



[12] 发明专利说明书

专利号 ZL 200580035970.4

[45] 授权公告日 2009 年 10 月 14 日

[11] 授权公告号 CN 100551015C

[22] 申请日 2005.11.12

US5592552A 1997.1.7

[21] 申请号 200580035970.4

US6028933A 2002.2.22

[30] 优先权

CN1273490A 2000.11.15

[32] 2004.11.12 [33] KR [31] 10-2004-0092431

审查员 王 峥

[32] 2005.10.25 [33] KR [31] 10-2005-0100726

[74] 专利代理机构 北京铭硕知识产权代理有限公司

[32] 2005.11.8 [33] KR [31] 10-2005-0106604

代理人 韩明星 李友佳

[86] 国际申请 PCT/KR2005/003842 2005.11.12

[87] 国际公布 WO2006/052111 英 2006.5.18

[85] 进入国家阶段日期 2007.4.20

[73] 专利权人 三星电子株式会社

地址 韩国京畿道

[72] 发明人 金大烨 秦元镒 金焕俊 朴盛骏
千丁熙 金明煥 赵南洙 刘恩先

[56] 参考文献

US2002/133701A1 2002.9.19

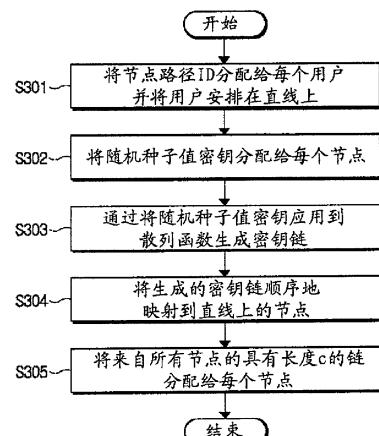
权利要求书 3 页 说明书 22 页 附图 5 页

[54] 发明名称

管理广播加密的用户密钥的方法

[57] 摘要

提供一种管理广播加密的用户密钥的方法，所述方法包括：向顺序排列的节点分配节点路径标识符(ID)；根据节点路径标 ID 向节点分配随机种子值密钥；通过将散列函数重复应用到分配的随机种子值密钥来生成密钥值；以及按照次序向节点分配生成的密钥值。因此，可将广播加密中最重要的传输开销减小到小于撤销用户的数目。此外，存在这样的优点：与作为当前已知的最好的方法的子集差分方法相比，本发明的示例性实施例的传输开销被显著地减小。



1、一种管理广播加密的用户密钥的方法，所述方法包括：

将节点路径标识符分配给按次序排列的节点；

根据节点路径标识符将随机种子值密钥分配给所述节点；

通过将散列函数重复地应用到分配的随机种子值密钥来生成密钥值；和

将生成的密钥值按次序分配给所述节点，其中，通过将散列函数重复应

用到分配给由按次序排列的 N 个节点形成的间隔中的第一节点的种子值密钥
N-1 次来生成所述由按次序排列的 N 个节点形成的间隔的加密密钥。

2、如权利要求 1 所述的方法，其中，所述间隔是一组连续的未撤销节点。

3、如权利要求 1 所述的方法，其中，所述间隔包括多于一个撤销节点，
并且将独立散列函数应用到所述撤销节点。

4、一种管理广播加密的用户密钥的方法，所述方法包括：

将随机种子值密钥分配给按次序排列的节点；

通过将第一散列函数重复地应用到分配的随机种子值密钥来生成第一密
钥值；

分配随机种子密钥值；

将第一密钥值按次序分配给所述节点；

在按次序排列的节点之中以特定间隔设置特殊节点；

将特殊种子值密钥分配给特殊节点；

通过将第二散列函数重复地应用到分配的特殊种子值密钥来生成第二密
钥值；和

将第二密钥值按次序分配给特殊节点。

5、如权利要求 4 所述的方法，其中，当将特殊节点密钥 K 分配给特殊
节点的第一特殊节点时，将通过将第二散列函数应用到特殊节点密钥 K 获得
的第二密钥值分配给位于以特定间隔远离第一特殊节点的第二特殊节点。

6、如权利要求 4 所述的方法，其中，通过将散列函数重复应用到分配给
由按次序排列的 N 个节点形成的特定间隔中的第一节点的种子值密钥 N-1 次
来生成所述由按次序排列的 N 个节点形成的特定间隔的加密密钥。

7、如权利要求 6 所述的方法，其中，所述间隔是一组连续的未撤销节点。

8、如权利要求 6 所述的方法，其中，所述间隔包括多于一个撤销节点，

并且将独立散列函数应用到所述撤销节点。

9、一种管理广播加密的用户密钥的方法，所述方法包括：

将节点路径标识符分配给配置为圆形群组的节点；

根据节点路径标识符将随机种子值密钥分配给所述节点；

通过将散列函数重复地应用到分配的随机种子值密钥来生成密钥值；和以循环的方式将生成的密钥值分配给所述节点，

其中，通过将散列函数重复应用到分配给圆形群组中的 N 个节点构造的循环间隔中的第一节点的种子值密钥 N-1 次来生成所述圆形群组中的 N 个节点构造的循环间隔的加密密钥。

10、如权利要求 9 所述的方法，其中，所述循环间隔是一组连续的未撤销节点。

11、如权利要求 9 所述的方法，其中，通过将配置新圆形群组的节点链接配置圆形群组的每个节点下面来形成分层结构的圆形群组。

12、如权利要求 11 所述的方法，其中，分层结构具有 16 层。

13、如权利要求 11 所述的方法，其中，圆形群组中的节点的数目是相同的。

14、如权利要求 9 所述的方法，其中，由圆形群组中的 N 个节点构成的循环间隔包括多于一个撤销节点，并且将独立散列函数应用到所述撤销节点。

15、如权利要求 9 所述的方法，其中，N 个节点形成圆形群组，并将节点路径标识符从 0 到 N-1 分配给所述 N 个节点。

16、如权利要求 11 所述的方法，其中，具有至少一个撤销节点的节点被视为分层结构中的撤销节点。

17、一种管理广播加密的用户密钥的方法，所述方法包括：

将随机种子值密钥分配给配置为圆形群组的节点；

通过将第一散列函数重复地应用到分配的随机种子值密钥来生成第一密钥值；

分配随机种子密钥值；

以循环方式将第一密钥值分配给所述节点；

在所述节点之中以特定间隔设置特殊节点；

将随机特殊种子值密钥分配给所述特殊节点；

通过将第二散列函数重复地应用到分配的特殊种子值密钥来生成第二密

钥值；和

以循环方式将第二密钥值分配给特殊节点。

18、如权利要求 17 所述的方法，其中，如果将特殊节点密钥 K 分配给特殊节点的第一特殊节点，则将通过将第二散列函数应用到特殊节点密钥 K 获得的第二密钥值分配给位于以特定间隔远离第一特殊节点的第二特殊节点。

19、如权利要求 17 所述的方法，其中，通过将散列函数重复应用到分配给圆形群组中的 N 个节点形成的间隔中的第一节点的种子值密钥 N-1 次来生成所述圆形群组中的 N 个节点形成的间隔的加密密钥。

20、如权利要求 19 所述的方法，其中，所述循环间隔是一组连续的未撤销节点。

21、如权利要求 19 所述的方法，其中，所述环形间隔包括多于一个的撤销节点，并且将独立散列函数应用到所述撤销节点。

管理广播加密的用户密钥的方法

技术领域

与本发明一致的方法涉及广播加密，更具体地讲，涉及管理广播加密的用户密钥。

背景技术

广播加密（BE）用于发送器（即，广播中心）以有效地将信息仅发送给全部用户中的期望用户。当一组用户接收到随机和动态改变的信息时，应有效地使用该方案。在 BE 中，最重要的是撤销或排除没有被许可的用户（例如，撤销用户或过期用户）。

图 1 是示出使用一般广播加密方案的数据传输系统的网络结构的概图。参照图 1，内容产生器 100 产生各种可用的数据（包括音频或视频数据）内容，并将产生的数据内容提供给服务提供器 110。服务提供器 110 向授权用户广播从内容产生器 100 提供的数据内容（例如，移动数字权限管理（DRM）网络 140 和智能家庭 DRM 网络 150），所述授权用户为通过各种有线或无线通信网络提供的相应的数据内容的支付费用。

也就是说，服务提供器 110 可经由卫星 120 将数据发送给配备各种卫星接收器的诸如机顶盒 141 的用户设备，服务提供器 110 也可通过移动通信网络将数据发送给移动通信终端 142。此外，提供器 110 可通过互联网 130 将数据发送到智能家庭 DRM 网络 150 中的各种终端 150、151、152、153、154 以及 155。

同时，为了使没有付费的撤销用户 160 不能使用数据，使用广播加密方案加密数据。

在这种加密/解密系统中的安全通常取决于加密密钥管理方案。此外，在这种加密密钥管理方案中，最重要的是如何获取加密密钥。同时，管理并更新获取的加密密钥也是很重要的。

自从在 1991 年首次提出该概念以来，已对 BE 进行了多次改变，假设用户在当前 BE 方案中用户处于无状态。这意味着即使会话改变，每个用户的

秘密密钥也永远不会被改变或被更新。顺便地，术语“ k 复原”(k -resilient)用于安全，其表示即使所有撤销用户中的 k 个撤销用户串通，撤销用户也不能恢复数据。如果 r 是撤销用户的数目，则术语“ r 复原”表示即使所有撤销用户串通也不存在安全问题。

同时，BE 的另一主要问题是最小化传输开销、存储开销和计算开销，分别表示将由发送器发送的头的长度、用户密钥的大小和用户获得会话密钥计算所需的计算时间。具体地说，其中最重要的问题是减小传输开销。在传输开销与总用户的数目 N 成比例时，其一般与撤销用户的数目成比例。因此传输开销随着 r 减少而减小。由于已开发了传输开销与 r 成比例的方案，因此将传输开销减小至小于 r 变为重要的问题。

在公布的 BE 方案中，D.Naor、M.Naor 和 J.Lospiech 的子集差分 (SD) 方法(模型)显得最为有效。在 SD 方法中，当总用户的数目为 n 时，存储开销为 $O(\log^{3/2} n)$ ，传输开销为 $O(2r-1)$ 。

然而，当存在许多用户时，SD 方法在效率上也是不利的。

如上所述，自从 1991 年以来已提出了各种算法。在它们之中，秘密共享方案、子集自由覆盖 (cover-free) 系统模型方案和基于树结构方案是最重要的算法。

首先，下面将示意性地描述秘密密钥共享方法。秘密密钥共享方法由 S.Berkovits 在 1991 年提出，并在 2000 年由 M.Noar 和 B.Pinkas 发表的名为“Efficient Trace and Revoke Schemes”的论文中做出了改进。S.Berkovits 在名为“How to Broadcast a Secret”的论文中提出了多项式内插法和基于向量的秘密密钥共享方法。

在多项式内插法中，中心(即，广播中心或发送器)通过秘密信道将点 (x_i, y_i) 发送到每个用户。此时，所有的 x_i 彼此不同，并且点 (x_i, y_i) 是每个用户的秘密密钥。其后，为了使中心通过会话向 t 个授权用户广播秘密信息 S ，选择 $t+j+1$ 次多项式 P 和随机整数 j 。多项式 P 是关于作为授权用户的秘密密钥的点 (x_i, y_i) 、不是任何其他授权用户的秘密密钥的随机选择的 j 个点 (x, y) 和点 (O, S) 的多项式表达式。此外，中心发送关于多项式 P 但不包含在所述 $(t+j)$ 个点中的任何点。其后，由于 t 个授权用户除了所述 $(t+j)$ 个点之外还多知道一个点(他们自己的秘密密钥)，所以他们可获得 $t+j+1$ 次多项式 P 并且还可对秘密信息 S 解密。然而，撤销的点仅知道 $(t+j)$

个点，因此他们不能获得多项式 P。

该方法具有大约 $O(t+j+1)$ 的传输开销、 $O(1)$ 的存储开销以及 t^3 倍的计算开销。因此，该方法具有这样的优点：可容易地撤销未授权的用户并避免撤销用户串通，并且还可进行叛逆者追踪。然而，该方法也具有这样的缺点：由于其对于大量的用户没有效率并且在重复使用该方法多次以后安全性变得更弱，因此不能进行实际地使用。在 M.Noar 和 B.Pinkas 的名为“Efficient Trace and Revoke Schemes”的论文中提出的方案中使用了使用 Lagrange 内插公式的阈值秘密共享方案。Noar-Pinkas 提出的方案使用这样的概念：可使用关于 $(r+1)$ 次的多项式的 $(r+1)$ 个点来恢复 $(r+1)$ 次的多项式表达式，但不能使用 r 个点（即，缺少一个点）来恢复 $(r+1)$ 次的多项式。也就是说，中心选择任意的 t 次多项式 P，并给每个用户关于多项式 P 的每个都不同的点作为秘密密钥。当 r 个用户被撤销时，中心发送总共 t 个点，即，作为撤销用户密钥的 r 个秘密密钥和为撤销用户任意选择的 $(t-r)$ 个点。结果，由于撤销用户仅知道包括他们/她们的秘密密钥的 t 个点，因此撤销用户不能恢复多项式 P。同时，由于没有被撤销的用户知道 $(t+1)$ 个点，因此所述用户可以恢复多项式 P。通过这个多项式 P 可获得会话密钥 P(0)。

该方法还具有这样的优点：可容易地进行撤销，并且可避免撤销用户串通。此外，该方法具有显著的优点：可添加新的用户，并且传输开销 $O(t)$ 和存储开销 $O(1)$ 具有相当好的效率。然而，该方法还具有这样的问题：不能撤销大于 t 个的用户， t 是最初确定的数目。此外，该方法在很多情况下有时效率低，这是因为被传输的点的数目和计算多项式的计算开销取决于 t 。此外，由于随着 t 变得更大，计算时间动态增加，因此该方案不适合具有大量的用户的情况。

其次，当一组总用户 S 包含多个子集时，可使用子集自由覆盖系统模型。可通过使用子集自由覆盖系统执行 BE。然而，因为存储开销和传输开销变为大约 $O(r \log n)$ ，所以该系统没有效率。此外，通过扩展 1 复原模型提出了 k 复原模型。由于可容易地设计有效的 1 复原技术，因此上述扩展看起来是有意义的，但是在使用到目前为止的方法进行扩展过程期间，效率降低地相当大。

第三，基于树结构的方法最近吸引了公众的注意。尽管在 1998 年，C.K.Wang、M.Gouda 和 G.S.Lam 提出了逻辑树层级 (LTH) 方法，但是其很

难在一个会话中撤销大量的用户。此外，由于在该方法中用户秘密密钥随会话改变而改变，因此其对于假设接收机处于无状态的最新的 BE 是不适用的。随后，在 2001 年，D.Noar、M.Noar 和 J.Lotspeich 提出了完备子集（CS）覆盖方案和 SD 方案。在两种方法中，给定 n 是总用户的数目， r 是撤销用户的数目，中心构造具有高度 ($\log n$) 的二元树，并向二元树的每个节点分配秘密密钥。此外，向每个用户分配每个节点。

第一，考虑 CS 覆盖方案，每个用户从中心接收位于从根节点开始到其自己的叶的它的路径上的节点的所有秘密密钥，并存储它们。这里，包括没有撤销用户的子树被称为 CS。此时，可通过适当地集合 CS 形成不包括任何撤销用户的树结构构造。当中心通过使用 CS 的根节点的每个秘密密钥对每个会话密钥加密，并将加密的会话密钥发送到相应的 CS 时，授权用户可恢复会话密钥，但是由于撤销用户不包括在任何 CS 中，所以其不能恢复会话密钥。

图 2 是示出密钥分配方法遵循基于树结构的模型的现有技术的广播加密的概念的树结构。参照图 2，一组用户 220 分别被排列在相应的节点 32 到 47，接收通过使用广播加密方案加密的数据。在其节点 32 到 47 上的用户分别具有他们唯一的密钥和分别具有在树结构中链接到他们的节点的所有节点的密钥。

例如，节点 34 上的用户具有节点 17、节点 8、节点 4 和节点 2 的密钥以及他/她的自己的密钥。也就是说，提供给节点 34 上的用户的节点 17 的密钥与节点 35 上的用户共享。以同样地方式，提供给节点 34 上的用户的节点 8 的密钥与节点 32、33、35 上的用户共享。

同时，在授权节点 32 到 47 上的所有用户的情况下，可通过将具有包含节点 2 的密钥的头的相同数据发送给所有的用户来执行数据传输以保持数据安全。

然而，如果具有最初分配给节点 36 上的用户 221 的密钥的用户是撤销用户，则由于用户 221 的密钥与其他用户共享，因此应更新与用户 221 的密钥有关的所有密钥。也就是说，应更新节点 18、节点 9、节点 4 和节点 2 的密钥。此时，从最低级的节点到最高级的节点向上进行密钥的更新。

第一，由于与用户 210 相应的节点 18 的密钥与节点 37 上的用户共享，因此中心将与用户 210 相应的节点 18 的更新的密钥加密，并将其发送到节点

37 上的用户。与用户 205 相应的节点 9 的密钥与位于与节点 37 上的用户以及位于与用户 211 相应的节点 19 的较低级的节点 38 和 39 的用户共享。因此，当将节点 9 上的用户 205 的更新的密钥应用到较低级的节点 37、38 和 39 时，节点 18 上的用户 210 的预先更新的密钥将被加密，并被发送到节点 37 上的用户。同时，节点 19 的更新的密钥将被加密，并被发送到节点 38 和 39 上的用户。

以同样的方式，由于与用户 202 相应的节点 4 的密钥与作为与用户 204 相应的节点 8 的下游节点的节点 32 到 35 的用户和作为与用户 205 相应的节点 9 的下游节点的节点 37 到 39 上的用户共享，以将与用户 202 相应的节点 4 的预先更新的密钥应用到节点 32 到 35，因此与用户 204 相应的节点 8 的更新的密钥被加密并被发送到节点 32 到 35。同时，与用户 205 相应的节点 9 的更新的密钥被加密，并被发送到节点 37 到 39。

最后，由于与用户 201 相应的节点 2 的密钥与作为与用户 202 相应的节点 4 的下游节点的节点 32 到 35 以及 37 到 39 上的用户和作为与用户 203 相应的节点 5 的下游节点的节点 42 到 47 上的用户共享，以将与用户 201 相应的节点 2 的预先更新的密钥应用到节点 32 到 35、37 到 39 以及 42 到 47，因此与用户 202 相应的节点 4 的更新的密钥被加密并被发送到节点 32 到 35 以及 37 到 39。同时，与用户 203 相应的节点 5 的更新的密钥被加密，并被发送到节点 40 到 47。通过这样的密钥更新过程，可避免撤销用户（或过期用户）访问广播的数据。

在该 CS 模型中的传输开销是所有 CS 的数目 $O(r \log(n/r))$ ，其中，CS 不包括任何撤销用户。此外，存储开销是 $O(\log n)$ 。

同时，SD 模型是上述 CS 模型的改进，并且已显著地改进了传输开销。也就是说，在 SD 方法中，传输开销为 $O(2r-1)$ ，存储大小为 $O(\log^2 n)$ 。在 SD 模型中，假设存在以节点 v 为根的第一子树。子树具有用作第二子树的根的节点 w。此时，我们可认为第三子树包括以节点 v 为根的第一子树中的所有叶，但是不包括以节点 w 为根的第二子树中的叶。第三子树中的所有叶被视为授权用户，第二子树中的所有叶被视为撤销用户。在存在包括合理数目的授权用户和少数撤销用户的一组用户的情况下，对于这种 SD 方法仅需要一个子集，不像 CS 方法需要至少两个子集。在 SD 方法中，被获得的阻断节点 v 和节点 w 之间的路径的节点分配的密钥的散列值被获得，并且获得的散列

值被用作会话密钥。也就是说，每个节点具有阻断根节点和他/她的自己的节点之间的路径的每个节点的兄弟节点的散列值作为秘密密钥。因此，由于散列函数的单项属性使得仅授权用户可恢复会话密钥。此时，SD 模型的传输开销最大为 $O(2r-1)$ ，存储开销为 $O(\log^2 n)$ ，并且计算开销最大为 $O(\log n)$ 。

其后，在 2002 年提出了从 SD 模型改进的 LSD 模型。在 LSD 模型中，通过将层结构应用到每个子树将存储开销减小到 $O(\log^{3/2} n)$ ，但是传输开销变为 SD 模型的两倍。

发明公开 技术问题

在上述 BE 模型中最有效的模型是基于树结构的模型，诸如 LSD、SD 等。然而，由于在基于树结构的方法中广播所需的子集的数目在相当程度上取决于用户的位置，因此不期望显著的改进。此外，基于树结构的 BE 模型具有这样的缺点：它们需要相当大的维护成本。因此，需要除了上述基于树结构的模型以外的更有效的 BE 模型。

技术解决方案

本发明的一方面在于提供一种管理广播加密的用户密钥的方法，所述方法按照次序对每个节点顺序地构造单向密钥链，并通过使用直线结构分发密钥。

本发明的另一方面在于提供一种管理广播加密的用户密钥的方法，所述方法标记直线上的所有节点中的第 c 个节点，然后将标记的节点设置为特殊节点，并从特殊节点密钥开始生成特殊节点链。

本发明的另一方面在于提供一种管理广播加密的用户密钥的方法，所述方法能够通过定义间隔来设置间隔以包括一个撤销用户来降低传输开销。

根据本发明的一方面，提供一种管理广播加密的用户密钥的方法，所述方法包括：将节点路径标识符（ID）分配给按次序排列的节点；根据节点路径 ID 将随机种子值密钥分配给所述节点；通过将散列函数重复地应用到分配的随机种子值密钥来生成密钥值；和将生成的密钥值按次序分配给所述节点。

可通过将散列函数重复应用到分配给间隔中的第一节点的种子值密钥 N-1 次来生成由按次序排列的与 N 有关个节点形成的间隔的加密密钥。

所述间隔可以是一组连续的未撤销节点。

所述间隔可包括多于一个撤销节点，并且将独立散列函数应用到所述撤销节点。

根据本发明的一方面，提供一种管理广播加密的用户密钥的方法，所述方法包括：将随机种子值密钥分配给按次序排列的节点；通过将第一散列函数重复地应用到分配的随机种子值密钥生成密钥值；将生成的密钥值按次序分配给所述节点；在按次序排列的节点之中以特定间隔设置特殊节点；将特殊种子值密钥分配给特殊节点；通过将第二散列函数重复地应用到分配的特殊种子值密钥生成密钥值；和将生成密钥值按次序分配给特殊节点。

当将特殊节点密钥 K 分配给特殊节点的第一特殊节点时，可将通过将第二散列函数应用到特殊节点密钥 K 获得的第二密钥值分配给位于以特定间隔远离第一特殊节点的第二特殊节点。

可通过将散列函数重复应用到分配给特定间隔中的第一节点的种子值密钥 N-1 次来生成由按次序排列的与 N 有关个节点构造的间隔的加密密钥。

所述间隔可以是一组连续的未撤销节点。

所述间隔可包括多于一个撤销节点，并且将独立散列函数应用到所述撤销节点。

根据本发明的一方面，提供一种管理广播加密的用户密钥的方法，所述方法包括：将节点路径标识符 (ID) 分配给配置为圆形群组的节点；根据节点路径 ID 将随机种子值密钥分配给所述节点；通过将散列函数重复地应用到分配的随机种子值密钥生成密钥值；和以循环的方式将生成的密钥值分配给圆形群组中的节点。

可通过将散列函数重复应用到分配给间隔中的第一节点的种子值密钥 N-1 次来生成圆形群组中的与 N 有关个节点构造的循环间隔的加密密钥。

所述循环间隔可以是一组连续的未撤销节点。

可通过将配置新圆形群组的节点链接配置圆形群组的每个节点下面来构造分层结构的圆形群组。

分层结构可以具有 16 层。

各个圆形群组中的节点的数目可以是相同的。

所述由圆形群组中的与 N 有关个节点构造的循环间隔可包括多于一个的撤销节点，并且将独立散列函数应用到所述撤销节点。

与 N 有关个节点可构造圆形群组，并将节点路径 ID 从 0 到 N-1 分配给所述与 N 有关个节点。

具有至少一个撤销节点的节点可被视为分层结构中的撤销节点。

根据本发明的一方面，提供一种管理广播加密的用户密钥的方法，所述方法包括：将随机种子值密钥分配给构造圆形群组的节点；通过将第一散列函数重复地应用到分配的随机种子值密钥生成密钥值；以循环方式将生成的密钥值分配给构造圆形群组的节点；在构造圆形群组的节点之中以特定间隔设置特殊节点；将随机特殊种子值密钥分配给所述特殊节点；通过将第二散列函数重复地应用到分配的随机特殊种子值密钥来生成密钥值；和以循环方式将生成的密钥值分配给特殊节点。

当将特殊节点密钥 K 分配给特殊节点的第一特殊节点时，将通过将第二散列函数应用到特殊节点密钥 K 获得的密钥值分配给位于以特定间隔远离第一特殊节点的第二特殊节点。

可通过将散列函数重复应用到分配给间隔中的第一节点的种子值密钥 N-1 次来生成由按次序排列的与 N 有关个节点构造的间隔的加密密钥。

所述循环间隔可以是一组连续的未撤销节点。

所述环形间隔可包括多于一个撤销节点，并且将独立散列函数应用到所述撤销节点。

有益的效果

如上所述，根据本发明，可将广播加密中最重要的传输开销减小到小于 r。此外，存在这样的优点：与作为当前已知的最好的方法的 SD 方法相比，本发明的示例性实施例的传输开销显著地减小。

此外，根据本发明，存在这样的优点：即使很多用户串通也不可能得到新的密钥，并且由于使用通过非法的解码器产生的串通用户的密钥，因此可进行叛逆者追踪。

附图说明

通过结合附图对本发明的特定示例性实施例进行的描述，本发明的上述和/或其它方面将会变得更加清楚，其中：

图 1 是示出使用一般广播加密方案使用的数据传输系统的网络结构的概

图；

图 2 是示出根据现有技术的广播加密的概念的树结构；

图 3 是示出根据本发明示例性实施例的通过将单向密钥链映射到每个节点上来分配密钥的过程的流程图；

图 4 是示出根据本发明示例性实施例的将随机种子值密钥分配给直线结构上的每个节点的方法的示图；

图 5 是示出根据本发明示例性实施例的将单向密钥链映射到直线结构上的每个节点的方法的示图；

图 6 是示出根据本发明示例性实施例的将密钥分配给直线结构上的每个节点的方法的示图；

图 7 是示出根据本发明示例性实施例的将密钥分配给直线结构上的每个节点的结果的示图；

图 8 是示出根据本发明示例性实施例的将会话密钥发送到位于两个撤销用户之间的用户的过程的流程图；

图 9 是示出根据本发明示例性实施例的在直线结构上定义间隔的示图；

图 10 是示出根据本发明示例性实施例的将会话密钥发送到直线结构的间隔的方法的示图；

图 11 是示出根据本发明示例性实施例的使用由每个节点的用户接收的会话密钥解密数据的过程的流程图；

图 12 是示出根据本发明的第一修改示例性实施例的在直线结构中定义特殊节点的示图；

图 13 是示出根据本发明的第一修改示例性实施例的将密钥分配给直线结构上的每个节点的方法的示图；

图 14 是示出根据本发明的第一次修改示例性实施例的划分发送会话密钥间隔的方法的示图；

图 15 是示出根据本发明的第一次修改的示例性实施例的当将间隔划分为多个子间隔时发送会话密钥的方法的示图；

图 16 是示出根据本发明的第二修改示例性实施例的定义间隔的方法的示图；

图 17 是示出根据本发明的第二修改示例性实施例的将密钥分配给直线结构上的每个节点的方法的示图；

图 18 是示出根据本发明的第四修改示例性实施例的将密钥分配给圆形结构上的每个节点的方法的示图；以及

图 19 示出根据本发明示例性实施例的具有圆形节点群组的分层结构的。

最佳实施方式

将参照附图来详细描述本发明的特定示例性实施例。

基本示例性实施例

图 3 是示出根据本发明示例性实施例的通过将单向密钥链映射到直接结构的每个节点上来分配密钥的过程的流程图。参照图 3，将节点路径标识符 (ID) 分配给每个节点 (S301)。节点路径 ID 用于标识与每个节点相应的每个用户。

接下来，根据每个节点的节点路径 ID 将随机种子值密钥分配给直线结构上的每个节点 (S302)。在本发明示例性实施例中，可独立地确定随机种子值密钥。

通过将单向散列函数应用到分配给每个节点的随机种子值密钥来生成密钥值。重复地将单向散列函数应用到生成的密钥值以生成连续密钥值。其后，生成根据各个随机种子值密钥的密钥 (散列) 链 (S303)。

这里，单向散列函数是将任意长度的输入值转换为固定长度的输出值的函数。单向散列函数具有以下特点：(1) 不能从给出的输出值计算原始输入值；(2) 不能找到能够产生与给出的输入值相同的输出值的另一输入值；以及 (3) 不能找到产生相同输出值的两个不同的输入值。

如上所述，这种散列函数是请求数据完整性、验证以及不可否认关键函数的一种。在本发明示例性实施例中，单向散列函数可以是“HBES SHA-1”。

接下来，将在步骤 S303 从各个种子值密钥生成的密钥值顺序地分配给从分配了各个种子值密钥的节点的下一节点开始的节点 (S304, S305)。在本发明示例性实施例中，对于每个装置分配密钥值的方向应一致。

其后，将参照图 4 到图 6 更详细地描述密钥分配过程。

图 4 是示出根据本发明示例性实施例的将随机密钥分配给直线结构上的每个节点的方法的示图。参照图 4，可将随机种子值密钥从第一节点逐个地映射到直线上的每个节点。

例如，假设在直线上排列 N 个节点，将随机选择的种子值密钥 K_1 ，

$K_2, \dots K_N$ 分别地分配给节点。也就是说，将密钥 K_1 分配给第一节点 401，将密钥 K_2 分配给第二节点 402，将密钥 K_3 分配给第二节点 403，将密钥 K_4 分配给第二节点 404，... 将密钥 K_{N-1} 分配给第 (N-1) 节点 405，将密钥 K_N 分配给第 N 节点 406，其中， K_1 到 K_N 是随机选择的。

通过将单向散列函数应用到种子值密钥来构造单向密钥链。下面是构造单向密钥链的方法。

令 h 为单向散列函数 $\{0,1\}^{128} \rightarrow \{0,1\}^{128}$ 。从密钥 K 开始的具有长度 C 的单向密钥链为 $\{K, h(K), h(h(K)) = h^{(2)}(K), \dots, h^{(c-1)}(K)\}$ 。将构造的单向密钥链中的密钥顺序地分配给直线上的每个节点。

图 5 是示出根据本发明示例性实施例的将单向密钥链映射到直线结构上的每个节点的方法的示图。参照图 5，通过将单向散列函数 h 应用到每个密钥来构造从每个节点密钥开始的具有长度 c 的单向密钥链，并将构造的单向密钥链中的密钥映射到每个节点。这里， c 表示链大小。

因此，第 i 节点 501 与种子值密钥 K_i 相映射，第 $(i+1)$ 节点 502 与 $h(K_i)$ 相映射，第 $(i+2)$ 节点 503 与 $h(h(K_i))$ 相映射，...，第 $(i+c-1)$ 节点 504 与 $h^{(c-1)}(K_i)$ 相映射。

在本发明示例性实施例中，单向密钥链的长度 c 被预定，并且每个用户存储的密钥的数目取决于长度 c 。因此，可由分配给各个节点的所有种子值密钥从所有的节点开始构造具有长度 c 的单向密钥链，并且可将每个构造的单向密钥链中的密钥分配给各个节点。因此，每个节点将具有与 c 有关个密钥。此时，位于直线的两端部分附近的一些节点可具有小于 c 的密钥数目。

图 6 示出根据本发明示例性实施例的将每个密钥分配给直线结构上的每个节点相应的方法。参照图 6，将种子值密钥 K_i 分配给第 i 节点 601。同时将通过以密钥 K_i 运算单向散列函数 h 获得的密钥 $h(K_i)$ 和已分配给第 $(i+1)$ 节点 602 自己的密钥 K_{i+1} 分配给第 $(i+1)$ 节点 602。此外，将通过将单向散列函数 h 应用到分配给节点 $(i+1)$ 的密钥获得的密钥 $h(K_{i+1})$ 和第 $(i+2)$ 节点 603 自己的密钥 K_{i+2} 分配给第 $(i+2)$ 节点 603。

也就是说，将通过两次应用单向散列函数获得的密钥 $h(h(K_i))$ 、通过将单向函数 h 应用到 K_{i+1} 获得的密钥 $h(K_{i+1})$ 和第 $(i+2)$ 节点 603 自己的密钥 K_{i+2} 分配给第 $(i+2)$ 节点 603。以同样方式，将密钥 $h^{(c-1)}(K_i), h^{(c-2)}(K_{i+1}), h^{(c-3)}(K_{i+2}), \dots, K_{i+c-1}$ 分配给作为从第 i 节点开始的第 c 节点的第 $(i+c-1)$ 节点

605。

因此，根据每个用户的位置通过将与 c 有关个密钥之一分配给与每个节点相应的每个用户作为其秘密密钥。

假定 $K_{i,i} = K_i$, $K_{i,j} = h^{(j-i)}(K_{i,j})$, $i \leq j$, 则被设置为由用户 u_i 存储的密钥可由下面的等式 1 表示。

等式 1

$$u_i = \{K_{ki} \mid 0 \leq i - k \leq c, k \geq 1\}$$

此外，根据等式 1 分配给各个节点的密钥与图 7 所示的表中的密钥相同。图 7 是示出根据本发明示例性实施例的分配给直线结构上的每个节点的密钥的示图。参照图 7 可知：与 c 有关个密钥（图 7 中的密钥 701）被分配给用户 u_c 。

此外，在本发明中，可考虑将所有用户划分为至少一个子集的方案，并且在该方案中，会话密钥与消息一起被发送到每个子集。

图 8 是示出根据本发明示例性实施例的将会话密钥发送到两个撤销用户之间的间隔的过程的流程图。参照图 8，将放置于撤销用户之间的一组连续的用户定义为发送会话密钥的间隔（S801）。接下来，会话密钥被发送到与每个子集相应的每个间隔（S802）。

此时，放置于两个撤销用户之间的一个间隔期望这样的情况：撤销用户被连续的排列。因此，至多可以将会话密钥发送到 $(r+1)$ 个间隔。然而，当间隔的最大长度为 c 时，在间隔长于 c 时传输开销变得更大。

现在对设置连续地排列授权用户的间隔的示例性方法进行描述。在用户 U_1 到 U_{10} 被呈现，并且用户 U_5 是撤销用户，同时间隔的最大长度被限制在 5 的情况下，建立从 U_1 到 U_4 的一个间隔和从 U_6 到 U_{10} 的另一间隔。

图 9 是示出根据本发明示例性实施例的在直线结构上定义间隔的示图。参照图 9，将位于两个撤销用户 901 和 903 之间的一组连续的授权用户定义为间隔 902。

同时，在设置上述间隔之后，定位从用户 U_i 的节点密钥 K_i 开始的单向密钥链（S803）。其后，使用定位的单向密钥链的最后的密钥 $h^{(s)}(K_i)$ 对会话密钥 SK 加密，然后将其发送到相应的间隔（S804）。最后，发送加密消息（S805）。

下面的方法将更详细。为了将会话密钥 SK 发送到间隔 $\{u_i, u_{i+1}, u_{i+2}, \dots, u_{i+s}\}$ （这里， s 小于 c ），中心使用从用户 U_i 的节点密钥 K_i 开始的单向密钥链。通

过使用从节点密钥 K_i 开始的单向密钥链中的密钥 $h^{(s)}(K_i)$ 对会话密钥 SK 加密，其中，密钥 $h^{(s)}(K_i)$ 相应于用户 u_{i+s} ，并且将加密的会话密钥发送到所述间隔。也就是说，当 $E(K, M)$ 是使用密钥 K 的秘密密钥加密算法时，消息 $E(h^{(s)}(K_i), SK)$ 被发送到所有用户。

上述能够基于预先分配的密钥对发送的消息解密的用户仅是可获得密钥 $h^{(s)}(K_i)$ 的用户。因此，仅间隔 $\{u_i, u_{i+1}, u_{i+2}, \dots, u_{i+s}\}$ 中的用户可获得相应的密钥。

也就是说，由于间隔中的用户知道从密钥 K_i 开始的单向密钥链中的一个密钥，并且该密钥位于 $h^{(s)}(K_i)$ 的左侧，因此用户可通过将单向函数 h 应用到他/她的密钥来获得 $h^{(s)}(K_i)$ 。

相反，没有在间隔中的用户中的间隔左侧的用户不能获得与密钥 K_i 相关的密钥，从而他们不能获得密钥 $h^{(s)}(K_i)$ 。此外，即使间隔右侧的用户可获得单向密钥链中的一些密钥，由于单向函数的单向性，他们也不能获得位于单向密钥链左侧的密钥。

因此，尽管不在相应间隔中的特定叛逆者串通，他们也不可能获得密钥 $h^{(s)}(K_i)$ 。因此，他们不能对解密会话密钥解密。

图 10 是示出根据本发明示例性实施例的将会话密钥发送到直线结构中的间隔的方法的示图。参照图 10，根据本发明示例性实施例，可以同时地将会话密钥 SK 发送到间隔中的用户。

也就是说，假设撤销用户分别位于第 $(i-1)$ 节点 1001 和第 $(i+t+1)$ 节点 1005，并且 $(t+1)$ 个连续授权用户 1002、1003 和 1004 位于两个撤销用户之间，则可以仅对授权用户发送仅一个秘密密钥。也就是说，假设 $E(K, m)$ 是以 K 为密钥的秘密密钥加密方案，则用户 u_i, \dots, u_{i+1} 的会话密钥的头可被表示为下面的等式 2。

$$\text{头} = E(h^{(t)}(K_i), SK) \quad \text{等式 2}$$

图 11 是示出根据本发明示例性实施例的每个节点上的用户通过使用从中心接收的会话密钥对数据解密的过程的流程图。参照图 11，根据上述方法仅授权用户可使用从中心发送的密钥对接收的数据解密。也就是说，当接收包括加密头的消息的每个用户处于相应的间隔时 (S1102)，用户通过使用他/她的自己的密钥运算 $h^{(s)}(K_i)$ 来执行解密 (S1103)。相反，由于不在相应的间隔中的每个用户不能运算 $h^{(s)}(K_i)$ ，因此其不能对接收的数据解密。

更具体地说，在图 10 中，由于位于第 i 节点 1002 的左侧的用户不能获得密钥 K_i ，因此其不能获得密钥 $h^{(i+t)}(K_i)$ 。此外，尽管位于第 $(i+t)$ 节点的右侧的用户可获得从密钥 K_i 开始的单向密钥链的在右侧部分的密钥，但由于单向散列函数的单向性特性他们也不能获得密钥 $h^{(i+t)}(K_i)$ 。

另一方面，在间隔中的所有授权用户通过重复地将单向散列函数 h 应用到基于他们自己的密钥中的密钥 K_i 获得的密钥可获得密钥 $h^{(t+i)}(K_i)$ 。

同时，在存在包括 r 个撤销用户的总共 N 个用户的情况下，传输开销可如下产生。

首先，每个用户应存储 c 个或更少的密钥。此时，在最坏的情况下，传输开销为 $\{r+(N-2r)/c\}$ 个密钥。这种情况发生在当所有的撤销用户聚集在直线上的一个部分并且授权用户只集中在另一部分时。当连续地安置两个或更多的撤销用户时，传输开销降低。因此，应考虑交替地安置撤销用户和授权用户的情况。此时，由于通过一次传输可发送密钥的间隔的最大长度被设置为 c ，因此额外需要 N/c 。

此外，用户的计算开销变为最多 c 次的单向函数运算和一次秘密密钥算法的运算。在 $N = 1000000$ 并且 $r = 50000$ 的情况下，通过下面的表 1 获得计算开销。

表 1

C (存储成本)	传输开销 (最坏的情况)	比例
50	50000+18000	1.36r
100	50000+9000	1.18r
200 (大约 3K)	50000+4500	1.09r

其后，将在下面描述本发明的基本示例性实施例的修改。在基本示例性实施例中，由于间隔的长度被限制在 c ，因此存在传输开销变得大于 r 的问题。因此，第一修改示例性实施例是基于间隔被设置地具有长于 c 的长度的想法，从而通过一次传输将密钥发送给较长的间隔。

此外，第二修改示例性实施例将新的单向函数应用到撤销用户的节点，以便将传输开销减小为小于 r 。此外，第三修改示例性实施例是通过组合第一和第二修改示例性实施例获得的方法。

第一修改示例性实施例

在上述基本示例性实施例中，因为间隔的长度被限制在 c ，所以传输开

销大于 r 。因此，为了将传输开销减小为与 r 差不多，提出通过一次传输将密钥发送到比 c 长的间隔的第一修改示例性实施例。

在本发明第一修改示例性实施例中，以特定间隔（例如每第三个节点）设置特殊节点。其后，将随机选择的特殊种子值密钥和不同于现有的种子值密钥分配给各个特殊节点，并且构造从一个特殊节点密钥开始的特殊节点链。

图 12 是示出根据本发明的第一修改示例性实施例的在直线结构上定义的特殊节点的方法的示图。参照图 12，为每第 c 节点设置特殊节点 1201、1202 和 1203。分别向特殊节点 1201、1202 和 1203 分配新的特殊种子值密钥，通过应用这些密钥构造具有长度 $c \times c_2$ 的单向密钥链。

更具体地说，新的特殊种子值密钥是随机选择的，并且被分别分配给特殊节点 1201、1202 和 1203，通过应用新的单向散列函数为各个特殊种子值密钥构造从每个特殊节点开始的特殊节点链。

此时，特殊节点链具有长度 $c \times c_2$ ，其中， c_2 为新的常数。以下是通过使用构造的特殊节点链分别将密钥分配给所有节点的方法。

图 13 示出根据本发明的第一修改示例性实施例的将密钥分配给直线结构上的相应节点的方法。在第一修改示例性实施例中构造密钥链的方法基本上与上述基本示例性实施例中的方法相同。假设间隔 $\{u_i, u_{i+1}, u_{i+2}, \dots, u_{i+s}\}$ 从特殊节点开始并被排列在直线上的超出长度 c 的范围内，则通过从节点 u_i 的密钥开始的特殊节点密钥链执行对这一间隔的密钥分配。在这个修改示例性实施例中，对 SK 加密的方案与本发明的基本示例性实施例的对 SK 加密的方案相同。也就是说，使用与从 u_i 的密钥开始的特殊节点密钥链中与密钥中的节点 u_{i+s} 相应的密钥对 SK 加密，然后将其发送到间隔 $\{u_i, u_{i+1}, u_{i+2}, \dots, u_{i+s}\}$ 中的每个节点。

参照图 13，当将特殊节点密钥 K 分配给的第一特殊节点 1301（第 c 节点）时，将通过以特殊节点密钥 K 运算单向函数 h_2 1309 获得的特殊节点密钥 $h_2(K)$ 1310 分配给第二特殊节点 1305（第 $2c$ 节点）。以同样的方式，将通过以特殊节点密钥 K 两次运算单向函数 h_2 1309 获得的特殊节点密钥 $h_2^{(2)}(K)$ 1312 分配给第二特殊节点 1307（第 $3c$ 节点）。

因此，将以特殊节点密钥 K 运算单向函数 h 获得的密钥 $h(K)$ 分配给第 $(c+1)$ 节点 1202，并将通过以特殊种子值密钥 K 两次运算单向函数获得的密钥 $h^{(2)}(K)$ 1312 分配给第 $(c+2)$ 节点 1303。以同样的方式，将通过以第 $2c$

节点 1305 的特殊种子值密钥 $h_2(K)$ 运算单向函数 h 获得的密钥 $h(h_2(K))$ 分配给第 $(2c+1)$ 节点 1306。将通过以第 $3c$ 节点 1307 的特殊种子值密钥 $h_2^{(2)}(K)$ 1312 运算单向函数 h 获得的密钥 $h(h_2^{(2)}(K))$ 分配给第 $(3c+1)$ 节点 1308。

此时，当 $1 \leq t \leq c$ 时，第 $(c+t)$ 用户存储他/她的种子值密钥和密钥 $h_2(K)$ 。因此，每个节点应额外地存储全部的 c_2 密钥。

如上所述，在本发明第一修改示例性实施例中，将存储在每个节点中的密钥的数目增加，但是通过中心发送的会话密钥的大小减小。

图 14 示出根据本发明的第一次修改示例性实施例的划分发送会话密钥的间隔的方法。参照图 14，在连续地排列若干授权用户的情况下，将其仅划分为将被提供会话密钥的两个间隔 1401 和 1402。

图 15 是示出根据本发明的第一次修改的示例性实施例的将会话密钥发送到多个间隔的方法。参照图 15，在授权用户被划分为四个间隔 1501、1502、1503 和 1504 的情况下，构造如 $E(h^{(2)} h_2^{(2)}(K), SK)$ 的会话密钥，从而仅授权用户可对所述会话密钥解密。

因此，可根据本发明第一修改示例性实施例通过应用函数 h_2 减小计算开销。也就是说，需要最多 $(c+c_2)$ 次单向函数的计算。

根据本发明第一修改示例性实施例，尽管用户的存储开销与基本示例性实施例相比有些增加，但如果撤销用户的数目不是很多，则可显著减小传输开销。

第二修改示例性实施例

根据本发明第一修改示例性实施例，可获得大约与 r 相同的传输开销。该方法示出在诸如具有 $2r-1$ 的传输开销的 SD 方法的当前已知的方法中在传输开销上的最好结果。以下将要描述的第二修改示例性实施例可将传输开销减小到远小于 r 。

下面是第二示例性实施例的基本概念。在位于两个撤销用户之间的一组用户被视为间隔的情况下，在最坏的情况下间隔的总数从未低于 r 。在这种情况下，由于应为每个间隔进行一次传输，因此传输开销变得低于 r 是不可能的。因此，需要改变定义间隔的方法。

因此，在第二修改示例性实施例中，可通过包括多于一个撤销用户设置传输间隔。下面的描述提供间隔可包括一个撤销用户的示例。尽管在第二修改示例性实施例中的示例中公开仅有一个撤销用户的间隔，但是毫无疑问可

考虑具有多于一个撤销用户的间隔。如果一个间隔包括总共 3 个撤销用户，则在理想的情况下传输开销可被减小到 $r/2$ 。

图 16 示出根据本发明的第二修改示例性实施例的定义间隔的方法。根据本发明的第二修改示例性实施例，由于间隔被设置为包括撤销用户，因此传输开销降低，存储开销增加。也就是说，可一次将会话密钥发送到两个撤销用户之间的间隔。

如果间隔包括一个撤销用户，则可考虑图 16 示出的两种情况。在图 16 的情况（1）中，可如基本示例性实施例中公开的那样执行密钥传输。然而在图 16 的情况（2）中，密钥传输过程遵从本发明的第二修改示例性实施例。

执行如第二情况（2）中的对间隔的会话密钥的传输如下。此时，根据本发明的第二修改示例性实施例，需要新的单向散列函数 g 。也就是说，假设间隔 $\{u_i, u_{i+1}, u_{i+2}, \dots, u_{i+s}\}$ 包括撤销用户 u_{i+j} ，这里，间隔的长度不能超过 c ，中心使用密钥 $h^{(s-j)}gh^{(j-2)}(K_i)$ 对会话密钥 SK 加密。

图 16 示出仅有一个撤销用户的间隔的示例。然而，图 16 所示出的第二修改示例性实施例可应用到间隔包括两个或更多撤销用户的情况。

图 17 示出根据本发明的第二修改示例性实施例的将密钥分配给直线结构上的相应节点 1701 到 1708 的方法。参照图 17，直到找到与节点 1702、1703 和 1704 相应的撤销用户，才通过沿着单性密钥链在右侧应用单向散列函数 h 来修改单向密钥链。在撤销用户 u_{i+j} 的节点 1705，应用另一单向散列函数 g 而非单项散列函数 h 以修改单向密钥链。

在撤销用户 1706 和 1707 之后，通过再次使用单项散列函数 h 产生密钥值来构造单向密钥链。对于传输，使用与最后用户的节点相应的密钥对会话密钥 SK 加密。

此时，由于两个单向散列函数 h 和 g 是公知的，因此位于撤销用户的左侧的用户可容易地计算加密使用的密钥。然而，因为撤销用户不知道密钥 $hg^{(j-i)}(K_i)$ ，所以撤销用户 u_{i+j} 不能计算后来的密钥。

同时，位于撤销用户的右侧的用户不得不额外地分别存储与他们在密钥链中的位置相应的密钥。此时，在间隔的长度被设置为 c 的情况下，间隔的数目为 $1+2+3+\dots+(c-2)$ 。也就是说，每个用户不得不额外地存储 $(c-1)(c-2)/2$ 个密钥。

在上述本发明的第二修改示例性实施例中，尽管总的存储开销为

$c+(c-1)(c-2)/2$, 即 $O(c^2)$, 但是传输开销为 $r/2+(N-2r)/c$ 。也就是说, 尽管基本示例性实施例的传输开销为 $r+(N-2r)/c$, 但是第二修改示例性实施例的传输开销最大为 $r/2+(N-2r)/c$ 。此外, 计算开销变为如基本示例性实施例那样最多 c 次单向函数的计算。

在 $N = 1000000$, $r = 50000$ 的情况下, 计算开销和传输开销如表 2 所示。

C	存储开销	传输开销(最坏情况)	比例
64	1955	$25000+14000$	$0.78r$
100	4951	$25000+9000$	$0.68r$

参照表 2, 尽管在这个示例性实施例中基本示例性实施例的传输开销中的第一项 r 被显著地减小到 $r/2$, 但是传输开销中的第二项 $(N-2r)/c$ 增加。

同时, 上述第二修改示例性实施例的方法可扩展到一般情况。也就是说, 随着存储开销增加到 $O(c^3)$, 可执行密钥传输以一次将密钥发送到包括三个撤销用户的间隔。因此, 如上所述, 该方法也被应用于包括多个撤销用户的间隔以及包括一个撤销用户的间隔。

第三修改示例性实施例

通过组合第一和第二修改示例性实施例得到本发明的第三修改示例性实施例。在该情况下, 最坏的情况是当具有长度 c 的每个间隔包括一个撤销用户时。在具有长度小于 c 的间隔包括两个或更多个撤销用户的情况下, 可通过使用上述第二修改示例性实施例一次实现对于两个撤销用户执行的传输。在这种最坏的情况下, 传输开销和存储开销分别为 $r/2+(N-2r)/2(c-2)$ 和 $c+c_2+(c-1)(c-2)/2$ 。

传输开销 $r/2+(N-2r)/2(c-2)$ 可被应用到 r 大于 N/c 的情况。如果 r 小于 N/c , 则获得不同的结果。例如, 假设 r 等于 0, 则传输开销变为 $N/(c \times c_2)$ 。此时, 随着 r 的逐渐增大, 对于包括多个撤销用户并具有长度 c 的间隔需要一次传输。此外, 由于第一修改示例性实施例的方法被应用到其他间隔, 所以传输开销变为近似 $r+(N-cr)/(c \times c_2)$ 。

也就是说, 传输开销形成具有初始值为 $N/(c \times c_2)$, 斜率值为 2 的直线。传输开销沿着直线增加, 其后当 r 为 N/c , 即为拐点时, 传输开销变为 $r/2+(N-2r)/2(c-2)$ 。

根据第三修改示例性实施例, 尽管用户的存储开销与基本示例性实施例相比有些增加, 但是在撤销用户的数目没有很多的情况下可显著地减小传输

开销。

第四修改示例性实施例

本发明的第四修改示例性实施例提出了将直线结构的基本示例性实施例和第一到第三修改示例性实施例应用到圆形结构的方法。

第一，可容易地将在上述示例性实施例中的直线结构重构为圆形结构。也就是说，考虑到直线 L 包括从 u_1 到 u_N 的 N 个用户，通过连接直线 L 的两端将直线结构变成圆形结构。

上述所有定义间隔的方法将被应用到该圆形结构。例如，可构造从用户 u_N 开始的单向密钥链。

在具有上述直线结构的基本示例性实施例中，从用户 u_N 开始的单向密钥链可具有一个密钥 $K_{N,N}$ 。同时，因为在圆形结构中单项密钥链通过粘合用户 u_N 和 u_i 连续下去，所以从用户 u_N 开始的单向密钥链具有如等式 3 所示的与 c 有关个密钥。

$$K_{N,N}, K_{N,1}, K_{N,2}, K_{N,3}, \dots, K_{N,c-1} \text{ 等式 3}$$

通过推广等式 3，从用户 u_i 开始的单向密钥链可被表示为等式 4。

$$K_{i,i}, K_{i,i+1(\bmod N)}, \dots, K_{i,i+c-1(\bmod N)} \text{ 等式 4}$$

特定地，在第四修改示例性实施例中规定：构成连续的授权用户的间隔的最大长度为 c，根据直线结构中用户的位置，每个用户存储一个到与 c 有关个密钥，从而每个用户在圆形结构中存储与 c 有关个密钥。

图 18 描述根据本发明的第四修改示例性实施例的将密钥分配给圆形结构上的每个节点的方法。参照图 8，在本发明的第四修改示例性实施例中规定：10 个节点构成圆形群组，并且包括连续授权用户的间隔的最大长度为 5，每个节点存储 5 个密钥。

当间隔的长度如在第一修改示例性实施中提到的那样被设置为 c 时，为了避免传输开销超过 r，可应用在圆形结构中一次将密钥值发送到长间隔的方法。

此外，为了如第二修改示例性实施例那样将传输开销减小到小于 r，从撤销用户的位置开始应用新的单向函数的方法对于圆形结构是可用的。同样地，组合第一和第二修改示例性实施例的第三修改示例性实施例对于圆形结构也是可用的。

第五修改示例性实施例

本发明的第五修改示例性实施例提出分层圆形结构。

图 19 示出根据本发明示例性实施例的具有圆形节点群组的分层结构。

参照图 19，分层结构中的每个圆形节点包括 c 个节点。分层结构中每个用户相应于每个叶，即，每个圆形结构。如果分层结构除了根节点具有 16 层，则分层结构可相应于 c^{16} 个用户。

因此，可为层上的所有群组节点构造具有上述密钥链的圆形结构。此时，与每个节点相应的每个用户具有分配给他/她的父节点的所有密钥。

在该结构中，具有至少一个撤销用户的具有子节点的每个节点被认为是撤销节点。其后，为了加密中心首先标记撤销节点。中心在整个分层结构中标记撤销节点的父节点。

这样的过程被执行到根节点。如果存在至少一个撤销节点，则根节点变为撤销节点。

在标记撤销节点之后，中心在每层设置间隔。如图 19 所示，在层 0 上仅包括一个节点。中心在层 0 上的圆形群组中设置循环间隔，并使用用于设置的循环间隔的间隔密钥对会话密钥加密。其后，中心仅考虑在层 1 上与层 0 的撤销节点的子节点相应的圆形群组。该过程一直执行到层 15。

例如，在间隔中存在一个撤销用户的情况下，在标记撤销用户的同时在每一层中标记撤销节点。此外，在加密步骤中，由于在层 0 存在撤销节点，因此中心使用除撤销节点以外的循环间隔的间隔密钥对会话密钥加密。同时，中心为层 1 只考虑与在层 0 中的撤销节点的子节点相应的一个圆形群组。

与授权节点的子节点相应并形成循环群组的节点可获得分配给其父节点的会话密钥。因此，中心可通过 16 次加密完成整个分层结构的加密。

尽管第四修改示例性实施例可实现对更多用户的加密并因此需要与以前的示例性实施例相比更多的密钥，但是特别是与第二修改示例性实施例相比，其可以显著地减小传输开销。

规定第四修改示例性实施例的层是层 k ，并且在每个圆形群组中的节点数目为 c ，那么在第四修改示例性实施例中每个用户的存储开销为 $kc+(c-1)(c-2)/2$ ，并且密钥增加为 $(k-1)c$ 。

同时，对于 $c^{k-1}/2 < r$ ，传输开销变为大约 $r/2+3N/4c$ 。可以理解：对于 $r < N/6$ ，第四修改示例性实施例具有比第二修改示例性实施例小的传输开销。

此外，尽管上述第四修改示例性实施例的方法被应用到包括一个撤销用

户（具有 1 个刻点）的情况，显然该方法可被应用到如第二修改示例性实施例所述的包括多个撤销用户（具有 p 个刻点）的间隔的情况。此外，可使用对具有更多层的分层结构设置每个具有撤销用户的间隔以及发送会话密钥的方法。

上面已经描述了根据本发明的每个示例性实施例。同时，在将上述示例性实施例具体地应用到广播加密中时，很难考虑到所有用户同时初始地被加入。也就是说，中心不得不预备在将来将加入的潜在的用户的密钥，并且与所述潜在用户相应的一些预备密钥应被认为是撤销的。否则，新加入的用户可恢复先前发送的消息。

考虑到传输开销取决于 r ，其对中心是个很大的负担。

因此，非常重要的事：当在传输开销方面随着新用户加入需要密钥时，添加新密钥而不是预先预设与潜在用户相应的密钥。上面提出的示例性实施例不管新用户何时新加入都在可以在直线的端部容易地添加新节点。此时，因为由于选择与新订户数目相同的几个新的随机密钥和函数的计算次数的增加引起的计算开销的增加，所以能够在不影响现有用户的密钥的情况下有效地添加新用户。

相反，对于替换用户，涉及随着时间的消逝维护系统。在一旦排列到节点的新户被撤销以后，永久地保持具有属于撤销用户的节点不被使用。因此，在传输开销取决于 r 的系统中，在长时间过后传输开销显著的增加。

在该情况下，通过删除撤销用户的密钥减小不起作用的节点的数目，然后将新用户排列到已经属于撤销用户的不起作用的节点。在传统的内插方法中，可容易地执行用户的替换，但在基于分层树结构的 BE 方案中却是件非常难的事情。在 SD 的情况下，为了仅替换一个用户，由于根节点应被改变所以每个用户密钥应被更新。

同时，在上述本发明的示例性实施例中，用户替换比基于树结构的诸如 SD 等的方法更有用。也就是说，在基本示例性实施例的情况下，可通过更新总共 $2c$ 的用户来替换一个用户。

叛逆者是指通过公开他/她的秘密密钥帮助未授权用户使用消息的授权用户。叛逆者追踪是一种当发现至少一个未授权用户时定位公开他/她的密钥的授权用户的算法。对于这种叛逆者追踪的各种结果是已知的。

已知在每个用户的密钥可被彼此区别并且不能从许多用户的密钥获得新

密钥的情况下，基本上可使用叛逆者追踪。同时，因为满足叛逆追踪的条件，因此可将叛逆追踪应用到上述提出的本发明的示例性实施例中。

同时，通过将基本示例性实施例修改为使用公共密钥对方法，可将每个用户的秘密密钥的数目减少为 2。在该情况下需要的公共密钥为 $O(c^2)$ 。当将修改应用到公共密钥的大小不受限制的应用领域时，该修改是非常有用的。

总之，在用本发明的各种广播加密方法中作为当前最有效的 BE 方案的 CS 和 SC 方法的比较结果如下所示。

表 3

	C	C2	存储开销	传输开销(最坏情况)
基本示例性实施例	200		200 (2K)	50000+4500 (1.1r)
第二修改示例性实施例	64		1955	25000+14000 (0.78r)
第三修改示例性实施例	64	20	1955	25000+7260 (0.64r)
100	100	5151	25000+4500 (0.59r)	
CS			20	$r \times (\log(N/r))$ (4r)
SD			200	100000(2r)

参照图 3，根据本发明示例性实施例，可将作为广播加密中最重要的问题的传输开销减小为低于 r。也就是说，可以理解：与已知的当前最好的方法 SD 方法相比，在本发明示例性实施例中传输开销被显著地降低了。同时，本发明示例性实施例解决很多上述的需要进行实际应用的情况。

上述的示例性实施例和优点仅是示例性的，不能被解释为限制本发明。本教导可被容易地应用到其他类型的设备。此外，本发明示例性实施例的描述是示例性目的，而不是限制权利要求的范围，对于本领域的技术人员，许多替换、修改和改变是显而易见的。

产业上的可利用性

上述发明方法可被用于广播加密系统。

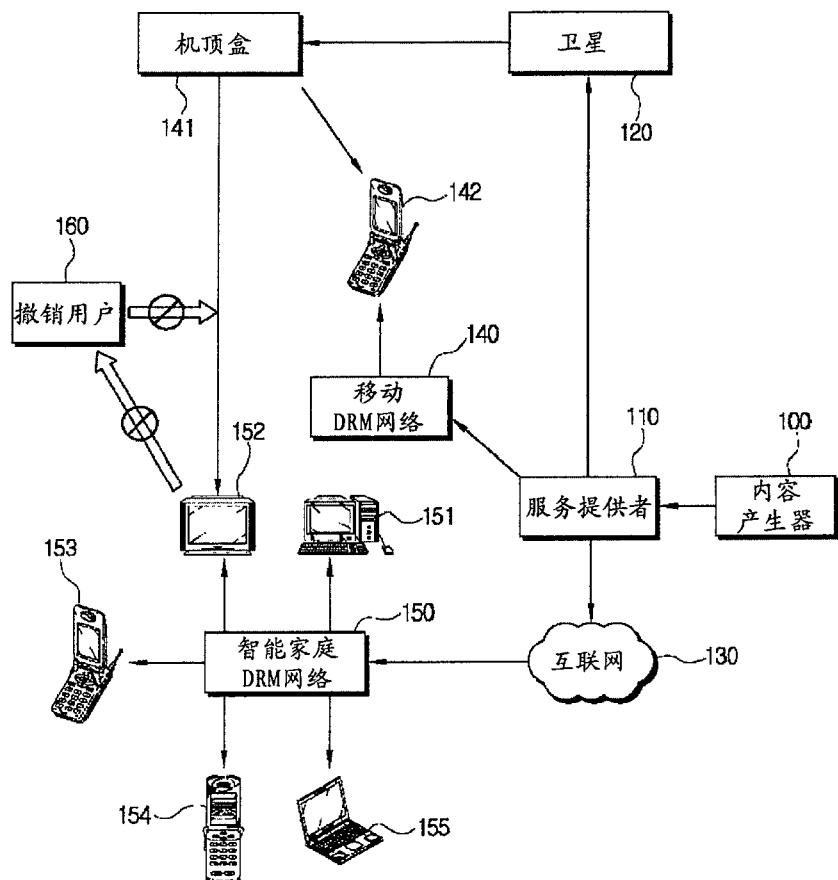


图1

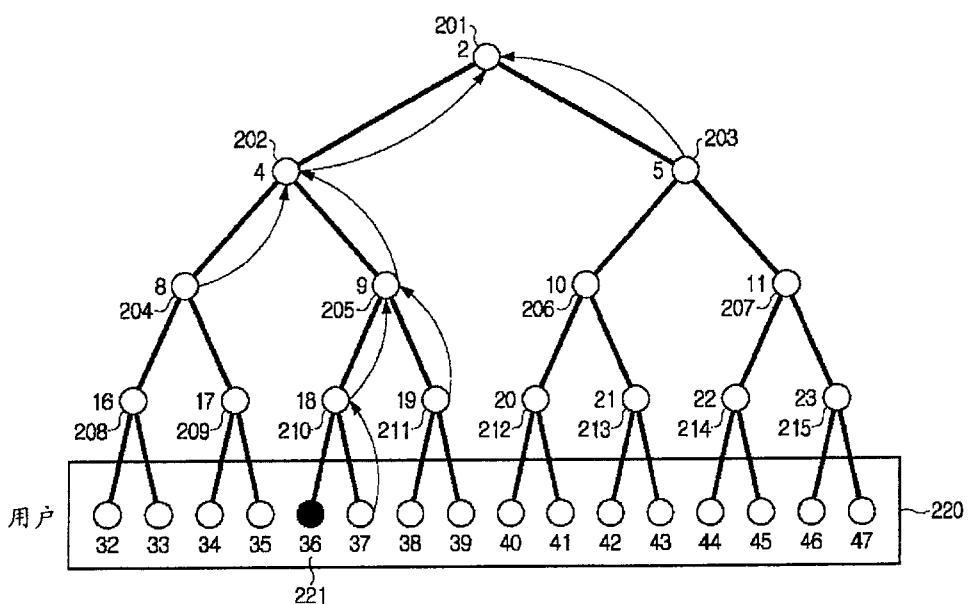


图2

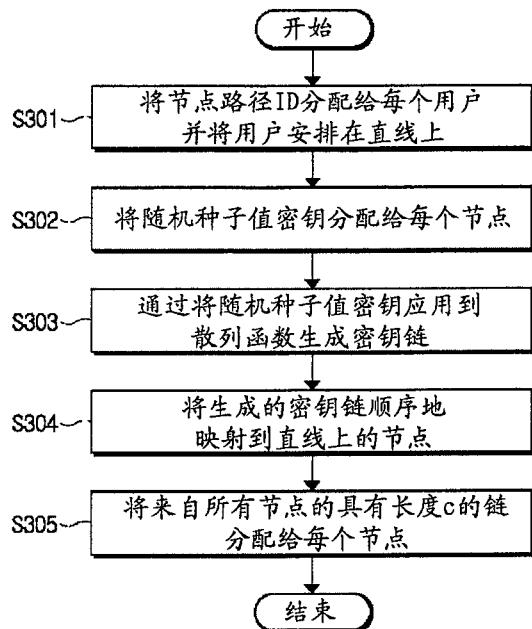


图3

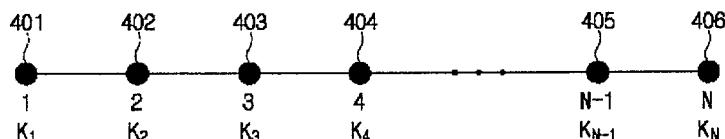


图4

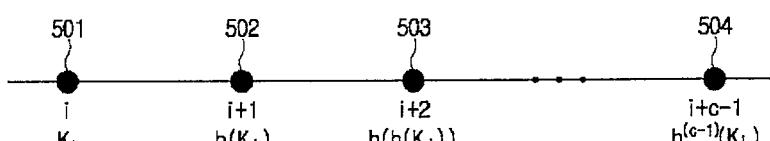


图5

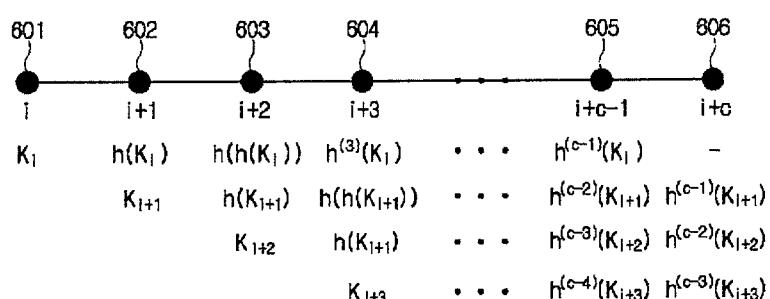
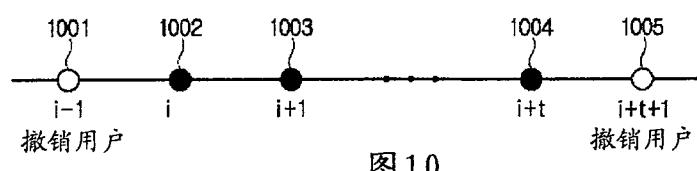
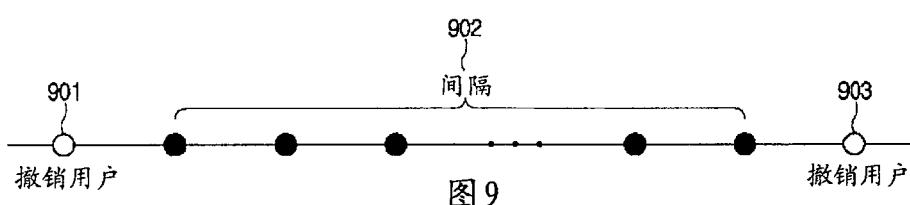
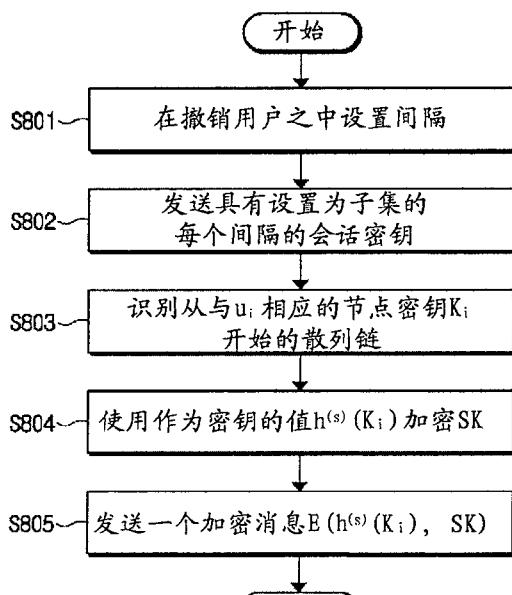
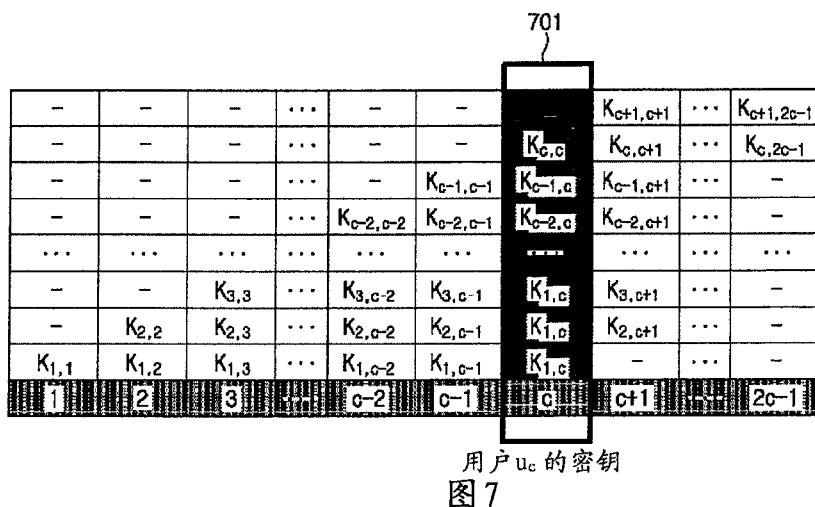


图6



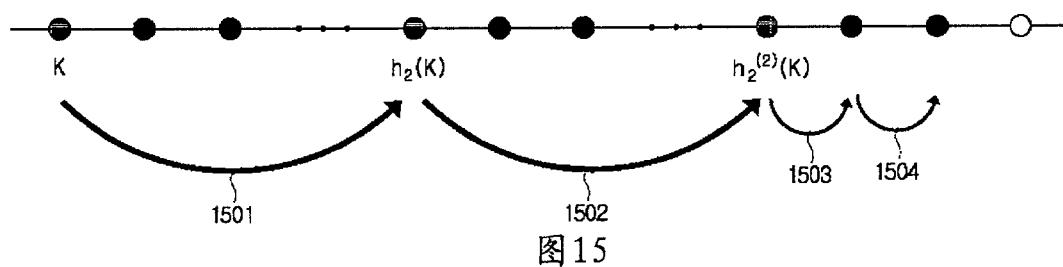
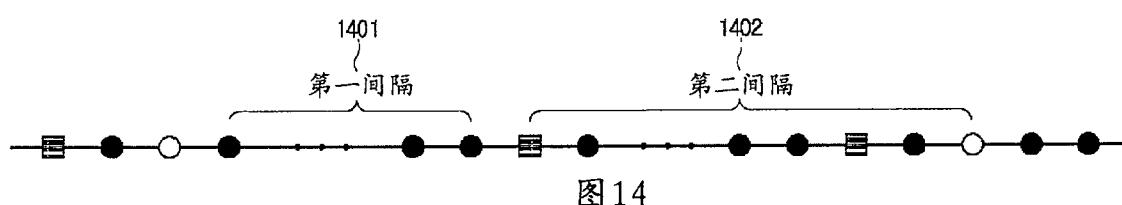
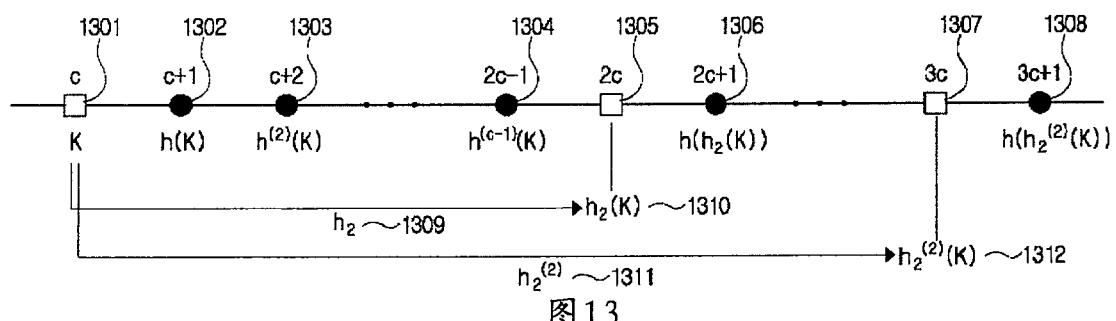
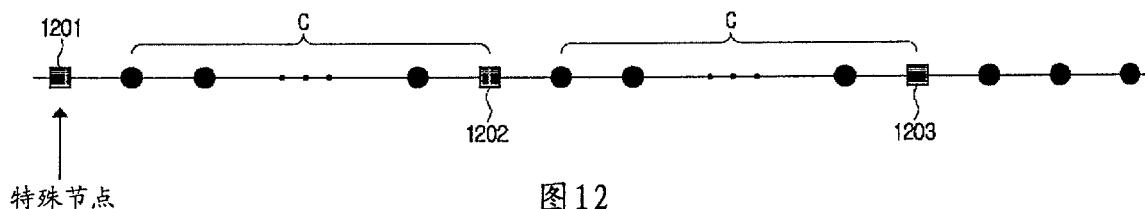
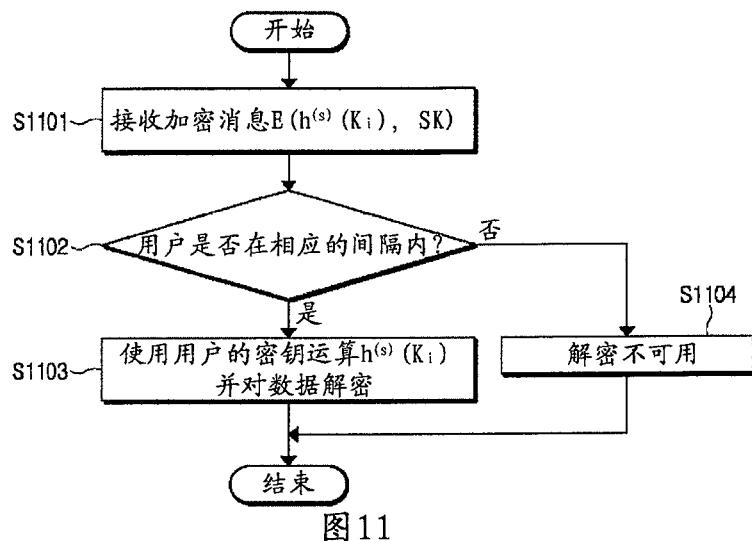




图 16

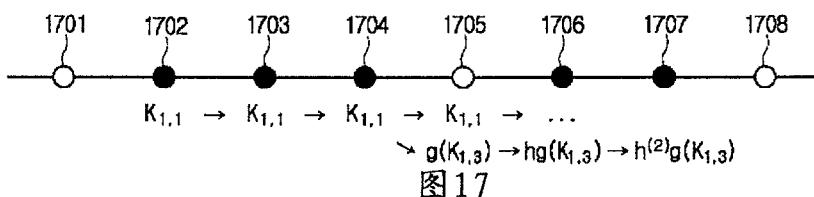


图 17

$K_{10,2}$	$K_{10,3}$	$K_{10,4}$	$K_{10,5}$						$K_{10,1}$	
$K_{9,3}$	$K_{9,4}$	$K_{9,5}$							$K_{9,1}$	$K_{9,2}$
$K_{8,4}$	$K_{8,5}$							$K_{8,1}$	$K_{8,2}$	$K_{8,3}$
$K_{7,5}$						$K_{7,1}$	$K_{7,2}$	$K_{7,3}$	$K_{7,4}$	
					$K_{6,1}$	$K_{6,2}$	$K_{6,3}$	$K_{6,4}$	$K_{6,5}$	
				$K_{5,1}$	$K_{5,2}$	$K_{5,3}$	$K_{5,4}$	$K_{5,5}$		
			$K_{4,1}$	$K_{4,2}$	$K_{4,3}$	$K_{4,4}$	$K_{4,5}$			
		$K_{3,1}$	$K_{3,2}$	$K_{3,3}$	$K_{3,4}$	$K_{3,5}$				
	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$	$K_{2,4}$	$K_{2,5}$					
$K_{1,1}$	$K_{1,2}$	$K_{1,3}$	$K_{1,4}$	$K_{1,5}$						
1	2	3	4	5	6	7	8	9	10	

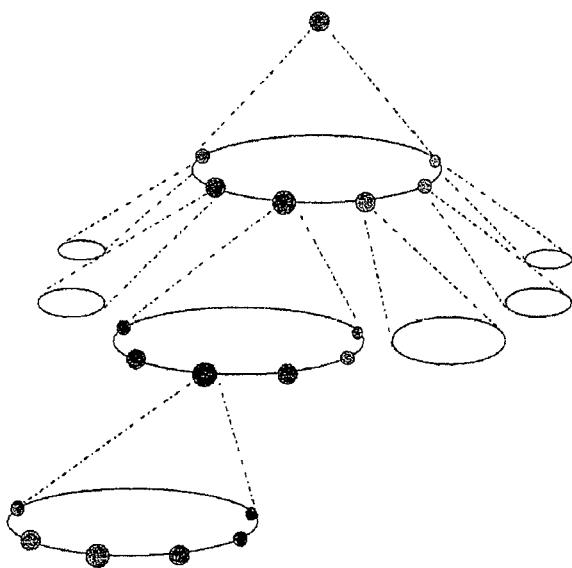
图 18

根节点 : 第一层仅包括一个点

第二层 : c 个节点,
以圆形方式安排

第三层 : c^2 个节点,
存在 c 个圆形

第四层 : c^3 个节点
 $*$ 个圆形



第 $K+1$ 层 : $*$ 个节点
通过相应于每个节点上的一个用户存在 $*$ 个用户

图 19