证者用存储部件内的公开参数和组公开密钥，对该组署名的正当性进行验证，

其中，^ 是表示幂的记号，

上述通信部件 (33) 将上述验证的结果发送到上述署名者装置，

上述密码数据是由上述署名者装置根据上述公开参数和组公开密钥对上述署名者确定信息 T_i 进行了加密的数据，

上述零知识证明是由上述署名者装置根据上述公开参数、上述组公开密钥、上述成员秘密密钥和消息、上述署名者确定信息 T_i 的密码数据生成的数据。

6. 一种组管理者装置 (10) 的方法，该组管理者装置 (10) 能够与使用组署名方式的署名者装置 (20_i) 和验证者装置 (30) 进行通信，其特征在于，包括如下步骤：

将包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数写入到管理者用存储部件 (11) 中的步骤；

组密钥生成步骤，根据上述管理者用存储部件内的公开参数，生成包含值 a，$b \in Z_q$ 的组秘密密钥、包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2，f 和上述生成元 g_1 的组公开密钥；

成员秘密密钥生成步骤，根据上述组秘密密钥、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$，计算出由满足第四关系式 $f = g_1\hat{}\{k_{i1}\} g_2\hat{}\{k_{i2}\}$ 的继承 k_{i1}、k_{i2} 构成的成员秘密密钥；

署名者确定信息计算步骤，根据上述成员秘密密钥和上述生成元 g_1，计算出署名者确定信息 $T_i = g_1\hat{}\{k_{i1}\}$；

将用于生成上述组署名方式中的组署名的上述公开参数、上述组公开密钥、上述成员秘密密钥和上述署名者确定信息 T_i 发送到上述署名者装置的步骤；以及

将用于对上述组署名方式中的组署名进行验证的上述公开参数和上述组公开密钥发送到上述验证者装置的步骤，

其中 ^ 是表示幂的记号。

7. 根据权利要求 6 所述的组管理者装置的方法，其特征在于，还包括如下步骤：

相互关联地将上述署名者确定信息 T_i 和用户识别信息 ID(i) 存储到上述存储器中的步骤；

从上述署名者装置接收组署名和消息的步骤，其中该组署名由针对上述署名者确定信息 $T_i = g_1^{\wedge}\{k_{i1}\}$ 表示知道了上述成员秘密密钥并且基于上述署名者确定信息 T_i 正确地生成了上述密码数据的零知识证明、上述署名者确定信息 T_i 的密码数据构成；

根据上述接收到的组署名和消息、上述公开参数、上述生成的组秘密密钥和组公开密钥，对该组署名的正当性进行验证的步骤；以及

在上述验证的结果表示正当性时，根据上述组秘密密钥从上述密码数据计算署名者确定信息 T_i，从上述管理者用存储部件中确定与所得到的署名者确定信息 T_i 对应的用户识别信息 ID(i) 的步骤，

其中，

上述密码数据是由上述署名者装置根据上述公开参数和组公开密钥对上述署名者确定信息 T_i 进行了加密的数据，

上述零知识证明是由上述署名者装置根据上述公开参数、上述组公开密钥、上述成员秘密密钥和消息、上述署名者确定信息 T_i 的密码数据生成的数据。

8. 一种署名者装置 (20_i) 的方法，该署名者装置 (20_i) 能够与使用组署名方式的组管理者装置 (10) 和验证者装置 (30) 进行通信，其特征在于，包括如下步骤：

从上述组管理者装置接收包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、包含根据上述公开参数使得满足值 $a, b \in Z_q$、第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 那样地生成的值 g_2、f 和上述生成元 g_1 的组公开密钥、由根据上述值 $a, b \in Z_q$、上述组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$ 而使得满足第四关系式 $f = g_1^{\wedge}\{k_{i1}\} g_2^{\wedge}\{k_{i2}\}$ 那样地生成的继承 k_{i1}、k_{i2} 构成的成员秘密密钥、根据上述成员秘密密钥和上述生成元 g_1 生成的署名者确定信息 $T_i = g_1^{\wedge}\{k_{i1}\}$ 的步骤；

将上述接收到的公开参数、上述组公开密钥、上述成员秘密密钥、上述署名者确定信息 T_i 和消息写入到署名者用存储部件 (21) 中的步骤；

生成上述消息并写入到上述署名者用存储部件的步骤；

根据上述署名者用存储部件内的公开参数和组公开密钥，对上述署名者确定信息 T_i 进行加密，生成该署名者确定信息 T_i 的密码数据的步骤；

根据上述署名者用存储部件内的公开参数、上述组公开密钥、上述成员秘密密钥和上述消息、上述署名者确定信息 T_i 的密码数据，生成表示知道了该成员秘密密钥且基于该署名者确定信息 T_i 正确地生成了上述密码数据的零知识证明的零知识证明生成步骤；以及

将由上述密码数据和上述零知识证明构成的组署名和上述消息发送到上述验证者装置的步骤，

其中，^ 是表示幂的记号。

9. 一种验证者装置 (30) 的方法，该验证者装置 (30) 能够与使用组署名方式的组管理者装置 (10) 和署名者装置 (20_i) 进行通信，其特征在于，包括如下步骤：

从上述组管理者装置接收包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡

回群G的生成元g_1的公开参数、包含根据上述公开参数使得满足值$a,b \in Z_q$、第一关系式$g_2 = g_1^a$和第二关系式$f = g_1^b$那样地生成的值g_2、f和上述生成元g_1的组公开密钥的步骤；

将上述接收到的公开参数、上述组公开密钥写入到验证者用存储部件(31)中的步骤；

从上述署名者装置接收组署名和消息的步骤，其中该组署名由以下部分构成：由根据上述值$a, b \in Z_q$、上述组公开密钥和第三关系式$k_{i1} = b - ak_{i2} \mod q$而使得满足第四关系式$f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$那样地生成的继承$k_{i1}$、$k_{i2}$构成的成员秘密密钥、针对根据上述成员秘密密钥和上述生成元g_1生成的署名者确定信息$T_i = g_1\hat{}\{k_{i1}\}$而表示知道了上述成员秘密密钥并且基于上述署名者确定信息T_i而正确地生成了上述密码数据的零知识证明、上述署名者确定信息T_i的密码数据；

根据上述接收到的组署名和消息、上述验证者用存储部件内的公开参数和组公开密钥，对该组署名的正当性进行验证的步骤；以及

将上述验证的结果发送到上述署名者装置的步骤，

其中，^是表示幂的记号，

上述密码数据是由上述署名者装置根据上述公开参数和组公开密钥对上述署名者确定信息T_i进行了加密的数据，

上述零知识证明是由上述署名者装置根据上述公开参数、上述组公开密钥、上述成员秘密密钥和消息、上述署名者确定信息T_i的密码数据生成的数据。

组署名系统、装置和方法

技术领域

[0001] 本发明涉及组署名系统、装置和程序，例如涉及能够减少计算量并提高计算速度的组署名系统、装置和程序。

[0002] 背景技术

[0003] 作为具有匿名性的电子署名在1991年由Chaum提出了组署名方式（参考D Chaum and E.van Heyst，“Group Signatures”，In Proc.of EUROCRYPT’91，LNCS 547，pp.257～265，1991）。在通常的电子署名方式中，由于用于署名验证的公开密钥和用于署名生成的秘密密钥是一对一对应的，所以不保持署名生成者的匿名性。

[0004] 与此相对，在组署名方式中，用于署名验证的组公开密钥和用于署名生成的成员秘密密钥是一对一对应的，因此保持了署名生成者的匿名性。即，组署名方式由于1个组公开密钥与n个成员秘密密钥对应，所以有以下的性质，即在署名验证时，无法确定署名生成者。另外，组署名方式还具有以下的性质：只有作为特权者的组管理者才能够确定署名者。

[0005] 但是，在现有的组署名方式中，署名长度、署名生成计算量与成员数成正比，因此具有许多成员的组中的效率非常低，不适于使用。

[0006] 与此相对，在1997年由Camenisch等提出了效率不依存于成员数的组署名方式（参考J.Camenisch and M.stadler，“Effcient groupsignature schemes for large groups”，In Proc.of CRYPTO’97，LNCS1294，pp.410～424，1997）。在该方式下，将与成员秘密密钥对应的组管理者的署名用作成员证明书(membership certificate)。在组署名中包含用组管理者的公开密钥进行了加密的成员证明书（或其一部分）、以及表示正确地对成员证明书进行了加密和持有成员秘密密钥和成员证明 书的情况的非对话知识证明。署名验证者根据非对话知识证明的验证，能够验证是成员的署名。进而，组管理者通过成员证明书的解密，能够确定署名者。使用这样的成员证明书的概念对于成为其后的组署名方式的基础是重要的。

[0007] 但是，该Camenisch等的方式虽然效率不依存于成员数，但从实用的观点出发，效果低。

[0008] 最初的高效(practical)的组署名方式是2000年由Ateniese等提出的方式(G.Ateniese，J.Camenisch，M.Joye，and G.Tsudik，“Apractical and provably secure coalition-resistant group signaturescheme”，In Proc.of CRYPTO 2000，LNCS 1880，pp.255～270，2002，以下称为“ACJT00”方式）。Ateniese的组署名方式大幅提高了效率，可以研究实用化。Ateniese的组署名方式在生成署名时需要RSA署名生成的200倍左右的计算量，因此要继续研究改进。Ateniese的方式的安全性基于强RSA问题(strong-RSA problem)。

[0009] 现在，广为人知的高速的组署名方式是2004年由Camenisch等提出的方式（J.Camenisch and J.Groth，“Group Signatures：BetterEfficiency and New Theoretical Aspects”，Forth Int.Conf.on Securityin Communication Networks-SCN 2004，LNCS 3352，120～133，2005. 以下称为“CG04”方式。可以从以下的URL取得完整说

明 (2007 年 6 月现在)http://www.brics.dk/jg/)。“CG04”方式的署名生成计算量被降低到 RSA 署名生成的 8 倍左右。“CG04”方式的安全性也基于强 RSA 问题。

[0010] 以上那样的“CG04”方式的组署名方式与“ACJT00”方式相比,计算量小,但根据本发明者的研究,考虑到还需要强化对组署名方式的实用性方面,而有进一步减少计算量提高计算速度的余地。

发明内容

[0011] 本发明的目的在于 :提供一种能够减少计算量而提高计算速度的组署名系统、装置和程序。

[0012] 本发明的第一方面是一种组署名系统,具备能够相互进行通信的组管理者装置、署名者装置和验证者装置,各装置使用组署名方式,上述组管理者装置具备 :存储包含在上述组署名方式中使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数的参数存储单元 ;根据上述参数存储单元内的公开参数,生成包含值 $a,b \in Z_q$ 的组秘密密钥、包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2,f 和上述生成元 g_1 的组公开密钥的组密钥生成单元 ;根据上述组秘密密钥、上述组公开密钥和第三关系式 $k_{i1} = b-ak_{i2} \mod q$,计算出由满足第四关系式 $f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$ 的继承 k_{i1}、k_{i2} 构成的成员秘密密钥的成员秘密密钥生成单元 (其中 ^ 是表示幂的记号) ;根据上述成员秘密密钥和上述生成元 g_1,计算出署名者确定信息 $Ti = g_1\hat{}\{k_{i1}\}$ 的署名者确定信息计算单元,上述署名者装置具备 :存储包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、上述组公开密钥、上述成员秘密密钥、上述署名者确定信息 T_i 和消息的署名者用存储单元 ;根据上述署名者用存储单元内的公开参数和组公开密钥,对上述署名者确定信息 T_i 进行加密,生成该署名者确定信息 T_i 的密码数据的密码生成单元 ;根据上述署名者用存储单元内的公开参数、上述组公开密钥、上述成员秘密密钥和上述消息、上述署名者确定信息 T_i 的密码数据,生成表示知道了该成员秘密密钥和该署名者确定信息 T_i 的零知识证明的零知识证明生成单元 ;将由上述密码数据和上述零知识证明构成的组署名和上述消息发送到上述验证者装置的单元,上述验证者装置具备 :存储包含上述组署名方式所使用的素数位数 q、上述 q 的乘法巡回群 G 的生成元 g_1 的公开参数、上述组公开密钥的验证者用存储单元 ;从上述署名者装置接收上述组署名和消息的单元 ;根据上述接收到的组署名和消息、上述验证者用存储单元内的公开参数和组公开密钥,对该组署名的正当性进行验证的验证单元 ;将上述验证的结果发送到上述署名者装置的单元 ;为了署名者确定,而向组管理者装置发送消息和组署名的单元。

[0013] 根据第一方面,使用素数位数 q 的乘法巡回群 G 而不使用位数未 知的乘法巡回群,成为只利用了位数已知的组署名方式,并且实现了将继承 k_{i1}、k_{i2} 作为成员秘密密钥的组署名方式,由此与现有的 [CG04] 方式相比,能够减少计算量提高计算速度。

[0014] 另外,以上的方面表现为由各装置构成的“系统”,但并不只限于此,也可以表现为各装置的集合或每个装置的“装置”、“程序”、“计算机可读的存储介质”或“方法”。

附图说明

[0015] 图 1 是表示本发明的一个实施例的组署名系统的结构的模式图。

[0016] 图 2 是表示该实施例的组管理者装置的结构的模式图。

[0017] 图 3 是表示该实施例的组管理者用存储部件的结构的模式图。

[0018] 图 4 是表示该实施例的署名者装置的结构的模式图。

[0019] 图 5 是表示该实施例的署名者用存储部件的结构的模式图。

[0020] 图 6 是表示该实施例的验证者装置的结构的模式图。

[0021] 图 7 是表示该实施例的验证用存储部件的结构的模式图。

[0022] 图 8 是用于说明该实施例中的密钥对的生成处理的流程图。

[0023] 图 9 是用于说明该实施例中的成员秘密密钥的生成处理的流程图。

[0024] 图 10 是用于说明该实施例中的署名者确定信息的计算处理的流程图。

[0025] 图 11 是用于说明该实施例中的加密处理的流程图。

[0026] 图 12 是用于说明该实施例中的零知识证明的计算处理的流程图。

[0027] 图 13 是用于说明该实施例中的署名验证处理的流程图。

[0028] 图 14 是用于说明该实施例中的署名验证处理的流程图。

[0029] 图 15 是用于说明该实施例中的署名者确定处理的流程图。

[0030] 图 16 是与现有技术相比表示该实施例的效果的图。

具体实施方式

[0031] 以下，参考附图，详细说明本发明的一个实施例，但之前先说明本发明的一个实施例的组署名方式（以下称为实施例方式）的概要。

[0032] 实施例方式的最大特长是效率极高。在使用作为高速地进行幂余数运算的方法的指数同时乘法 (Simultaneous Multiple Exponentiation) 法的情况下，与“CG04”方式是 RSA 署名生成的 8 倍以上的计算量的情况相比，在实施例方式下，能够以 RSA 署名生成的大致 3 倍左右的计算量进行署名生成。另外，在指数同时乘法法中，需要根据底的值进行表的事前计算，但在实施例方式中，幂余数运算的底始终固定，因此不需要每次进行表的事前计算，通过保存表，能够进一步减少一些计算量。

[0033] 进而，实施例方式的署名生成所利用的成员秘密密钥非常短，其比特长只有 [CG04] 方式的 1/10、RSA 的 1/9。

[0034] 相对于 [ACJT00] 方式、[CG04] 方式的安全性基于强 RSA 问题的情况，实施例方式的安全性基于 DDH(decisional Diffile-Hellman) 问题。与此相伴，实施例方式也可以高效地在椭圆曲线上实现，能够大幅地缩短署名长度和密钥长度，能够高速化。实施例方式作为只基于 DDH 问题的高效的组署名，是最初的方式。进而，实施例方式可以通过单纯的计算的组合来实现，因此能够期待在广范围的平台上的应用。

[0035] < 组署名 >

[0036] 以下，定义实施例方式的前提的组署名的功能和安全性。

[0037] [组署名的功能]

[0038] 高效的现有方式大都利用与成员秘密密钥对应的组管理者的署名作为成员证明书。在实施例方式中，不利用组管理者的署名，因此为了与现有方式的成员证明书区别，而使用署名者确定信息 (tracinginformation) 这样的用语。在组署名中，包含加密了的署名者确定信息、表示署名者确定信息被正确地加密的非对话知识证明、表示具有成员秘密密

钥和署名者确定信息的非对话知识证明是与成员证明书一样的。

[0039] 组署名方式 GS 由以下的 4 个多项式时间算法 GKg、GSig、GVf、Open 组成。

[0040] [密钥生成算法 GKg]

[0041] 密钥生成算法 GKg 是将公开参数和组的成员数 n 作为输入，用于生成并输出组公开密钥 gpk、组秘密密钥 gmsk、成员秘密密钥的集合 gsk = (gsk[1]、……gsk[n])、与之对应的署名者确定信息 T = (T_1、……T_n) 的概率多项式时间算法。

[0042] [署名生成算法 GSig]

[0043] 署名生成算法 GSig 是针对组公开密钥 gpk、成员秘密密钥 gsk[i]、署名者确定信息 T_i、消息 msg 生成组署名 σ 的概率多项式时间算法。

[0044] [署名验证算法 GVf]

[0045] 署名验证算法 GVf 是将组公开密钥 gpk、消息 msg、组署名 σ 作为输入，如果署名正确则输出有效 (valid)，如果不正确则输出无效 (invalid) 的确定多项式时间算法。

[0046] [署名者确定算法 Open]

[0047] 署名者确定算法 Open 是将组公开密钥 gpk、组秘密密钥 gmsk、消息 msg、组署名 σ 作为输入，如果署名正确则输出生成该署名的用户的 ID = i，如果不正确则输出无效 (invalid) 的确定多项式时间算法。

[0048] [组署名的安全性]

[0049] 当初对组署名的安全性定义了很多的要素。其后，由 Bellare 等总结了静态组 (static group) 的组署名的安全性的要素 (参考 M.Bellare, D.Micciancio, and B.Warinschi,“Foundations of Group Signatures :Formal Definitions, Simplified Requirements, and a Construction Basedon General Assumptions”, In Proc.of EUROCRYPT 2003, LNCS 2656, pp614 ～ 629, 2003.)。另外，静态组是指不具有成员的追加、删除功能，如果一度生成了组则不变更成员的组。在此，Bellare 的要素是非常严格的，考虑到对组成员全体的勾结的安全性。因此，一般减弱 Bellare 的要素而定义安全性。在此，根据 Bellare 的要素，再定义没有组管理者、成员的勾结的情况下的安全性。勾结以外的定义与 Bellare 的定义一样。

[0050] 在具有以下的正当性 (correctness)、匿名性 (anonymity)、可追踪性 (traceability) 的 3 个性质时，组署名方式 GS 被称为是安全的。

[0051] [1. 正当性 (correctness)]

[0052] GVf(gpk, msg, GSig(gsk[i], msg)) = valid 并且

[0053] Open(gmsk, msg, GSig(gsk[i], msg)) = i

[0054] 即，正确生成的署名通过署名验证算法 GVf 验证成功，通过署名者确定算法 Open 能够确定署名者。

[0055] [2. 匿名性 (anonymity)]

[0056] 考虑以下的情况。

[0057] (1) 设置 (setup) :执行密钥生成算法 GKg(n)，生成组公开密钥 gpk、组秘密密钥 gmsk、成员秘密密钥的集合 gsk、署名者确定信息 T，向对手 (adversary)A 提供组公开密钥 gpk。

[0058] (2) 询问 (queries) :对手 A 进行以下的 2 种询问 (a)、(b)。其中，收买询问

(corruption query) 只限于进行 1 次。

[0059] (a) 署名 (signing) :指定用户 i 和消息 msg,进行署名询问 (signing query),得到组署名 σ = GSig(gpk, gsk[i], msg)。

[0060] (b) 收买 (corruption) :指定用户 u(1 ≤ u ≤ n),进行收买询问,得到成员秘密密钥 gsk[u]。

[0061] (3) 查询 (challenge) :对手 A 输出消息 msg 和用户 ID i0、i1。这时,不能是 u = i0 或 u = i1。查询者 (challenger) 随机地选择用户 ID b ← {0,1},计算出组署名 σ * ← GSig(gpk, gsk[ib], msg) 返回给对手 A。

[0062] (4) 限定的询问 (restricted queries) :以下的询问 (a)、(b)

[0063] (a) 署名 (signing) :与上述一样。

[0064] (b) 收买 (corruption) :与上述一样。其中,在已经进行了 1 次的情况下,无法进行询问。另外,这时,必须是 u = i0 或 u = i1。

[0065] (5) 输出 (output) :对手 A 输出用户 ID b'。

[0066] 在 b' = b 时,称为“对手 A 攻击成功”。在可以无视对手 A 的成功概率时,称为组署名方式具有匿名性 (anonymity)。

[0067] [3. 可跟踪性 (traceability)]

[0068] 考虑以下的情况。

[0069] (1) 设置 (setup) :执行密钥生成算法 GKg(n),生成组公开密钥 gpk、组秘密密钥 gmsk、成员秘密密钥 gsk、署名者确定信息 T,向对手 A 提供组公开密钥 gpk。

[0070] (2) 询问 (queries) :对手可以进行以下的 2 种询问 (a)、(b)。其中,收买询问 (corruption query) 只限于进行 1 次。

[0071] (a) 署名 (signing) :指定用户 i 和消息 msg,进行署名询问 (signing query),得到组署名 σ = GSig(gpk, gsk[i], msg)。

[0072] (b) 收买 (corruption) :指定用户 u(1 ≤ u ≤ n),进行收买询问,得到成员秘密密钥 gsk[u]。

[0073] (3) 应答 (response) :对手 A 输出消息 msg* 和组署名 σ *。在署名者确定算法 Open 的结果是 Open(gmsk, msg*, σ *) = i ≠ u,在署名询问 (signing query) 中没有指定 i、msg* 时,称为“对手 A 攻击成功”。在可以无视对手 A 的成功概率时,称为组署名方式具有可跟踪性 (traceability)。

[0074] < 准备 >

[0075] 以下,在理解实施例方式的基础上,说明重要的 DDH(decisionalDiffie-Hellman) 问题、继承 (representation)、Cramer-Shoup 暗号。

[0076] [DDH 问题]

[0077] 将素数位数 q 的乘法巡回群设为 G。将随机的 4 组 (quadruples) $(g_1, g_2, u_1, u_2) \in G^4$ 的分布设为 R。随机地选择 g_1、$g_2 \in G$ 和 $r \in Z_q$,将 $u_1 = g^r$、$u_2 = g^r$ 的 4 组 $(g_1, g_2, u_1, u_2) \in G^4$ 的分布设为 D。这时,将找出任意给出的 4 组 (g_1, g_2, u_1, u_2) 属于分布 R、D 的哪个的问题称为 DDH 问题。实施例方式的安全性归结为 DDH 问题的困难性。

[0078] 另外,如果能够解开离散对数问题 (discrete logarithm problem),则能够解开 DH 问题 (Diffie-Hellman problem),如果能够解开 DH 问题,则能够解开 DDH 问题。DH 问题

是根据给定的 g、g^x、g^y 计算 g^{xy} 的问题。离散对数问题是根据给定的 g、g^x 计算 x 的问题。可以相信解开这些 DDH 问题、DH 问题和离散对数问题都是困难的。

[0079] [继承 (representation)]

[0080] 在乘法巡回群 G 上的计算中，将满足 $h = g_1^{e_1} g_2^{e_2} \cdots\cdots g_k^{e_k}$ 的 $(e_1, e_2, \cdots\cdots e_k)$ 称为以 $(g_1, g_2, \cdots\cdots g_k)$ 为底的 h 的继承。另外，“^”是表示幂的记号。

[0081] 继承在暗号理论的领域中以前也被用作缓和离散对数 (relaxeddiscrete log(RDL))(参考 D.Chaum, J.H.Evertse, and J.van de Graaf,“An improved protocol for demonstrating possession of discretelogarithms and some general izations”, In Proc.of EUROCRYPT’87, LNCS 304, pp.127 ～ 141,1987)，其后也有时使用。在 1997 年的 Camenisch 的方式中，使用了应用了 Schnorr 署名 (参考 C.P.Schnorr,“Efficient Signature Generation by Smart Cards”, Journal ofCryptology, Vol.4, pp.161 ～ 174, 1991.) 的继承的非对话知识证明。在实施例方式中，将成员秘密密钥作为继承，在组署名中包含与继承对应的非对话知识证明。

[0082] [Cramer-Shoup 暗号]

[0083] 在实施例方式中，在署名者确定信息的加密中使用 Cramer-Shoup 暗号 (参考 R.Cramer and V.Shoup,“A Practical Public KeyCryptosystem Provably Secure against Adaptive Chosen CiphertextAttack”, In Proc.of CRYPTO’98, LNCS 1462, pp.13 ～ 25,1998)。但是，实施例方式并不只限于 Cramer-Shoup 暗号。

[0084] 以下，说明 Cramer-Shoup 暗号。

[0085] [公开密钥 (public key)/ 秘密密钥 (private key) 对生成]

[0086] 作为公开参数，将素数位数 q 的乘法巡回群 G 和其生成元 g_1 和通用单向性哈希 (universal one-way hash) 函数作为输入，进行以下的处理。

[0087] (1) 随机地选择 $g_1, g_2 \in G$。

[0088] (2) 随机地选择 $x_1, x_2, y_1, y_2, z \in Z_q$。

[0089] (3) 计算 $c = g_1^{x_1} g_2^{x_2}$，$d = g_1^{y_1} g_2^{y_2}$，$h = g_1^{z}$。

[0090] (4) 从通用单向性哈希函数的集合中选择哈希函数 H。

[0091] (5) 输出公开密钥 $pk = (g_1, g_2, c, d, h, H)$，秘密密钥 $sk = (x_1, x_2, y_1, y_2, z)$。

[0092] [加密]

[0093] 将公开密钥 $pk = (g_1, g_2, c, d, h, H)$、消息 $m \in G$ 作为输入，进行以下的处理。

[0094] (1) 随机地选择 $r \in Z_q$。

[0095] (2) 计算 $u_1 = g_1^r$，$u_2 = g_2^r$，$e = h^r m$。

[0096] (3) 计算 $\alpha = H(u_1, u_2, e)$。

[0097] (4) 计算 $v = c^r d^{r\alpha}$。

[0098] (5) 输出密码 (u_1, u_2, e, v)。

[0099] [解密]

[0100] 将密码 (u_1, u_2, e, v) 作为输入，进行以下的处理。

[0101] (1) 计算 $\alpha = H(u_1, u_2, e)$。

[0102] (2) 验证 $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$ 是否成立，在否的情况下，作为无效的密码而拒绝，结束处理。

[0103] (3) 计算 $m = e/u_1^z$，作为明文输出。

[0104] 以上是 Cramer-Shoup 暗号的处理。

[0105] < 实施例方式的概要 >

[0106] 接着，说明实施例方式的概要。

[0107] 本实施例通过以离散对数为基础的方式，谋求组署名方式的高速化。理由是：由于在以 RSA 为基础的方式中幂指数长，所以位数未知的群中的非对话知识证明的效率低，由此全体的效率也低。另外，[ACJT00] 方式、[CG04] 方式也都是以 RSA 为基础的方式，因此与实施例方式相比，效率低。

[0108] 如果补足说明，则相对于 [ACJT00] 方式是以 RSA 为基础的方式，[CG04] 方式的一部分以离散对数为基础，大幅改善了效率，但还剩余以 RSA 为基础的部分。与此相对，在实施例方式中，全部作为以离散对数为基础的方式，谋求了高速化。

[0109] 实施例方式进而将继承设为成员秘密密钥。在离散对数是秘密密钥 的情况下，针对一个公开密钥只具有 1 个秘密密钥。与此相对，在继承是秘密密钥的情况下，针对 1 个公开密钥可以作成多个秘密密钥，因此适合于具有许多成员的组。在 Kiayias 等的方式（参考 A. Kiayias and M. Yung, "Extracting Group Signatures from Traitor Tracing Schemes", In Proc. of EUROCRYPT 2003, LNCS 2656, pp. 630 ～ 648, 2003）中，也使用继承，但使用继承自身作为署名者确定信息，因此效率低。

[0110] 与此相对，在实施例方式中，不是继承自身，而是使用根据继承唯一计算的值作为署名者确定信息，因此效率高。

[0111] （实施例方式）

[0112] 图 1 是表示本发明的一个实施例的组署名系统的结构的模式图。该组署名系统具备能够相互进行通信的 1 台组管理者装置 10；n 台署名者装置 20_1、……20_i、……、20_j、……、20_n；1 台验证装置 30。对于各装置 10、20_1、…… 20_n、30 的每个装置，都可以通过硬件结构、硬件资源与软件的组合结构的任意一个来实施。作为组合结构的软件，使用预先从网络或存储介质 M 安装到对应的装置的计算机中，使其实现对应的装置的功能的程序。另外，各署名者装置 20_1、……、20_n 是相互相同的硬件结构，因此在以下的说明中，以第 i 个署名者装置 20_i 为代表进行说明。另外，本实施例的组署名方式如在后述的图 8 ～图 15 中表示的例子所示，加密方式使用 Cramer-Shoup 暗号，零知识证明方式使用应用了 Schnorr 署名的方式，但并不只限于这些加密方式和零知识证明方式。即，本实施例的组署名方式并不只限于图 8 ～图 15 所示的方式，使用其他的加密方式和零知识证明方式也可以实现。

[0113] 在此，组署名管理者装置 10 如图 2 所示，具备管理者用存储部件 11、输入部件 12、通信部件 13、组密钥生成部件 14、成员秘密密钥生成部件 15、署名验证部件 16、署名者确定部件 17 和输出部件 18。

[0114] 管理者用存储部件 11 是能够从各部件 12 ～ 17 访问的存储装置，如图 3 所示，存储公开参数、组公开密钥 gpk、组秘密密钥 gmsk、成员信息、用户管理信息、计算表、消息 msg 和组署名 σ。也可以暂时存储 该消息 msg、组署名 σ。

[0115] 公开参数至少包含组署名方式所使用的素数位数 q、q 的乘法巡回群 G 的生成元 g_1，在此还包含哈希函数 H。

[0116] 组秘密密钥 gmsk 还至少包含根据公开参数选择出的值 $a, b \in Z_q$，在此，还包含值

$x_1, x_2, y_1, y_2, z \in Z_q$。

[0117] 组公开密钥 gpk 至少包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2、f 和生成元 g_1，在此，还包含值 c、d、h 和哈希函数 H。另外，$c = g_1\hat{}\{x_1\}g_2\hat{}\{x_2\}$、$d = g_1\hat{}\{y_1\}g_2\hat{}\{y_2\}$、$h = g_1^z$。

[0118] 成员信息是使成员秘密密钥 gsk[i] 和署名者确定信息 T_i 与每个用户识别信息 ID(i) 相互关联而成的信息 ($1 \leqslant i \leqslant n$)。

[0119] 用户管理信息是使用户信息与每个用户识别信息 ID(i) 关联而成的信息 ($1 \leqslant i \leqslant n$)。用户信息例如包含用户的名字、联系地址信息（电话号码、电子邮件地址等），在组署名的目标是电子商务交易的情况下，还包含决算信息。

[0120] 计算表是在各部件 14 ～ 16 使用指数同时乘法 (simultaneous multipleexponetiation) 法的情况下所参照的信息。指数同时乘法法是高速地进行 $g_1\hat{}\{e_1\}g_2\hat{}\{e_2\}\cdots\cdots g_k\hat{}\{e_k\}$ 的形式的计算的方法，需要预先执行最大 2^k 次的乘法计算，作成最大 2^k 大小的计算表。因此，与底 g_1、……g_k 的个数 k 对应地，计算表所需要的存储量变大。其中，如果底是固定的，则不需要每次作成计算表，可以通过事前计算而以幂 1 次左右的计算量进行计算。即，例如在 $g_1\hat{}\{e_1\}g_2\hat{}\{e_2\}$ 这样的幂 2 次的计算中，通过参照计算表，能够以幂 1 次的计算量执行。因此，如果作为计算表，组管理者和验证者装置具有 $1, g_1, g_2, g_1 \times g_2, f, f \times g_1, f \times g_2, f \times g_1 \times g_2$ 和 $1, h, g_1, h \times g_1$，署名者装置具有 $1, h, g_1, h \times g_1$ 和 $1, c, d, c \times d$，则可以以幂 1 次的计算量，执行后述的步骤 ST4、ST5、ST34、ST36、ST42、ST44、ST52、ST54、ST62、ST64 的幂 2 次或 3 次的计算。

[0121] 消息 msg 是由署名者装置 20_i 生成的任意的信息。

[0122] 组署名 σ 由后述的密码 (u_1, u_2, e, v)、零知识证明 (A, B, C, s_1, s_2, s_r) 组成，是由署名者装置 20_i 生成的信息。在此，可以将消息 msg、组署名 σ 暂时存储在管理者用存储部件 11 中。

[0123] 输入部件 12 是组管理者装置 10 内部与外部之间的输入接口，使用键盘和鼠标等输入设备。

[0124] 通信部件 13 是组管理者装置 10 内部与外部之间的通信接口。通信部件 13 例如具有以下的功能：通过加密通信等安全的方法，将用于生成组署名方式中的组署名的公开参数、组公开密钥、成员秘密密钥和署名者确定信息 T_i 发送到署名者装置 20_1 ～ 20_n。另外，通信部件 13 例如具有以下的功能：将用于对组署名方式中的组署名进行验证的公开参数和组公开密钥发送到验证者装置 30。进而，通信部件 13 还具有从验证者装置 30 接收消息 msg、组署名 σ 的功能。

[0125] 组密钥生成部件 14 根据管理者用存储部件 11 内的公开参数，生成包含值 $a, b \in Z_q$ 的组秘密密钥、包含满足第一关系式 $g_2 = g_1^a$ 和第二关系式 $f = g_1^b$ 的值 g_2、f 和生成元 g_1 的组公开密钥。在此，组密钥生成部件 14 具有执行图 8 所示的处理的功能。另外，组密钥生成部件 14 也可以参照计算表，通过指数同时乘法法，进行幂运算，在成员秘密密钥生成部件 15 和署名验证部件 16 中对此也一样。

[0126] 成员秘密密钥生成部件 15 根据组秘密密钥、组公开密钥和第三关系式 $k_{i1} = b - ak_{i2} \bmod q$，计算出由满足第四关系式 $f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$ 的继承 k_{i1}、k_{i2} 组成的成员秘密密钥，并且根据成员秘密密钥和生成元 g_1，计算出署名者确定信息 $T_i = g_1\hat{}\{k_{i1}\}$。在此，成员秘密

密钥生成部件 15 具有执行图 9 和图 10 所示的处理的功能。

[0127] 署名验证部件 16 根据管理者用存储部件 11 内的组署名、消息、公开参数和组公开密钥，对该组署名内的零知识证明的正当性进行验证，并且根据管理者用存储部件 11 内的组署名、组秘密密钥和组公开密钥，对该组署名内的密码数据的正当性进行验证。在此，署名验证部件 16 具有执行后述的图 14 所示的处理的功能。

[0128] 署名者确定部件 17 根据管理者用存储部件 11 内的组署名和组秘密密钥，计算署名者确定信息 T。在此，署名者确定部件 17 具有执行后述的图 15 所示的处理的功能。

[0129] 输出部件 18 是组管理者装置 10 内部与外部之间的输出接口，使用显示器装置和打印机等输出设备。

[0130] 署名者装置 20_i 如图 4 所示，具备署名者用存储部件 21、输入部件 22、通信部件 23、消息生成部件 24、组署名生成部件 25 和输出部件 26。

[0131] 署名者用存储部件 21 是能够从各部件 22 ～ 25 访问的存储装置，如图 5 所示，存储公开参数、组公开密钥 gpk、计算表、成员秘密密钥、署名者确定信息、消息和组署名。

[0132] 输入部件 22 是署名者装置 20_i 内部与外部之间的输入接口，使用键盘和鼠标等输入设备。

[0133] 通信部件 23 是署名者装置 20_i 内部与外部之间的通信接口。通信部件 23 例如具有以下的功能：通过加密通信等安全的方法，从组管理者装置 10 接收用于组署名方式中的组署名的公开参数、组公开密钥、成员秘密密钥和署名者确定信息 Ti。另外，通信部件 23 例如具有以下的功能：根据署名者的输入部件 22 的操作，向验证者装置 30 发送由署名者用存储部件 21 内的密码数据和零知识证明组成的组署名、消息。

[0134] 消息生成部件 24 具有以下的功能：根据署名者的输入部件 22 的操作，作成消息 msg 并写入到署名者用存储部件 21 中。

[0135] 组署名生成部件 25 具有以下的功能：根据署名者用存储部件 21 内的公开参数和组公开密钥，对署名者确定信息 T_i 进行加密，生成该署名者确定信息 T_i 的密码数据，并写入到署名者用存储部件 21 中。另外，组署名生成部件 25 具有以下的功能：根据署名者用存储部件 21 内的公开参数、组公开密钥、成员秘密密钥和消息、署名者确定信息 T_i 的密码数据，生成表示知道了该成员秘密密钥和该署名者确定信息 T_i 的零知识证明，将零知识证明与密码数据关联起来写入到署名者用存储部件 21 中。另外，密码数据和零知识证明构成组署名。另外，在此，组署名生成部件 25 具有执行图 11 和图 12 所示的处理的功能。另外，图 12 所示的零知识证明是基于知道了加密的署名者确定信息 T_i、知道了继承的一个、正确地加密了署名者确定信息 T_i 的消息 msg 的零知识证明。另外，组署名生成部件 25 也可以参照计算表，通过指数同时乘法法来执行幂运算。

[0136] 输出部件 26 是署名者装置 20_i 内部与外部之间的输出接口，使用显示器装置和打印机等输出设备。

[0137] 验证者装置 30 如图 6 所示，具备验证者用存储部件 31、输入部件 32、通信部件 33、署名验证部件 34 和输出部件 35。

[0138] 验证者用存储部件 31 是能够从各部件 32 ～ 34 访问的存储装置，如图 7 所示，存储公开参数、组公开密钥 gpk、计算表、消息和组署名。

[0139] 输入部件 32 是验证者装置 30 内部与外部之间的输入接口，使用键盘和鼠标等输

入设备。

[0140] 通信部件 33 是验证者装置 30 内部与外部之间的通信接口。通信部件 33 例如具有以下的功能 :通过加密通信等安全的方法,从组管理者装置 10 接收用于生成组署名方式的组署名的公开参数和组公开密钥。另外,通信部件 33 例如具有以下的功能 :从署名者装置 20_i 接收由密码数据和零知识证明组成的组署名、消息 ;将接收到的组署名和消息写入到验证者用存储部件 31 中 ;将署名验证部件 34 的验证结果发送到署名者装置 20_i ;在验证的结果是 OK,并且输入了署名者确定要求的情况下,为了进行署名者确定,向组管理者装置 10 发送消息和组署名。另外,通信部件 33 不一定必须向署名者装置 20_i 发送署名验证部件 34 的验证结果。在不发送验证结果的情况下,例如是验证者装置 30 不是在线实时地进行验证的情况等。

[0141] 署名验证部件 34 根据验证者用存储部件 31 内的组署名、消息、公开参数和组公开密钥,对该组署名的正当性进行验证,将验证结果发送到通信部件 33 和输出部件 35。在此,署名验证部件 34 具有执行图 13 所示的处理的功能。另外,署名验证部件 34 也可以参照计算表,通过指数同时乘法法,执行幂运算。另外,署名验证部件 34 不一定必须将验证结果发送到通信部件 33 和 / 或输出部件 35。

[0142] 输出部件 35 是验证者装置 30 内部与外部之间的输出接口,使用显示器装置和打印机等输出设备。输出部件 35 例如显示从署名验证部件 34 接收到的验证结果。

[0143] 接着,使用图 8 ～图 15 的流程图,说明如上那样构成的组署名系统 的动作。

[0144] (组公开密钥 / 组秘密密钥对的生成 :图 8)

[0145] 假设在组管理者装置 10 中,在根据组管理者的输入部件 12 的操作,将公开参数 (q, G, g_1, H) 保存在管理者用存储部件 11 中之后,启动了组密钥生成部件 14。

[0146] 组密钥生成部件 14 参考管理者用存储部件 11 内的素数位数 q,随机地选择 7 组 $(a, b, x_1, x_2, y_1, y_2, z) Z_q^7$(ST1)。另外,$Z_q$ 是 0 以上并小于 q 的整数的集合 {0, ……, q-1}。另外,a、b 是高效地计算多个继承所需要的值。

[0147] 接着,组密钥生成部件 14 根据管理者用存储部件 11 内的生成元 g_1 和在步骤 ST1 中得到的 7 组,计算 $g_2 = g_1^a$、$f = g_1^b$、$c = g_1^{x_1} g_2^{x_2}$、$d = g_1^{y_1} g_2^{y_2}$、$h = g_1^z$(ST2 ～ ST6)。g1 和 g2 是 f 的继承的底。

[0148] 另外,组密钥生成部件 14 从管理者用存储部件 11 内的公开参数读出通用单向哈希函数 H。

[0149] 然后,组密钥生成部件 14 将组秘密密钥 $gmsk = (a, b, x_1, x_2, y_1, y_2, z)$、组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$ 保存在管理者用存储部件 11 中 (ST7)。

[0150] 由此,组密钥生成部件 14 将组公开密钥 gpk 和组秘密密钥 gmsk 的生成结束消息发送到输出部件 18,结束处理。输出部件 18 对该生成结束消息进行显示输出。

[0151] (成员秘密密钥的生成 :图 9)

[0152] 假设在组管理者装置 10 中,预先根据组管理者的输入部件 12 的操作,将与成员数 n 对应的 n 人的用户识别信息 ID(1)、……ID(i)、……、ID(j)、……、ID(n) 保存在管理者用存储部件 11 中。另外,也可以由输入了成员数 n 的成员秘密密钥生成部件 15 生成用户识别信息 ID(1)、……、ID(n),从成员秘密密钥生成部件 15 写入到管理者用存储部件 11 中。

[0153] 成员秘密密钥生成部件15参照管理者用存储部件11内的素数位数q，随机地选择成员秘密密钥的一部分 $k_{i2} \in Z_q$(ST11)。

[0154] 这时，成员秘密密钥生成部件15参照管理者用存储部件11，在存在具有 $k_{i2} = k_{i2}$ 的成员秘密密钥 $gsk_j = (k_{j1}, k_{j2})$ 的成员的情况下，重新选择 k_{i2}。即，k_{i2} 必须对每个用户全不同。

[0155] 接着，成员秘密密钥生成部件15根据管理者用存储部件11内的素数位数q和组秘密密钥gmsk，计算成员秘密密钥的其他一部分 $k_{i2} = b - ak_{i2} \bmod q$(ST12)。

[0156] 然后，成员秘密密钥生成部件15将由所得到的 k_{i1}、k_{i2} 组成的成员秘密密钥 (k_{i1}, k_{i2} = gsk[i]) 与用户识别信息ID(i)关联起来保存在管理者用存储部件11中(ST13)。

[0157] 在此，成员秘密密钥 (k_{i1}, k_{i2}) 是以 (g_1、g_2) 为底的f的继承。即，根据上述的 $f = g_1^b$、$g_2 = g_1^a$、和 $k_i^2 = b - ak_{i2} \bmod q$ 的公式，表示为 $f = g_1\hat{}\{k_{i1}\}g_2\hat{}\{k_{i2}\}$。另外，通过使用包含在组秘密密钥gmsk中的a、b，能够高效地计算多个成员秘密密钥。能够计算该继承 k_{i1}、k_{i2} 的只有组管理者。知道继承 k_{i1}、k_{i2} 表示被组管理者承认的组成员。

[0158] 成员秘密密钥生成部件15循环进行与成员数n相同的次数n的以上的步骤ST11～ST13的处理，在分别地将n人的成员秘密密钥gsk[1]～gsk[n]与用户识别信息ID(1)～ID(n)关联起来而保存在管理者用存储部件11中后，结束处理。

[0159] (署名者确定信息计算处理：图10)

[0160] 接着，成员秘密密钥生成部件15根据管理者用存储部件11内的生成元 g_1 和成员秘密密钥gsk[i](= k_{i1}, k_{i2})，计算署名者确定信息 $T_i = g_1\hat{}\{k_{i1}\}$(ST21)。即，署名者确定信息Ti并不是继承自身，而是将继承的一部分作为幂指数的值。

[0161] 然后，成员秘密密钥生成部件15将所得到的署名者确定信息 T_i 与用户识别信息ID(i)关联起来保存在管理者用存储部件11中(ST22)。

[0162] 成员秘密密钥生成部件15循环进行与成员数n相同的次数n的以上的步骤ST21～ST22的处理，将n人的成员秘密密钥gsk[1]～gsk[n]与用户识别信息ID(1)～ID(n)分别地关联起来而保存在管理者用 存储部件11中后，结束处理。

[0163] (署名生成的准备)

[0164] 用户i通过在线或离线，将用户信息登录到组管理者装置10。由此，用户i通过加密通信或存储介质的邮送等安全的方法，从组管理者取得公开参数、组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$、成员秘密密钥gsk[i](= k_{i1}, k_{i2})和署名者确定信息Ti。

[0165] 然后，署名者装置 20_i 根据用户i的输入部件22的操作，将这些公开参数、组公开密钥gpk、成员秘密密钥gsk[i]和署名者确定信息 T_i 保存到署名者用存储部件21中。由此，署名者装置 20_i 能够进行署名生成处理。

[0166] 另外，署名者装置 20_i 根据用户i的输入部件22的操作，由消息生成部件24一边将消息 $msg \in \{0,1\}^*$ 显示在输出部件26一边作成，将得到的消息msg保存在署名者用存储部件21中。另外，消息msg并不只限于使用消息生成部件24作成的消息的情况，也可以从组管理者、署名验证者取得。例如，也可以是在电子商务交易的情况下，使用消息生成部件24作成的消息msg，在20岁以上等的资格证明的情况下，使用从组管理者取得的消息msg，在认证中利用的情况下，使用从署名验证者取得的消息msg。

[0167] (加密处理：图11)

[0168] 假设在署名者装置 20_i 中，根据用户 i 的输入部件 22 的操作，启动了组署名生成部件 25。

[0169] 组署名生成部件 25 参照署名者用存储部件 21 内的素数位数 q，随机地选择保密的随机数 $r \in Z_q$(ST31)。

[0170] 接着，组署名生成部件 25 根据署名者用存储部件 21 内的组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$ 和署名者确定信息 T_i、在步骤 ST31 中得到的随机数 r，计算 $u_1 = g_1^r$，$u_2 = g_2^r$，$e = h^r T_i$(ST32 ～ ST34)。另外，也可以每次根据成员秘密密钥 gmsk[i] = (= k_{i1}, k_{i2})，计算出署名者确定信息 T_i(= $g_1\hat{}\{k_{i1}\}$)。在该情况下，也可以从署名者用存储部件 21 中省略署名者确定信息 T_i。

[0171] 另外，组署名生成部件 25 根据署名者用存储部件 21 内的组公开密钥 gpk 和在步骤 ST32 ～ ST34 中得到的值 u_1、u_2、e，计算哈希值 $\alpha = H(u_1, u_2, e)$(ST35)。

[0172] 进而，组署名生成部件 25 根据该哈希值 α、在步骤 ST31 中得到的随机数 r、组公开密钥 gpk，计算值 $v = c^r d^{r\alpha}$(ST36)。

[0173] 由此，组署名生成部件 25 将针对署名者确定信息 T_i 得到的密码 (u_1, u_2, e, v) 保存在署名者用存储部件 21 中 (ST37)。

[0174] (零知识证明 (zero-knowledge proof) 计算处理 :图 12)

[0175] 接着，组署名生成部件 25 参照署名者用存储部件 21 内的素数位数 q，随机地选择用于隐藏成员秘密密钥 (k_{i1}, k_{i2}) 和在步骤 ST31 中得到的随机数 r 的随机数 r_1、r_2、$r_r \in Z_q$(ST41)。

[0176] 接着，组署名生成部件 25 根据署名者用存储部件 21 内的组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$、在步骤 ST41 中得到的随机数 r_1、r_2、r_r，计算零知识证明的一部分的参数 $A = g_1\hat{}\{r_1\} g_2\hat{}\{r_2\}$，$B = g_1\hat{}\{r_r\}$，$C = h\hat{}\{r_r\} g_1\hat{}\{r_1\}$(ST42 ～ ST44)。

[0177] 另外，组署名生成部件 25 根据署名者用存储部件 21 内的组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$、密码 (u_1, u_2, e, v) 和消息 msg、在步骤 ST42 ～ ST44 中得到的零知识证明的一部分的参数 A、B、C，计算哈希值 $\beta = H(g_1, g_2, h, u_1, u_2, e, v, A, B, C, msg)$(ST45)。

[0178] 进而，组署名生成部件 25 根据该哈希值 β、在步骤 ST41 中得到的随机数 r_1、r_2、r_r、署名者用存储部件 21 内的成员秘密密钥 k_{i1}，k_{i2} 和素数位数 q，计算其他零知识证明的一部分的参数 $s_1 = r_1 + \beta k_{i1} \bmod q$，$s_2 = r_2 + \beta k_{i2} \bmod q$，$s_r = r_r + \beta_r \bmod q$(ST46 ～ ST48)。

[0179] 由此，组署名生成部件 25 将最终得到的零知识证明 (A, B, C, s_1, s_2, s_r) 与密码 (u_1, u_2, e, v) 关联起来保存在署名者用存储部件 21 中 (ST49)，结束处理。以后，将这些密码 (u_1, u_2, e, v) 和零知识证明 (A, B, C, s_1, s_2, s_r) 用作组署名 $\sigma = (u_1, u_2, e, v, A, B, C, s_1, s_2, s_r)$。

[0180] 该组署名 σ 由署名者确定信息 T_i 的密码 (u_1, u_2, e, v)、表示是知道了以 g_1、g_2 为底的 f 的继承 k_{i1}，k_{i2} 的正确的用户的情况和正确地对与之对应的署名者确定信息 T_i 进行了加密的情况的零知识证明 (A, B, C, s_1, s_2, s_r) 组成。

[0181] 以后，署名者装置 20_i 根据署名者的输入部件 22 的操作，将署名者用存储部件 21 内的组署名 σ 和消息 msg 显示在输出部件 26 上，并从通信部件 23 发送到验证者装置 30。由此，不表示成员秘密密钥 k_{i1}，k_{i2}，就可以证明是属于组的正确的成员，并且组管理者可以确定署名者。

[0182] （署名验证处理：图 13）

[0183] 假设验证者装置 30 预先根据验证者的输入部件 32 的操作，从组管理者装置 10 取得公开参数 (q, G, g_1, H) 和组公开密钥 gpk = (g_1, g_2, f, c, d, h, H) 并保存在验证者用存储部件 31 中。由此，验证者装置 30 能够进行署名验证处理。

[0184] 在验证者装置 30 中，由通信部件 33 接收从署名者装置 20_i 发送的消息 msg、组署名 σ = (u_1, u_2, e, v, A, B, C, s_1, s_2, s_r) 和验证要求，保存在验证用存储部件 31 中，并且由通信部件 33 将该验证要求发送到署名验证部件 34。

[0185] 署名验证部件 34 如果接收到验证要求，则根据验证者用存储部件 31 内的组公开密钥 gpk、消息 msg 和组署名 σ，计算哈希值 β = H(g_1, g_2, h, u_1, u_2, e, v, A, B, C, msg) (ST51)。另外，署名验证部件 34 也可以根据规定的基准范围，确认组署名 σ 的值的范围。

[0186] 接着，署名验证部件 34 根据组公开密钥 gpk 和组署名 σ，对零知识证明的验证公式 A = f^{-β} g_1^{s_1} g_2^{s_2}，B = u_1^{-β} g_1^{s_r}，C = e^{-β} h^{s_r} g_1^{s_1} 是否成立进行验证 (ST52 ～ ST54)。

[0187] 如果步骤 ST52 ～ ST54 的结果是全部的验证公式 A、B、C 成立，则判断为有效 (valid)，向通信部件 33 和输出部件 35 输出判断结果 OK(ST55)，如果即使 1 个验证公式不成立，也判断为无效 (invalid)，向通信部件 33 和输出部件 35 输出判断结果 NG(ST56)。

[0188] 通信部件 33 向署名者装置 20_i 发送判断结果 OK/NG，结束处理。但是，通信部件 33 并不一定必须发送判断结果 OK/NG。输出部件 35 显示输出判断结果 OK/NG。

[0189] （署名者验证处理和署名者确定处理：图 14 和图 15）

[0190] 例如，说明由于发现不正常、为了服务使用费用的征收这样的情况，需要确定署名者的情况。

[0191] 组管理者装置 10 由通信部件 33 接收从验证者装置 30 发送的消息 msg、组署名 σ 和署名者确定要求，保存在管理者用存储部件 11 中，并且由通信部件 33 将该署名者确定要求发送到署名验证部件 16。

[0192] 署名验证部件 16 如果接收到署名者确定要求，则如图 14 所示，根据管理者用存储部件 11 内的组公开密钥 gpk、消息 msg 和组署名 σ，计算哈希值 β = H(g_1, g_2, h, u_1, u_2, e, v, A, B, C, msg) (ST61)。另外，署名验证部件 16 也可以根据规定的基准范围，确认组署名 σ 的值的范围。

[0193] 接着，署名验证部件 16 根据组公开密钥 gpk 和组署名 σ，对零知识证明的值 A = f^{-β} g_1^{s_1} g_2^{s_2}，B = u_1^{-β} g_1^{s_r}，C = e^{-β} h^{s_r} g_1^{s_1} 是否成立进行验证 (ST62 ～ ST64)。

[0194] 如果步骤 ST62 ～ ST64 的结果即使 1 个验证公式不成立，也判断为无效 (invalid)，由通信部件 33 输出判断结果 NG(ST65)。通信部件 33 向验证者装置 30 发送判断结果 NG，结束处理。

[0195] 另一方面，如果步骤 ST62 ～ ST64 的结果是全部成立，则判断为有效 (valid)，署名验证部件 16 根据组公开密钥 gpk 和组署名 σ，计算哈希值 α = (u_1, u_2, e) (ST66)。

[0196] 然后，署名验证部件 16 根据管理者用存储部件 11 内的组署名 σ = (u_1, u_2, e, v, A, B, C, s_1, s_2, s_r)、组秘密密钥 gmsk = (a, b, x_1, x_2, y_1, y_2, z) 和哈希值 α，验证验证公式 u_1^{x_1+y_1α} u_2^{x_2+y_2α} = v 是否成立 (ST67)，前进到步骤 ST65，结束处理。

[0197] 另一方面，如果步骤 ST67 的结果是验证公式成立，则判断为有效 (valid)，署名验证部件 16 将判断结果 OK 和署名者确定要求发送到署 名者确定部件 17，结束处理。

[0198] 署名者确定部件 17 如果接收到判断结果 OK 和署名者确定要求，则如图 15 所示，根据管理者用存储部件 11 内的组署名 σ 和组秘密密钥 gmsk，计算署名者确定信息 $T = e/u_1^z$ (ST71)，得到署名者确定信息 T(ST72)。

[0199] 接着，署名者确定部件 17 根据署名者确定信息 T，检索管理者用存储部件 11，将与署名者确定信息 T 对应的用户识别信息 ID(j)（其中 $1 \leqslant j \leqslant n$）输出到输出部件 18。进而，署名者确定部件 17 也可以根据用户识别信息 ID()，检索管理者用存储部件 11，将与用户识别信息 ID(j) 对应的用户信息输出到输出部件 18。

[0200] 输出部件 18 显示输出这些用户识别信息 ID(j) 和用户信息。

[0201] < 实施例方式的安全性 >

[0202] 在此，证明实施例方式的安全性。

[0203] [定理 1] 提案组署名方式在随机预言模型 (random oracle model) 中 DDH 问题是困难的假定下，是安全的。

[0204] [引理 1] 实施例方式具有正当性 (correctness)。

[0205] （证明）根据实施例方式的定义是明确的。

[0206] [引理 2] 实施例方式在随机预言模型中 DDH 问题是困难的假定下，具有匿名性 (anonymity)。

[0207] （证明方法）利用以无法无视实施例方式的匿名性的概率破解的对手 A^{anon}，构成以无法无视 DDH 问题的概率破解的对手 A^{DDH}。

[0208] 将向对手 A^{DDH} 的输入设为 (g_1, g_2, u_1, u_2)。

[0209] 如下这样模拟密钥生成算法 GKg。

[0210] 随机地选择 $x_1, x_2, y_1, y_2, z \in Z_q$。

[0211] 随机地选择 $i \in \{1, \cdots\cdots, n\}$。

[0212] 随机地选择 $k_{i1}, k_{i2} \in Z_q$。

[0213] 计算 $f = g_1\hat{}\{k_{i1}\} g_2\hat{}\{k_{i2}\}$。

[0214] 设 $T_i = g_1\hat{}\{k_{i1}\}$。

[0215] 针对 $j \in \{1, \cdots\cdots n\} \backslash \{i\}$，随机地选择 $T_j \in G$。

[0216] 计算 $c = g_1\hat{}\{x_1\} g_2\hat{}\{x_2\}$，$d = g_1\hat{}\{y_1\} g_2\hat{}\{y_2\}$，$h = g_1^z$。

[0217] 从通用单向性哈希函数的集合选择哈希函数 H。

[0218] 假设组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$、用户 i 的成员秘密密钥 $gsk[i] = (k_{i1}, k_{i2})$。

[0219] 如下这样模拟对用户 j 的收买询问 (corruption query) 的应答。

[0220] 在 $j = i$ 的情况下，返回 $gsk[i] = (k_{i1}, k_{i2})$，在指定了除此以外的用户的情况下，作为错误而结束。

[0221] 针对用户 j、消息 msg 的署名要求，如下这样模拟对署名询问 (signing query) 的应答。

[0222] 署名者确定信息的密码的部分进行 T_j 的 Cramer-Shoup 加密。

[0223] 非对话知识证明的部分进行利用了随机预言模型的模拟。这是一般的方法，因此

省略详细的说明。

[0224] 如下这样模拟查询者 (challenger)。

[0225] 随机地选择 $b \in \{0,1\}$。

[0226] 与 Cramer-Shoup 暗号的安全性证明一样地对署名者确定信息的密码的部分进行模拟。

[0227] 非对话知识证明的部分进行利用了随机预言的模拟。

[0228] 对于对手 A^{DDH}，在 $b = b'$ 的情况下输出 1，在除此以外的情况下输出 0。

[0229] 由于都正确地进行了上述模拟，所以以无法无视 DDH 问题的概率破解对手 A^{DDH}。

[0230] 但是，该对手 A^{DDH} 与 DDH 问题是困难的这样的假设相反。因此，作为前提的以无法无视匿名性的概率破解的对手 A^{anon} 不存在。

[0231] [引理 3] 实施例方式在随机预言模型中离散对数问题是困难的假定下，具有可跟踪性 (traceability)。

[0232] (证明方法) 利用以无法无视实施例方式的可跟踪性的概率破解的对手 A^{trace}，构成以无法无视离散对数问题的概率破解的对手 A^{DL}。

[0233] 将向对手 A^{DL} 的输入设为 (g_1, f)。

[0234] 如下这样模拟密钥生成算法 GKg。

[0235] 随机地选择 $i \in \{1, \cdots\cdots, n\}$。

[0236] 随机地选择 $k_{i1}, k_{i2} \in Z_q$。

[0237] 设 $g_2 = (f g_1^{\wedge}\{-k_{i1}\})^{\wedge}\{1/k_{i2}\}$。

[0238] 设 $T_i = g_1^{\wedge}\{k_{i1}\}$。

[0239] 针对 $j \in \{1, \cdots\cdots, n\} \backslash \{i\}$，随机地选择 $T_j \in G$。

[0240] 随机地选择 $x_1, x_2, y_1, y_2, z \in Z_q$。

[0241] 计算 $c = g_1^{\wedge}\{x_1\} g_2^{\wedge}\{x_2\}$，$d = g_1^{\wedge}\{y_1\} g_2^{\wedge}\{y_2\}$，$h = g_1^{z}$。

[0242] 从通用单向性哈希函数中选择哈希函数 H。

[0243] 设组公开密钥 $gpk = (g_1, g_2, f, c, d, h, H)$、用户 i 的成员秘密密钥 $gsk[i] = (k_{i1}, k_{i2})$。

[0244] 与匿名性 (anonymity) 的证明一样地模拟署名询问 (signingquery) 和收买询问 (corruption query) 的应答。

[0245] 通过回放 (rewind) 而得到 2 个不同的署名

[0246] $\sigma = (u_1, u_2, e, v, A, B, C, s_1, s_2, s_r)$

[0247] $\sigma' = (u_1', u_2', e', v', A', B', C', s_1', s_2', s_r')$。

[0248] 如果设 $\beta = H(g_1, g_2, h, u_1, u_2, e, v, A, B, C, msg)$、

[0249] $\beta' = H(g_1, g_2, h, u_1', u_2', e', v', A', B', C', msg)$，

[0250] $k_1' = (s_1 - s_1')/(\beta - \beta')$，$k_2' = (s_2 - s_2')/(\beta - \beta')$，则 $f = g_1^{\wedge}\{k_1'\} g_2^{\wedge}\{k_2'\}$。另外，根据可跟踪性的定义，$(k_1', k_2') \neq j(k_{i1}, k_{i2})$，因此 $g_2 = g_1^{\wedge}\{-(k_{i1} - k_1')/(k_{i2} - k_2')\}$ 成立。

[0251] 如果设 $-(k_{j1} - k_1')/(k_{i2} - k_2') = \Gamma$，则 $\log_{g\_1} f = k_{i1} + \Gamma k_{i2}$，对手 A^{DL} 能够以无法无视的概率求出离散对数。另外，下附的“_”表示下标。即，“$\log_{g\_1} f$”表示以 g_1 为底的 f 的对数。

[0252] 但是，该对手 A^{DL} 与离散对数问题是困难的这样的假定相反。因此，作为前提的以无法无视可跟踪性的概率破解的对手 A^{trace} 不存在。

[0253] ＜实施例方式的效率＞

[0254] 为了评价实施例方式的效率，考虑以作为通常的电子署名的 RSA 署名方式的署名生成的计算量为基准时的现有的组署名方式和实施例方式的计算量和数据长度。

[0255] 作为现有的组署名方式，与非常高速的 [CG04] 方式进行比较。[CG04] 方式即使与 [ACJT00] 方式相比，也是 26 倍以上的高速，另外，与利用了双线性映射 (bilinear map) 的方式 (参考 D.Boneh, X.Boyen, and H.Shacham,“Short group signatures”, In Proc.of CRYPTO 2004, LNCS 3152, pp.41 ～ 55,2004 和 J.Furukawa and H.Imai,“An efficientgroup signature scheme from bilinear maps”,In Proc.of ACISP 2005,LNCS 3574, pp.455 ～ 467,2005) 相比，也是高速的。

[0256] 首先，以下总结计算量的比较方法的考虑方法。

[0257] 所比较的方式的计算量的大部分与幂余数运算对应。因此，无视幂余数运算以外的计算量，着眼于幂余数运算的计算量。

[0258] 幂余数运算的计算量与 (除数的比特长度)^2× 幂指数的比特长度成正比，因此在除数的比特长度相同的情况下，全体的计算量与幂指数的比特长度的总和成正比。

[0259] 另外，在知道了除数的素因数分解的情况下，可以利用中国人剩余定理 (Chinese remainder theorem :CRT)，因此相对于不知道素因数分解的情况，在 RSA 模数 (modulus(n ＝ pq, p ;q :素数))

[0260] $p \approx q$ 公式 1

[0261] 的情况下，计算量成为 1/4 ～ 1/3 左右。在此，假设计算量为 1/4，来预测计算量。

[0262] 进而，通过利用作为幂运算的高速处理方法的指数同时乘法 (simultaneous multiple exponentiation) 法，能够以与成为 $max_i(\{e_i\}) = e_j$ 的 $g_j\hat{}\{e_j\}$ 的计算相同的程度处理 $\Pi_i g_i\hat{}\{e_i\}$ 的形式的计算。

[0263] 比较时的安全参数以利用了 [CG04] 方式的推荐参数的情况为基准。推荐参数利用了 2048 比特的 RSA 模数，因此在 RSA 方式中，同样利用 2048 比特的 RSA 模数。对于在实施例方式中利用的乘法巡回群 G，利用 Z_p^* 和椭圆曲线的 2 个。在 Z_p^* 下，利用设 p 为 2048 比特的素数、除尽 p-1 的 q 为 224 比特的素数时的位数 q 的 Z_p^* 的部分群。p、q 的值是在 FIPS(federal information processing standard)186-3 的说明书 (draft)(参考“March 13,2006 :Draft Federal Information Processing Standard(FIPS)186-3-Digital Signature Standard(DSS)”,http://csrc.nist.gov/publications/drafts.html(2007 年 6 月现在)) 中也将用的值，被看作是与 2048 比特的 RSA 模数相同程度的安全参数。在椭圆曲线上，利用根据作为与之等同的安全参数的 224 比特的素数生成的椭圆曲线。

[0264] 在考虑到以上情况的基础上，图 16 表示 RSA 署名方式、[CG04] 方式、本实施例方式的主要处理的计算量和数据长度。另外，署名生成计算量和署名验证计算量表示幂指数的比特长度的总和，在能够利用 CRT 的情况下，以 1/4 进行计算。RSA 方式的署名验证计算量依存于公开密钥 d 的长度，一般比较小。RSA 方式的署名密钥长度是在具有素数 p、q 和秘密密钥 e 的情况下的值。RSA 方式的验证密钥长度是减小了公开密钥 d 的情况下的值。

[0265] 本实施例方式的署名生成计算量是 RSA 方式的 3 倍，因此与 RSA 方式的约 8 倍的

[CG04] 方式相比，被抑制得低。因此，能够高速地执行本实施例方式的署名生成。

[0266] 本实施例方式的署名密钥长度（成员秘密密钥长度）是 RSA 方式的 1/9 倍，因此与 RSA 方式的约 1.1 倍的 [CG04] 方式相比，变短了。

[0267] 另外，本实施例方式的组秘密密钥长度比 [CG04] 方式长。但是，组秘密密钥长度的增加并不影响组管理者装置 10 以外的装置 20_1 ～ 20_n、30 的计算量，一般组管理者装置与高性能、高可靠的计算机等的署名者装置、验证者装置相比，计算量的制约少的情况多，实用上没有问题。

[0268] 另外，本实施例方式在以椭圆曲线暗号方式实现的情况下，署名长度成为 RSA 方式的 1.5 倍，因此与 [CG04] 方式相比，能够大幅地缩短署名长度。

[0269] 即，本实施例方式与 [CG04] 方式相比，署名密钥长度和验证密钥长度短，能够高速地执行署名生成和署名验证。理由是相对于本实施例方式是以素数位数 q 为除数的以完全离散对数为基础的方式，[CG04] 方式是以合成数 $n = pq$ 为除数的以 RSA 为基础的方式。

[0270] 例如，在以离散对数为基础的方式中，在 $y = g^x \bmod q$ 的计算中，在除数 q 是 2048 比特的情况下，离散对数 x 为 224 比特左右。

[0271] 另一方面，在以 RSA 为基础的方式中，在 $C = m^e \bmod n$ 的计算中，在除数 n 是 2048 比特的情况下，公开密钥 e 也为 2048 比特左右。因此，在以 RSA 为基础的 [CG04] 方式中，不可能进行本实施例方式那样的密钥长度的缩短和计算的高速化。

[0272] 根据上述那样的本实施例，作为使用素数位数 q 的乘法巡回群 G 完全以离散对数为基础的组署名方式，并且实现了以继承 k_{i1}、k_{i2} 为成员秘密密钥的组署名方式，由此与现有的 [CG04] 方式相比，能够减少计算量而提高计算速度。另外，“完全以离散对数为基础的组署名方式”是指使用素数位数 q 的乘法巡回群 G 作为乘法巡回群，而不利用位数未知的方式而只利用位数已知的方式的组署名方式。

[0273] 例如，根据本实施例，由于是完全以离散对数为基础的方式，所以如图 16 所示，在以 RSA 为基础的 [CG04] 方式中，在不可能的层次，能够非常高速地实现数据长度短的组署名方式。

[0274] 如果补足说明，在组管理者装置 10 中，通过在组公开密钥中包含值 g_1、g_2、f，能够高效地生成组署名。另外，通过在组秘密密钥中包含值 a、b，能够高效地生成成员数 n 个的成员秘密密钥。

[0275] 在署名者装置 20_i 中，通过使用基于继承的一部分 k_{i1} 的署名确定信息 T_i，能够高效地生成零知识证明。即，并不是继承自身，而是使用根据继承唯一计算的值作为署名者确定信息，因此能够提高零知识证明的生成和验证效率。

[0276] 在验证者装置 30 和组管理者装置 10 中，根据包含零知识证明的组署名 σ，能够高效地生成零知识证明，另外，能够高效地验证组署名 σ。

[0277] 进而，在组管理者装置 10 中，组署名 σ 包含署名者确定信息 T_i 的密码数据，由此只通过对密码数据进行解密就能够得到署名者确定信息 T_i，因此能够高效地确定署名者。

[0278] 另外，根据本实施例，能够实现基于 DDH 问题的最初的实用的组署名方式。

[0279] 另外，根据本实施例，由于署名生成中的幂运算的底是固定的，所以通过事前计算指数同时乘法法的计算表，能够高效地执行幂运算。

[0280] 另外，上述实施例所记载的方法可以作为能够使计算机执行的程序，存储在磁盘

（软盘（注册商标）、硬盘等）、光盘（CD-ROM、DVD 等）、光磁盘（MO）、半导体存储器等存储介质中而分发。

[0281] 另外，作为该存储介质，只要是能够存储程序并且计算机可读的存储介质，其存储形式可以是任意的形态。

[0282] 另外，也可以由根据从存储介质安装到计算机中的程序的指示而在计算机上运转的 OS（操作系统）、数据库管理软件、网络软件等 MW（中间件）等来执行用于实现上述实施例的各处理的一部分。

[0283] 进而，本发明的存储介质并不限于与计算机独立的介质，也包含下载通过 LAN、因特网等传送的程序而存储或暂时存储的存储介质。

[0284] 另外，存储介质并不只限于 1 个，从多个介质执行上述实施例的处理的情况也包含在本发明的存储介质中，介质结构可以是任意的结构。

[0285] 另外，本发明的计算机根据存储在存储介质中的程序，执行上述实施例的各处理，可以是由 1 台个人计算机等构成的装置、多个装置与网络连接的系统等的任意的结构。

[0286] 另外，本发明的计算机并不限于个人计算机，还包含信息处理设备所包含的计算处理装置、微型计算机等，是对能够根据程序实现本发明的功能的设备、装置的总称。

[0287] 另外，本申请发明并不限于上述实施例本身，在实施阶段可以在不脱离其宗旨的范围内对构成要素进行变形而具体化。另外，可以通过上述实施例所揭示的多个构成要素的适当组合来形成各种发明。例如，可以从实施例所示的全部构成要素中删除几个构成要素。进而，也可以适当地组合不同实施例的构成要素。

[0288] 根据以上说明的本发明，能够提供可以减少计算量提高计算速度的组署名系统、装置和程序。

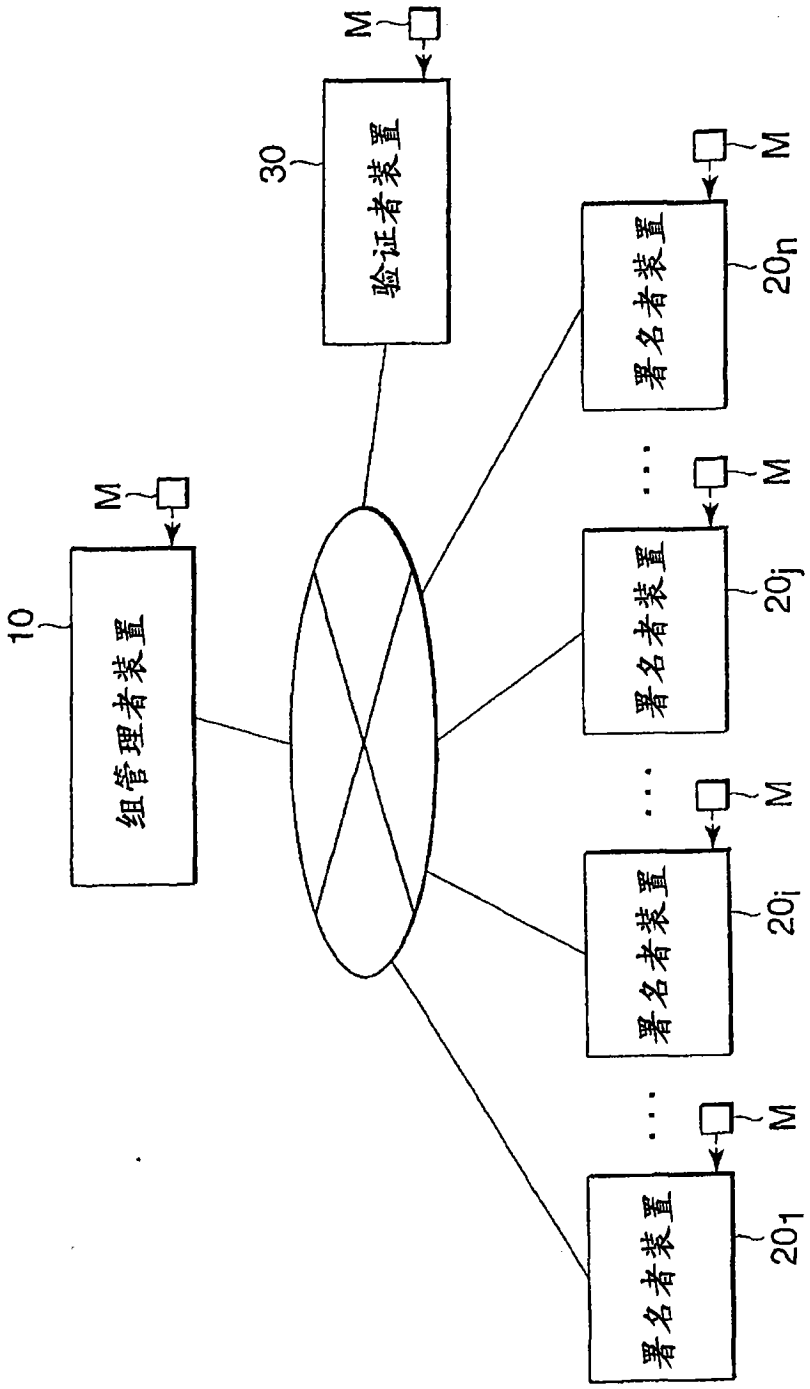

M
30
验证者装置
M
10
组管理者装置
M
署名者装置
20n
M
署名者装置
20j
M
署名者装置
20i
M
署名者装置
201

图 1

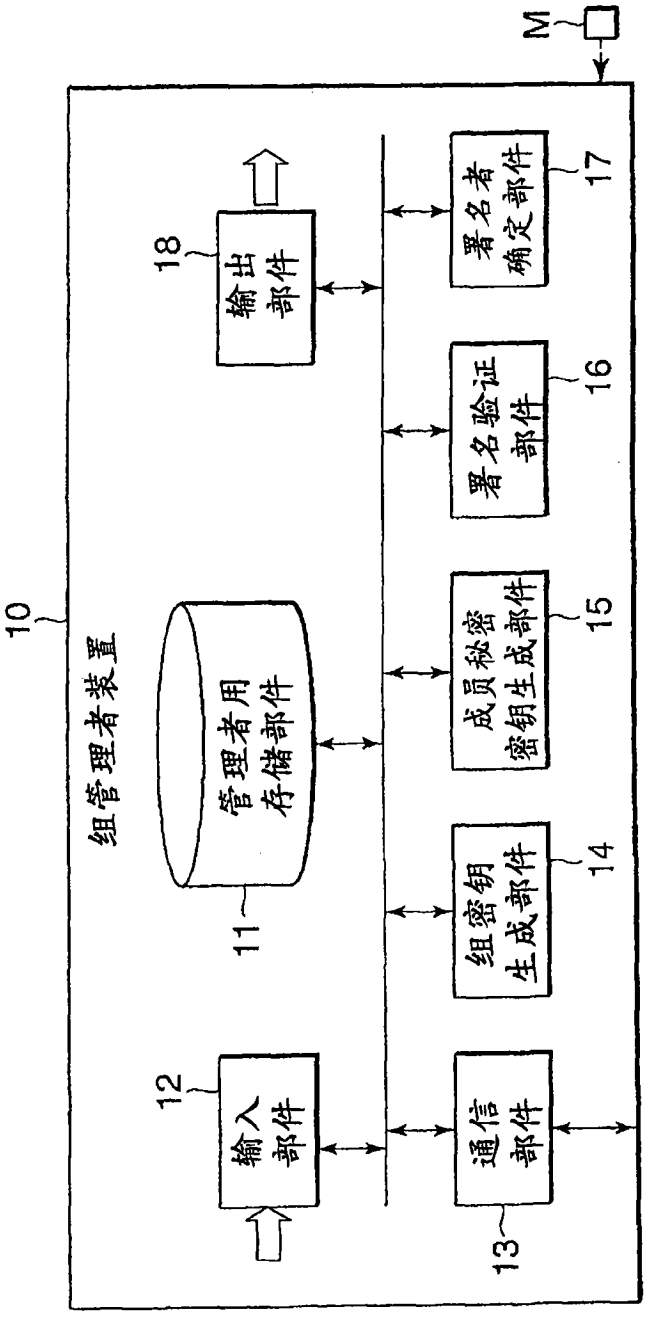

M
10
组管理者装置
18
输出部件
17
署名者确定部件
16
署名验证部件
15
成员秘密密钥生成部件
14
组密钥生成部件
11
管理者用存储部件
12
输入部件
13
通信部件

图 2

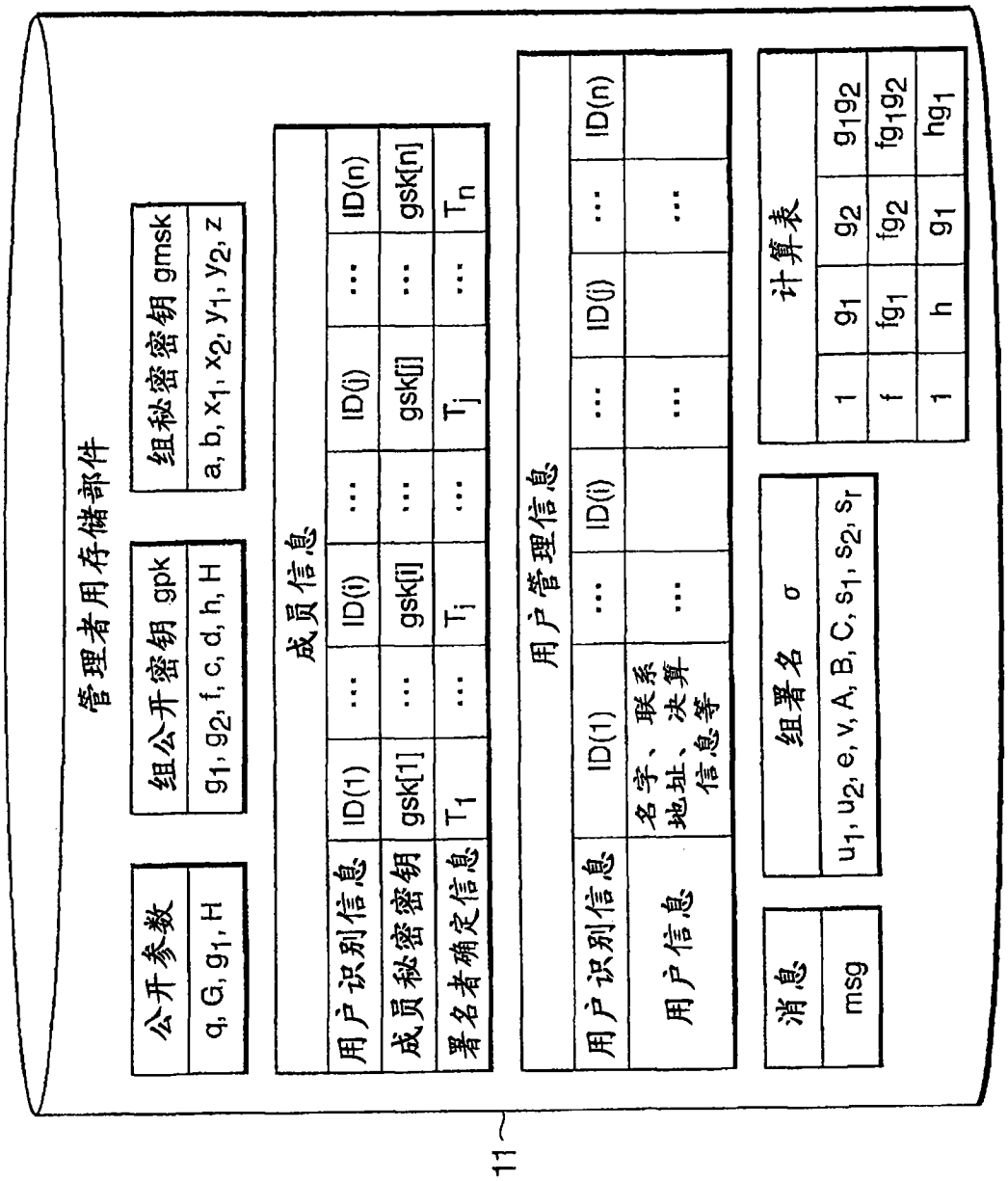

管理者用存储部件
公开参数
q, G, g1, H
组公开密钥 gpk
g1, g2, f, c, d, h, H
组秘密密钥 gmsk
a, b, x1, x2, y1, y2, z
成员信息
用户识别信息 ID(1) … ID(i) … ID(j) … ID(n)
成员秘密密钥 gsk[1] … gsk[i] … gsk[j] … gsk[n]
署名者确定信息 T1 … Ti … Tj … Tn
用户管理信息
用户识别信息 ID(1) … ID(i) … ID(j) … ID(n)
用户信息 名字、联系地址、决算信息等 … … …
消息
msg
组署名 σ
u1, u2, e, v, A, B, C, s1, s2, sr
计算表
1 g1 g2 g1g2
f fg1 fg2 fg1g2
1 h g1 hg1
11

图 3

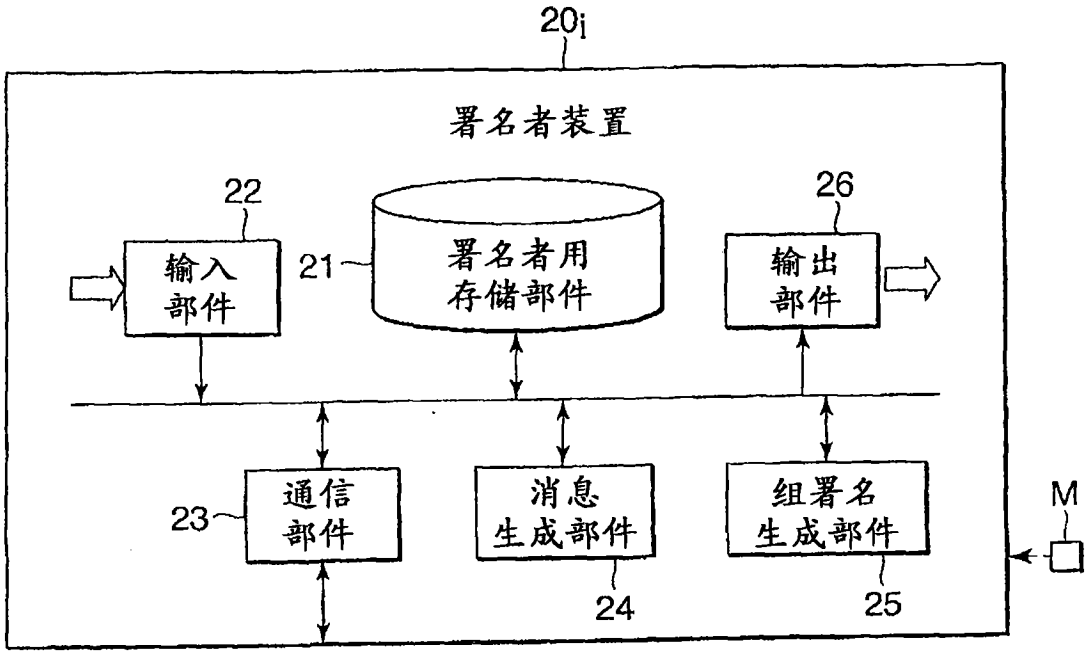

20i
署名者装置
22
输入部件
21
署名者用存储部件
26
输出部件
23
通信部件
消息生成部件
24
组署名生成部件
25
M

图 4

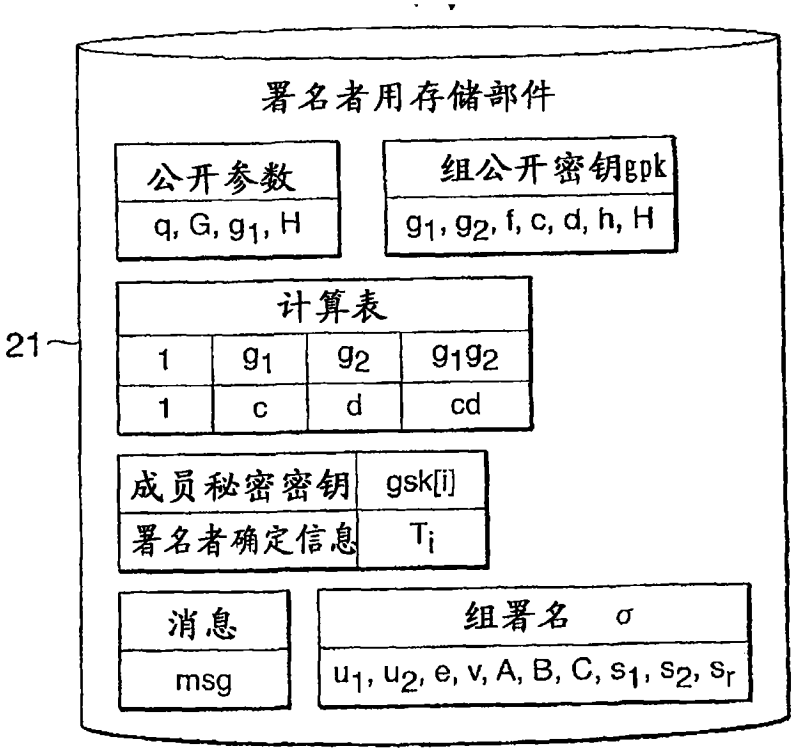

署名者用存储部件
公开参数
q, G, g1, H
组公开密钥gpk
g1, g2, f, c, d, h, H
21
计算表
1 g1 g2 g1g2
1 c d cd
成员秘密密钥 gsk[i]
署名者确定信息 Ti
消息
msg
组署名 σ
u1, u2, e, v, A, B, C, s1, s2, sr

图 5

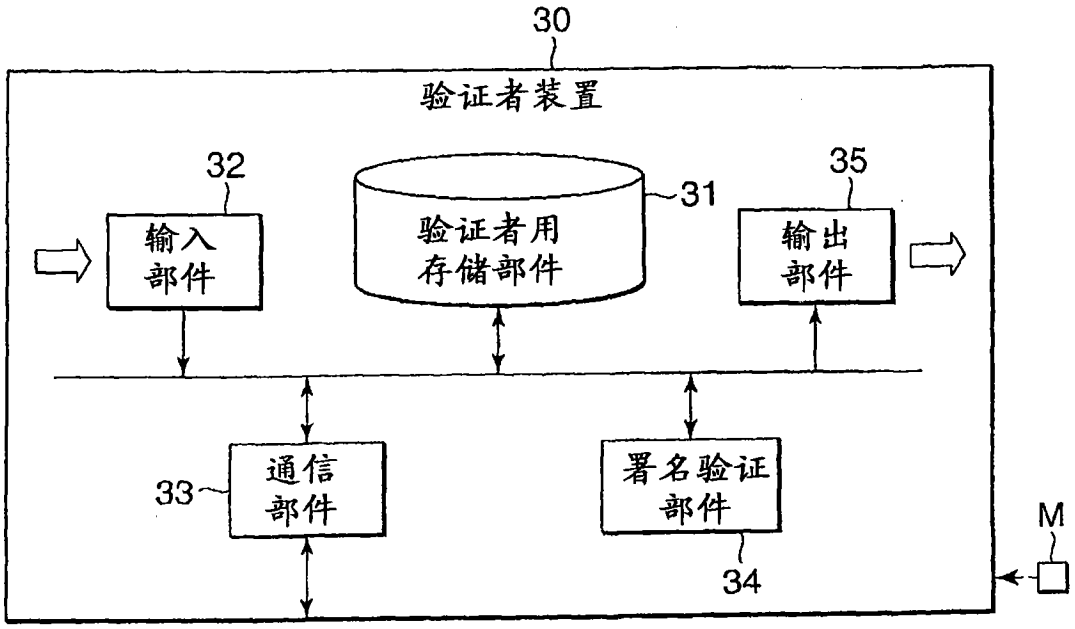

30
验证者装置
32
输入
部件
31
验证者用
存储部件
35
输出
部件
33
通信
部件
署名验证
部件
34
M

图 6

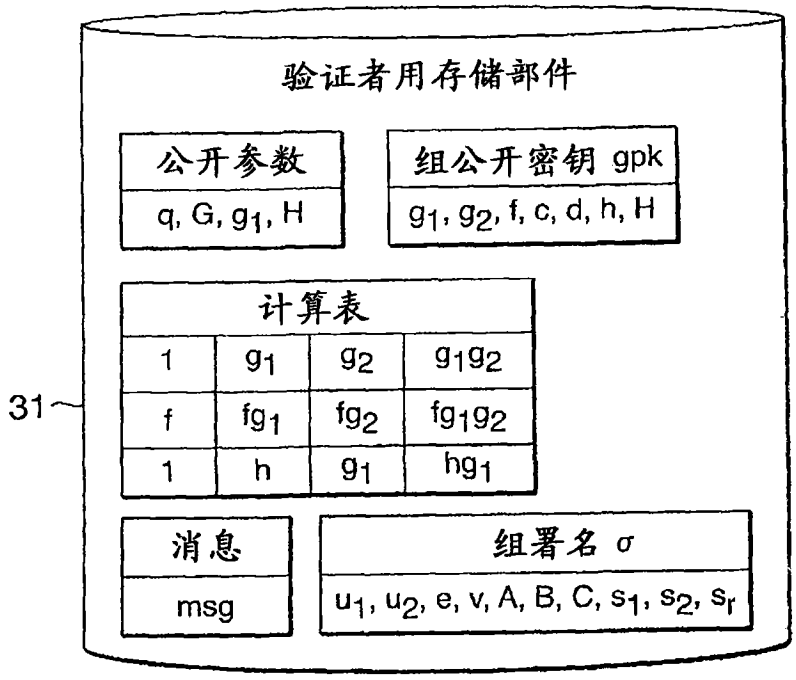

验证者用存储部件
公开参数
q, G, g1, H
组公开密钥 gpk
g1, g2, f, c, d, h, H
计算表
1 g1 g2 g1g2
f fg1 fg2 fg1g2
1 h g1 hg1
31
消息
msg
组署名 σ
u1, u2, e, v, A, B, C, s1, s2, sr

图 7

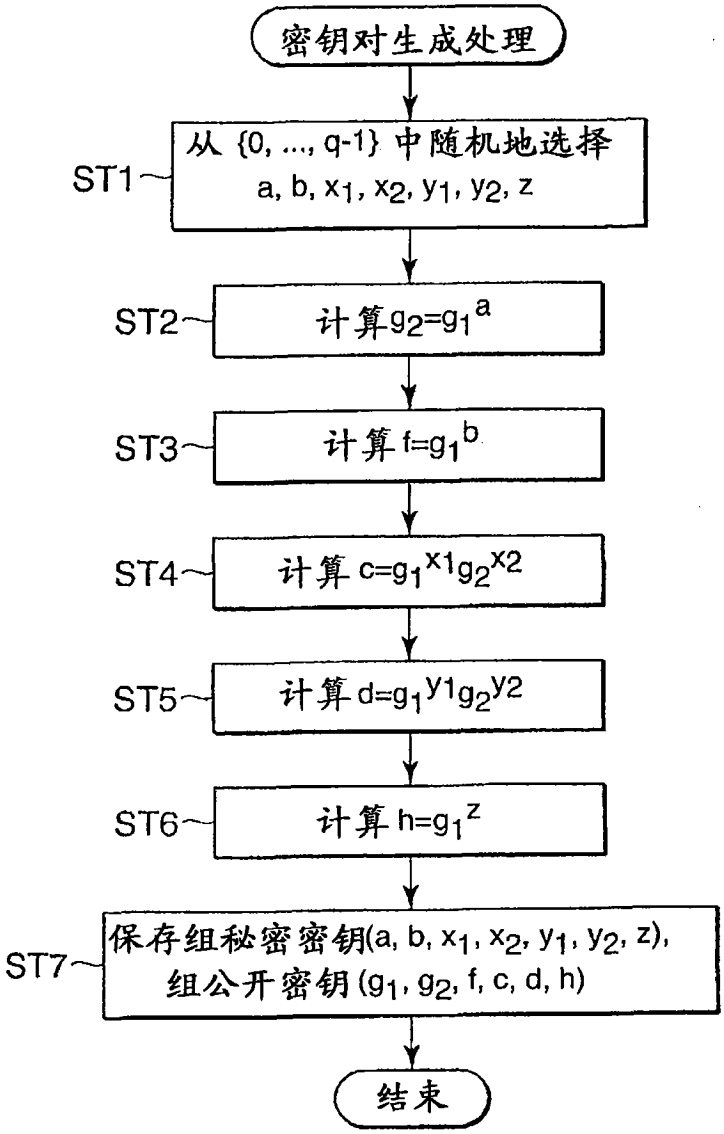

密钥对生成处理
ST1
从 {0, ..., q-1} 中随机地选择
a, b, x1, x2, y1, y2, z
ST2
计算g2=g1^a
ST3
计算 f=g1^b
ST4
计算 c=g1^x1g2^x2
ST5
计算 d=g1^y1g2^y2
ST6
计算 h=g1^z
ST7
保存组秘密密钥(a, b, x1, x2, y1, y2, z),
组公开密钥 (g1, g2, f, c, d, h)
结束

图 8

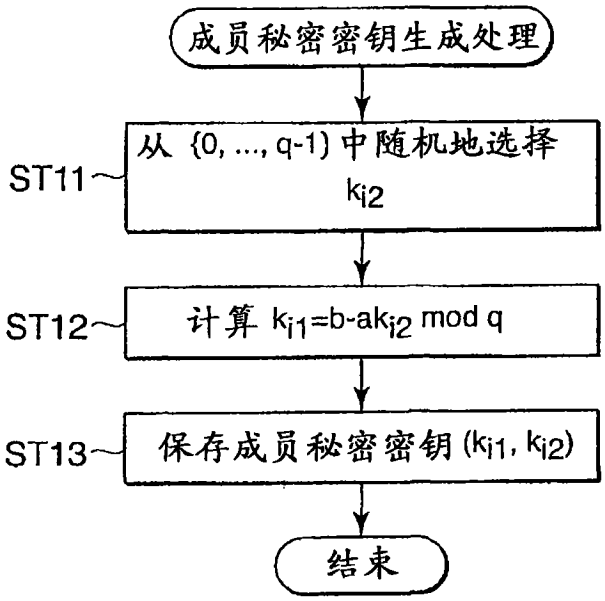

成员秘密密钥生成处理
ST11
从 {0, ..., q-1} 中随机地选择 k_{i2}
ST12
计算 $k_{i1}=b-ak_{i2} \bmod q$
ST13
保存成员秘密密钥 (k_{i1}, k_{i2})
结束

图 9

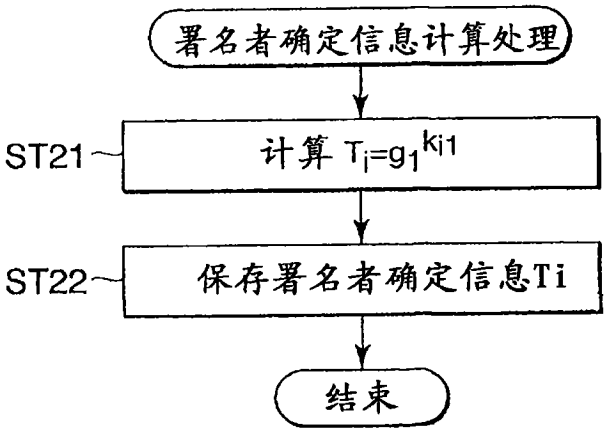

署名者确定信息计算处理
ST21
计算 $T_i=g_1^{k_{i1}}$
ST22
保存署名者确定信息Ti
结束

图 10

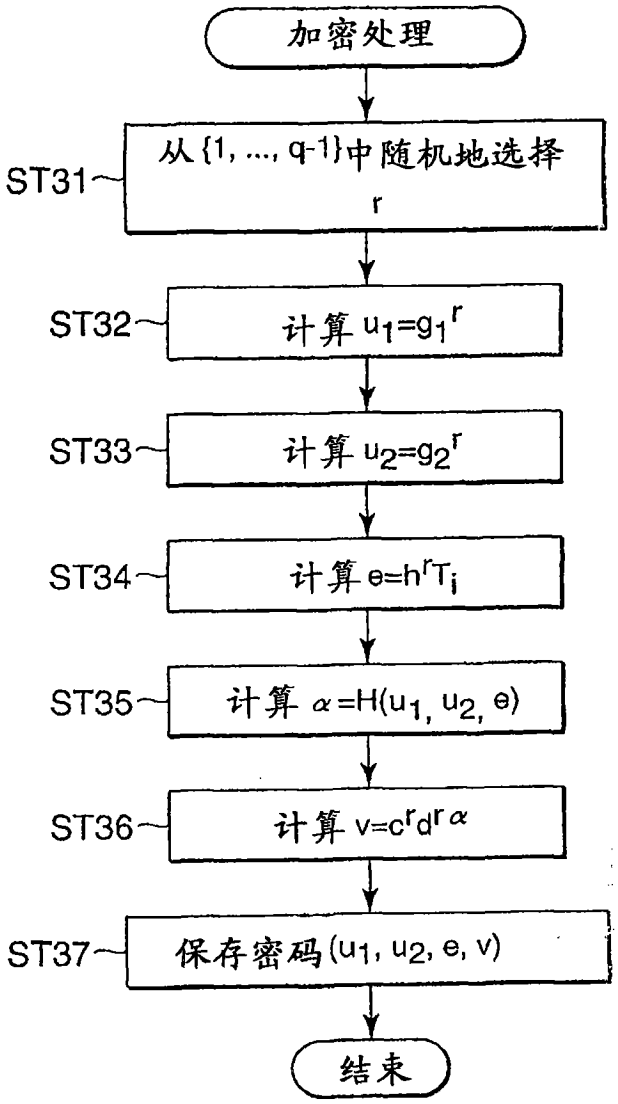

加密处理
ST31
从{1, ..., q-1}中随机地选择 r
ST32
计算 $u_1=g_1^r$
ST33
计算 $u_2=g_2^r$
ST34
计算 $e=h^rT_i$
ST35
计算 $\alpha=H(u_1, u_2, e)$
ST36
计算 $v=c^rd^r\alpha$
ST37
保存密码(u_1, u_2, e, v)
结束

图 11

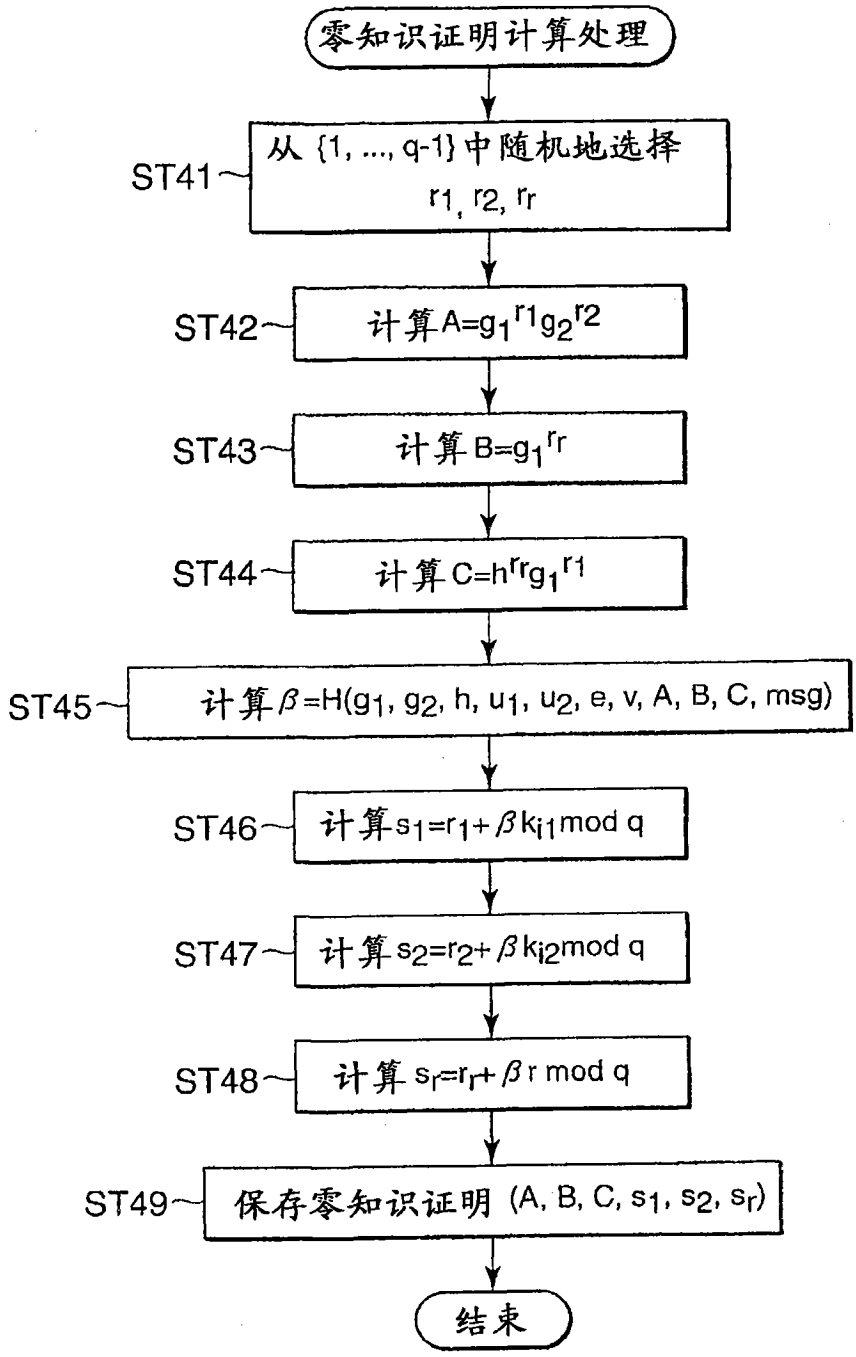

零知识证明计算处理
ST41
从 {1, ..., q-1} 中随机地选择 r1, r2, rr
ST42
计算 A=g1^r1 g2^r2
ST43
计算 B=g1^rr
ST44
计算 C=h^rr g1^r1
ST45
计算 β=H(g1, g2, h, u1, u2, e, v, A, B, C, msg)
ST46
计算 s1=r1+βki1 mod q
ST47
计算 s2=r2+βki2 mod q
ST48
计算 sr=rr+βr mod q
ST49
保存零知识证明 (A, B, C, s1, s2, sr)
结束

图 12

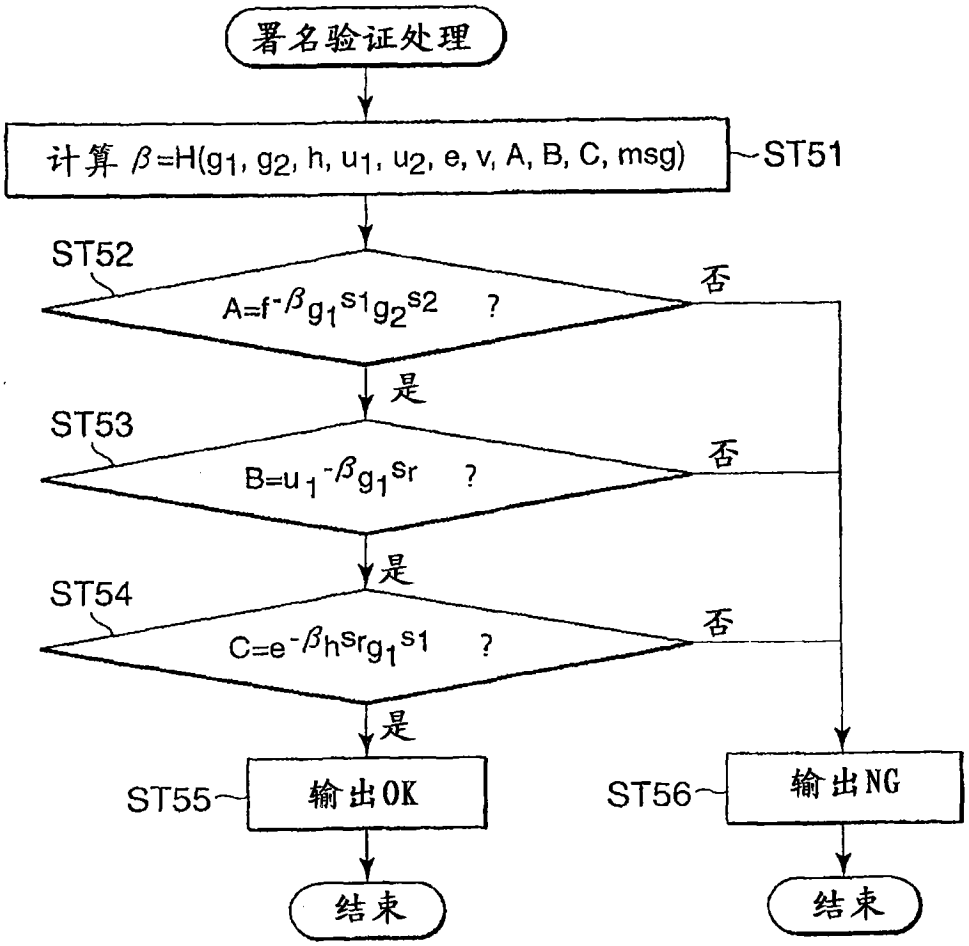

署名验证处理
计算 β=H(g1, g2, h, u1, u2, e, v, A, B, C, msg)
ST51
ST52
A=f-βg1s1g2s2 ?
否
是
ST53
B=u1-βg1sr ?
否
是
ST54
C=e-βhsrg1s1 ?
否
是
ST55
输出OK
ST56
输出NG
结束
结束

图 13

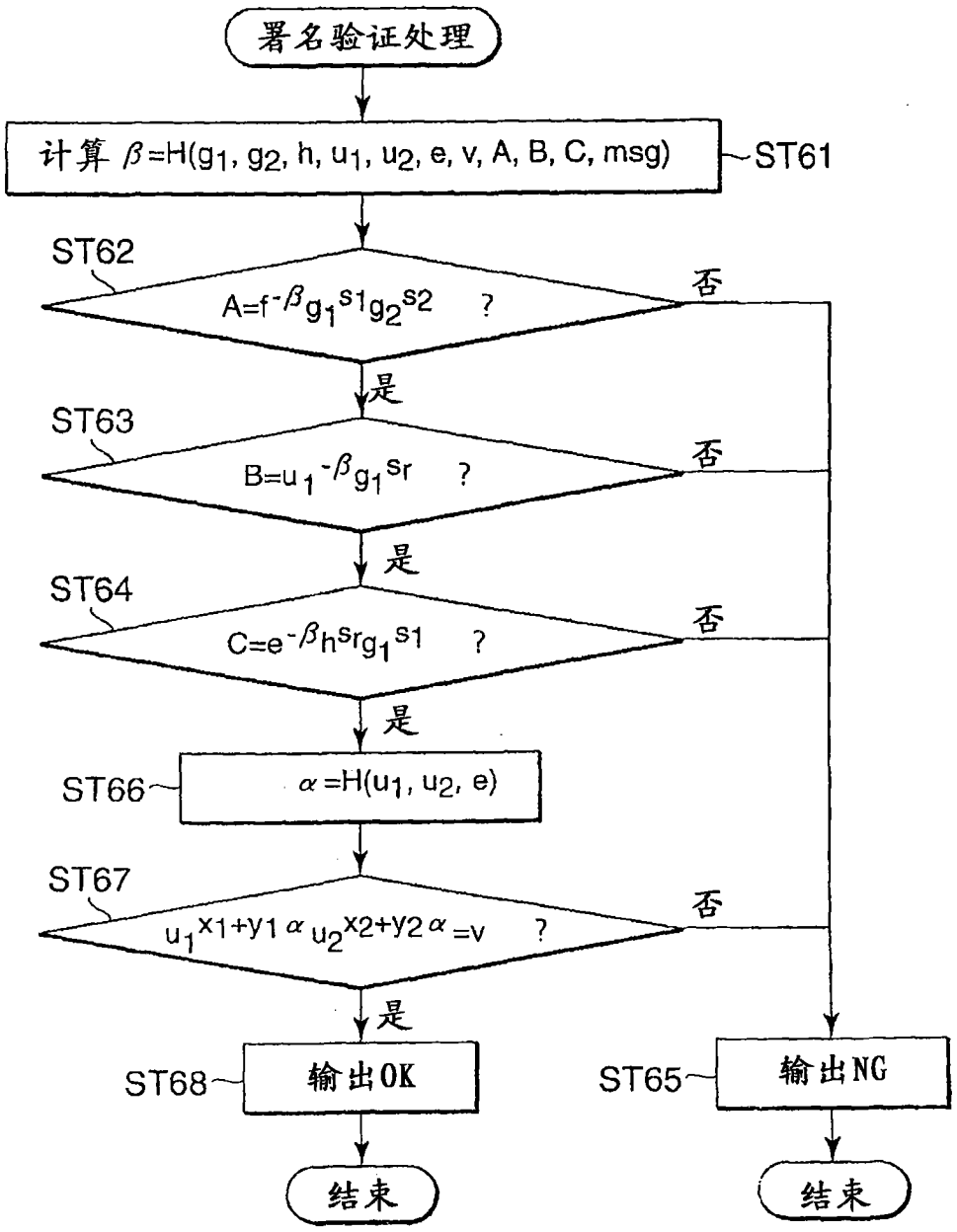

署名验证处理
计算 β=H(g1, g2, h, u1, u2, e, v, A, B, C, msg)
ST61
ST62
A=f^-β g1^s1 g2^s2 ?
否
是
ST63
B=u1^-β g1^sr ?
否
是
ST64
C=e^-β h^sr g1^s1 ?
否
是
ST66
α=H(u1, u2, e)
ST67
u1^x1+y1α u2^x2+y2α=v ?
否
是
ST68
输出OK
ST65
输出NG
结束
结束

图 14

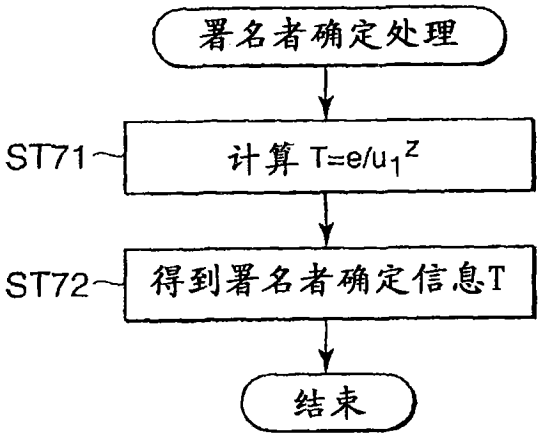


图 15

	通常署名	组署名		
	现有	现有	本实施例	
	RSA	[CG04]	Zp*	椭圆曲线
署名生成计算量	512	4180	1568	
署名验证计算量	小	2310	672	
署名密钥长度	4096	4438	448	448
验证密钥长度	≈2048	16666	12288	2688
组秘密密钥长度	—	282	1568	1568
署名长度	2048	12426	15008	3808

图 16