

## (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局



(43) 国际公布日  
2009 年 4 月 9 日 (09.04.2009)

PCT

(10) 国际公布号  
**WO 2009/043266 A1**

(51) 国际专利分类号:

H04L 9/08 (2006.01)

(21) 国际申请号:

PCT/CN2008/072434

(22) 国际申请日:

2008 年 9 月 19 日 (19.09.2008)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

200710175295.6

2007 年 9 月 28 日 (28.09.2007) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。上海交通大学 (SHANGHAI JIAO TONG UNIVERSITY) [CN/CN]; 中国上海市东川路 800 号, Shanghai 200240 (CN)。

(72) 发明人: 及

(75) 发明人/申请人 (仅对美国): 马春波 (MA, Chunbo) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。李建华 (LI, Jianhua) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。吴越

(WU, Yue) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。刘亚 (LIU, Ya) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京三高永信知识产权代理有限公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市学院路蓟门里和景园 A-1-102, Beijing 100088 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE,

[见续页]

(54) Title: METHOD AND DEVICE FOR GROUP KEY AGREEMENT

(54) 发明名称: 协商组群密钥的方法和设备

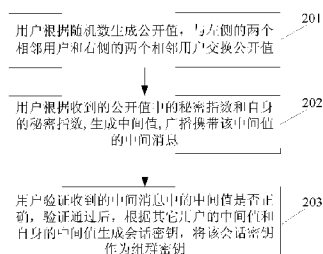


图2 / Fig 2

201 USER GENERATING CLEAR VALUE ACCORDING TO RANDOM NUMBER, EXCHANGING CLEAR VALUE WITH TWO NEIGHBOR USERS IN LEFT HAND SIDE AND TWO NEIGHBOR USERS IN RIGHT HAND SIDE  
202 USER GENERATING MIDDLE VALUE ACCORDING TO SECRET INDEX IN RECEIVED CLEAR VALUE AND OWNED SECRET INDEX, BROADCASTING MIDDLE MESSAGE WHICH CARRIES THE MIDDLE VALUE  
203 USER VERIFYING CORRECTNESS OF MIDDLE VALUE IN RECEIVED MIDDLE MESSAGE, AFTER PASSING VERIFYING, GENERATING SESSION KEY ACCORDING TO MIDDLE VALUE OF OTHER USERS, TAKING SESSION KEY AS GROUP KEY

(57) Abstract: A method and device for group key agreement. The method is based on the dual linear mapping of the elliptic curve, choosing the group key agreement method according to parity of the total number of the users in group. Each user in the group generates the group key through information exchange with other users. There are three types of device, the first of which includes: an information exchange module, a middle value generation module and a group key generation module. A second device includes: an information exchange module, a middle value generation module, a session key generation module, a new middle value generation module and group key generation module. The third device includes: an information exchange module, a middle value generation module, a session key decryption module and a middle value encryption module.

[见续页]

WO 2009/043266 A1



SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,  
GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告。

---

**(57) 摘要:**

协商群组密钥的方法和设备。所述方法基于椭圆曲线的双线性对映射,根据群组内的用户总数的奇偶性选择协商群组密钥的方法,群组内每个用户通过与其他用户的信息交互生成相同的群组密钥。所述设备有三种,其中一种设备包括:信息交互模块、中间值生成模块和群组密钥生成模块。另一种设备包括:信息交互模块、中间值生成模块、会话密钥生成模块、新中间值生成模块和群组密钥生成模块。第三种设备包括:信息交互模块、中间值生成模块、会话密钥解密模块和中间值加密模块。

# 说明书

## 协商组群密钥的方法和设备

### 5 技术领域

本发明涉及通信领域，特别涉及一种协商组群密钥的方法和设备。

### 背景技术

Ad Hoc 网络是一种多跳、自组织、拓扑结构动态变化的网络，节点移动频繁，电能储备有限，而且节点之间的信任关系以及无线传输链路都比较脆弱，这些特点使得对于 Ad Hoc 网络的组密钥协商协议的设计与传统方案具有很大的不同。在 Ad Hoc 网络中，为了保证通信安全，通常需要对消息进行加密后再传输，由于对称密码体制在效率上具有优势，因此采用群组共享密钥能在很大程度上降低消息处理的复杂性。同时，Ad Hoc 网络也是一种动态对等群组，缺少固定的可信第三方支持，因此用于加密消息的组会话密钥必须通过所有组成员协商建立，提高组密钥的安全可靠性。另外，Ad Hoc 网络组密钥协商协议还应考虑网络的动态拓扑特性，所以要求密钥协商协议能够实现密钥的前向安全性以及后向安全性，并能有效支持节点的加入与退出。

现有技术中有一种 Joux 三方密钥协商协议，以三个用户  $U_1$ 、 $U_2$  和  $U_3$  协商一个共享密钥为例，参见图 1，该协议的运行过程如下：

步骤 101：选择系统参数，为每个用户选择两个阶为  $q$ 、建立在椭圆曲线上的循环乘群  $G_1$  和  $G_2$ ， $g$  为群  $G_1$  的生成子，并且循环乘群  $G_1$  和  $G_2$  具有可有效计算的双线性映射，即  $G_1$  上的一个元素与  $G_2$  上的一个元素的乘积是  $G_2$  上的另外一个元素，表示为  $G_1 \times G_2 \rightarrow G_2$ ，这里在  $G_1$  和  $G_2$  上的双线性对的计算是比较容易的，就称作是可计算的。设  $g$  与  $g$  的双线性映射记为  $Q$ ， $Q$  为乘群  $G_2$  的生成子。

步骤 102： $U_1$  随机选择  $x_1 \in Z_q^*$ ，然后计算公开值  $R_1 = g^{x_1}$ ，并将  $R_1$  发送给  $U_2$  和  $U_3$ ； $U_2$  随机选择  $x_2 \in Z_q^*$ ，然后计算公开值  $R_2 = g^{x_2}$ ，并将  $R_2$  发送给  $U_1$  和  $U_3$ ； $U_3$  随机选择  $x_3$ ，然后计算公开值  $R_3 = g^{x_3}$ ，并将其发送给  $U_1$  和  $U_2$ 。

步骤 103： $U_1$  根据收到的公开值  $R_2$  和  $R_3$  及  $x_1$  计算三方会话的密钥  $\text{Key} = Q^{x_1 x_2 x_3}$ ； $U_2$  根据  $R_1$  和  $R_3$  及  $x_2$  计算三方会话的密钥  $\text{Key} = Q^{x_1 x_2 x_3}$ ； $U_3$  根据  $R_1$  和  $R_2$  及  $x_3$  计算三方会话的密钥  $\text{Key} = Q^{x_1 x_2 x_3}$ 。

通过上两步的计算，用户  $U_1$ 、 $U_2$  和  $U_3$  得到了相同的会话密钥，即密钥  $\text{Key} = Q^{x_1 x_2 x_3}$ 。

基于 Joux 三方密钥协商协议, 现有技术还构造了群密钥协商协议, 下面简单介绍该群密钥协商协议如下:

该协议有三个算法, 分别是 3-群密钥协商算法 (3-G), 2-群密钥协商算法 (2-G) 和群密钥协商算法 (KG)。

5 在密钥协商前, 每个群组分别选择两个阶为  $q$  的建立在椭圆曲线上的群  $G_1$  和  $G_2$ , 其中,  $G_1$  为加法循环群,  $G_2$  为乘法循环群,  $P$  为群  $G_1$  的生成子; 这两个群有可计算的双线性映射。另外, 设  $P$  与  $P$  的双线性映射记为  $W$ ,  $W$  也是群  $G_2$  的生成子。

10 设有  $n$  个用户进行密钥协商, 用  $U$  表示用户集合的子集。对于每一个用户  $i$ , 其公钥为  $Q_i$ , 该公钥与其身份相关。系统自身选取一个随机数  $s$ , 然后计算  $sP$  作为系统的公钥  $P(\text{pub})$ , 而各个用户的长期私钥  $S_i = sQ_i$ 。

这里先介绍 3-群密钥协商算法 (3-G): 设有三组用户进行密钥协商, 分别为  $U_1$ ,  $U_2$ ,  $U_3$ , 其临时私钥分别为  $S_1$ ,  $S_2$ ,  $S_3$ 。在这三组用户中, 每组有一个代表, 不失一般性, 设成员  $A_1$  为  $U_1$  的代表, 成员  $A_2$  为  $U_2$  的代表, 成员  $A_3$  为  $U_3$  的代表。成员  $A_1$  进行如下计算:

15 1) 计算临时私钥  $S_1$  和  $P$  的乘积  $P_1$ , 即  $P_1 = PS_1$ ;  
2) 计算  $P_1$  的 Hash 函数得到  $D_1$ , 即  $D_1 = H(P_1)$ ; 然后以  $D_1$  乘以  $S_1$  并加上临时私钥  $S_1$  和  $P_1$  的乘积得到  $T_1$ , 即  $T_1 = D_1S_1 + S_1P_1$ ;

3) 成员  $A_1$  将  $P_1$  和  $T_1$  发送给其它组群中的各个成员。

20 成员  $A_2$  和成员  $A_3$  也进行上述步骤, 成员  $A_2$  将  $P_2$  和  $T_2$  发送给其它组群中的各个成员, 成员  $A_3$  将  $P_3$  和  $T_3$  发送给其它组群中的各个成员。

最后,  $U_1$  内的成员根据收到的  $P_2$  和  $T_2$ 、 $P_3$  和  $T_3$ , 以及临时私钥  $S_1$  生成共享密钥  $\text{Key} = H(W^{S_1S_2S_3})$ ;  $U_2$  内的成员根据收到的  $P_1$  和  $T_1$ 、 $P_3$  和  $T_3$ , 以及临时私钥  $S_2$  生成共享密钥  $\text{Key} = H(W^{S_1S_2S_3})$ ;  $U_3$  内的成员根据收到的  $P_1$  和  $T_1$ 、 $P_2$  和  $T_2$ , 以及临时私钥  $S_3$  生成共享密钥  $\text{Key} = H(W^{S_1S_2S_3})$ 。

25 下面介绍 2-群密钥协商协议算法 (2-G):

设有两组用户参与该算法, 分别为  $U_1$ ,  $U_2$ , 其临时私钥分别为  $S_1$ ,  $S_2$ 。设  $U_1$  的代表为  $A_1$ ,  $U_2$  的代表为  $A_2$ 。成员  $A_1$  进行如下计算:

1)  $A_1$  计算临时私钥  $S_1$  和  $P$  的乘积  $P_1$ , 即  $P_1 = PS_1$ ;

2) 计算  $P_1$  的 Hash 函数得到  $D_1$ , 即  $D_1 = H(P_1)$ ; 然后以  $D_1$  乘以  $S_1$  并加上临时私钥  $S_1$  和  $P_1$  的乘积得到  $T_1$ , 即  $T_1 = D_1S_1 + S_1P_1$ ;

3) 成员  $A_1$  将  $P_1$  和  $T_1$  发送给  $U_2$  的各个用户。

同样的 A2 进行类似的计算，并将 P2 和 T2 发送给 U1 的用户。

4) A1 选取随机数  $sA1 \in Z_q^*$ ，并计算  $K1 = (sA1) P$ ;

5) A1 首先计算 K1 的 Hash 函数，记做  $H(K1)$ ，然后以  $H(K1)$  乘以 S1 并加上  $(sA1)$  和 K1 的乘积，这里记做  $T(sA1)$ ， $T(sA1) = H(K1)S1 + (sA1) K1$ ;

5 6) A1 将 K1 和  $T(sA1)$  发送给其余的用户。

完成以上步骤后，U1 中的用户通过 T2 对 P2 进行验证，验证通过后，再根据 P2 计算共享密钥  $Key = H(W^{S1S2sA1})$ ，即以 S1，S2 和 sA1 的乘积为幂，W 为底的指数，然后进行 Hash 运算。

10 这里只有 A1 选择了随机数 sA1。A1 选择这个随机数会使两个成员之间的运算象三个成员，同理，U2 中的用户进行上述运算，将得到相同的共享密钥 Key。

下面介绍群密钥协商算法 KG，该密钥协商算法是一个递归算法。描述如下：

输入的参数为 m 和组群  $U(i+1), U(i+2), \dots, U(i+m)$ 。其中，m 表示组群中用户的规模。例如：组群由用户 U1，U2，U3，U4，U5 构成，那么当  $i=2$ ， $m=2$  时，组群就是用户集合的一个子集，包括用户 U3，U4。进行该算法时，令  $U_j$  等于 j，这里  $n \geq j \geq 1$ ;

15 如果输入的参数  $m=1$ ，密钥协商后，共享密钥  $Key = s(i+1)$ ;

如果  $m=2$ ，调用上述 (2-G) 算法，输入的参数为  $U(i+1)$ ， $U(i+2)$  和  $s(i+1)$ ， $s(i+2)$ ，共享密钥 Key 是组群  $U(i+1)$  和  $U(i+2)$  的协商密钥;

当 m 大于 2 时，设  $n0$  为 0， $n1$  为大于 m 除以 3 的最小整数， $n3$  为小于 m 除以 3 的最小整数， $n2 = m - n1 - n3$ 。循环变量 j 从 1 到 3 进行如下过程：

20 进行密钥协商算法 KG，输入的参数为  $n_j$ ， $U(i+n(j-1)+1), \dots, U(i+n(j-1)+n_j)$ ;

设  $YU_j$  为  $U(i+n(j-1)+1), \dots, U(i+n(j-1)+n_j)$  的集合;  $Ys_j = Key$ ;  $n_j = n(j-1) + n_j$ 。

调用 3-G 算法，输入的参数为  $YU1, YU2, YU3, Ys1, Ys2$  和  $Ys3$ 。

则 KEY 等于  $YU1, YU2$  和  $YU3$  协商的会话密钥。

25 上述三种方案的缺点是：密钥协商的算法通过递归调用产生，增加了算法的复杂度；密钥协商的通信轮数随着参与者的人数的增加而增加，上述三种方案不但增加了时延，还增大了系统的通信量。

## 发明内容

30 为了简化密钥协商过程的通信量，并缩短密钥协商的时间，本发明实施例提供了一种协商组群密钥的方法和设备。所述技术方案如下：

本发明实施例提供了一种协商组群密钥的方法，当组群内的用户总数为奇数时，所述

方法包括：

步骤 A：用户根据秘密指数生成公开值，分别与左侧的两个相邻用户和右侧的两个相邻用户交换公开值；

5 步骤 B：所述用户收到四个相邻用户发送的公开值后，根据所述公开值中的秘密指数和自身的秘密指数生成中间值，广播携带所述中间值的中间消息；

步骤 C：所述用户收到其它用户的中间消息后，验证所述中间消息中的中间值是否正确，验证通过后，根据所述其它用户的中间值和自身的中间值生成会话密钥，将所述会话密钥作为组群密钥；

当组群内的用户总数为偶数时，所述方法包括：

10 步骤 A1：从组群中分离出一个用户，将所分离出的用户作为特定用户；将组群内的其余用户组成新的组群，所述新的组群内每个用户执行所述步骤 A 至所述步骤 C；

步骤 B1：所述特定用户与所述新的组群内的多个用户交换携带秘密指数的公开值；所述特定用户与所述多个用户根据收到的公开值中的秘密指数生成新中间值；

15 步骤 C1：所述多个用户用所述新中间值加密所述会话密钥，并将加密后的密文发送给所述特定用户；所述特定用户收到所述密文后，用所述新中间值对所述密文解密，得到所述会话密钥；

步骤 D1：所述多个用户和所述特定用户用所述会话密钥加密所生成的新中间值，并广播加密后的所述新中间值；

20 步骤 E1：所述特定用户和所述新的组群内的每个用户根据所述新中间值和所述会话密钥生成新的组群密钥。

本发明实施例还提供了一种协商组群密钥的设备，所述设备包括：

信息交互模块，用于根据秘密指数生成公开值，分别与左侧的两个相邻设备和右侧的两个相邻设备交换公开值，以及与其它设备进行信息交互；

25 中间值生成模块，用于提取所述信息交互模块收到的公开值中的秘密指数，根据所述公开值中的秘密指数和设备自身的秘密指数生成中间值，并通知所述信息交互模块广播携带所述中间值的中间消息；

组群密钥生成模块，用于验证所述信息交互模块收到的中间消息中的中间值，验证通过后，根据所述其它设备的中间值和自身的中间值生成会话密钥，将所述会话密钥作为组群密钥。

30 本发明实施例还提供了另一种协商组群密钥的设备，所述设备包括：

信息交互模块，用于根据秘密指数生成公开值，分别与左侧的两个相邻设备和右侧的

两个相邻设备交换公开值，以及与其它设备进行信息交互；

中间值生成模块，用于提取所述信息交互模块收到的公开值中的秘密指数，根据所述公开值中的秘密指数和设备自身的秘密指数生成中间值，并通过所述信息交互模块广播携带所述中间值的中间消息；

- 5        会话密钥生成模块，用于验证所述信息交互模块收到的中间消息中的中间值，验证通过后，根据收到的中间值和自身的中间值生成会话密钥；

新中间值生成模块，用于通知所述信息交互模块与特定设备交换携带秘密指数的公开值，并根据接收到的所述特定设备的公开值中的秘密指数和设备自身的秘密指数生成新中间值；

- 10       组群密钥生成模块，用于根据所述新中间值生成模块生成的新中间值和所述会话密钥生成新的组群密钥。

进一步地，本发明实施例还提供了一种协商组群密钥的设备，所述设备包括：

信息交互模块，用于根据秘密指数生成公开值，分别与组群中的多个设备交换公开值，以及与其它设备进行信息交互；

- 15       中间值生成模块，用于提取所述信息交互模块收到的公开值中的秘密指数，根据所述公开值中的秘密指数和设备自身的秘密指数生成中间值；

会话密钥解密模块，用于利用所述中间值生成模块生成的中间值解密所述信息交互模块收到的密文，得到会话密钥；

- 20       中间值加密模块，用于利用所述会话密钥解密模块解密出的会话密钥对所述中间值生成模块生成的中间值加密，并通过所述信息交互模块广播加密后的所述中间值。

本发明实施例提供的技术方案的有益效果是：

- 25       本发明实施例中每个用户与左侧相邻的两个用户和右侧的两个相邻用户交换携带秘密指数的中间消息，进而生成中间值，与其它用户交换中间值生成会话密钥，使密钥协商过程中的通信轮数较少，提高了通信的实时性。且密钥协商的轮数与成员的人数无关，减小密钥协商的通信量。

## 附图说明

图 1 是现有技术中的 Joux 三方密钥协商协议的运行过程流程图；

- 30       图 2 是本发明实施例 1 提供的组群内的用户总数为奇数时的协商组群密钥的方法流程图；

图 3 是本发明实施例 1 提供的组群内的用户总数为偶数时的协商组群密钥的方法流程

图;

图 4 是本发明实施例 1 提供的组群内的用户总数为奇数时的协商组群密钥的方法举例流程图;

图 5 是本发明实施例 1 提供的组群内的用户总数为偶数时的协商组群密钥的方法举例流程图;

图 6 是本发明实施例 1 提供的组群个数为 5 时的协商组群密钥的方法流程图;

图 7 是本发明实施例 2 提供的协商组群密钥的设备的结构图;

图 8 是本发明实施例 3 提供的另一种协商组群密钥的设备的结构图;

图 9 是本发明实施例 4 提供的第三种协商组群密钥的设备的结构图。

10

## 具体实施方式

为使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明实施方式作进一步地详细描述。

本发明以下实施例提供的协商组群密钥方案的系统参数包括:两个阶为  $q$ , 且建立在椭圆曲线上的循环乘群  $G1$  和  $G2$ ,  $g$  为群  $G1$  的生成子, 这两个乘群有可计算的双线性映射,  $g$  与  $g$  的双线性映射记为  $Q$ 。

### 实施例 1

本实施例提供了一种协商组群密钥的方法, 当组群内的用户总数为奇数时, 参见图 2, 该方法包括:

20 步骤 201: 用户根据秘密指数生成公开值, 分别与左侧的两个相邻用户和右侧的两个相邻用户交换公开值;

步骤 202: 该用户收到四个相邻用户发送的公开值后, 根据收到的中间消息中的秘密指数和自身的秘密指数生成中间值, 广播携带该中间值的中间消息;

25 步骤 203: 该用户收到其它用户的中间消息后, 验证收到的中间消息中的中间值是否正确, 验证通过后, 根据其它用户的中间值和自身的中间值生成会话密钥, 将该会话密钥作为组群密钥。

当组群内的用户总数为偶数时, 参见图 3, 该方法包括:

30 步骤 301: 从组群中分离出一个用户, 将所分离出的用户作为特定用户; 将组群内的其余用户组成新的组群, 新的组群内的用户总数为奇数, 每个用户执行步骤 201 至步骤 203 获取会话密钥;

步骤 302: 此特定用户与新的组群内的多个用户交换携带秘密指数的公开值; 此特定用

户与上述多个用户根据收到的公开值中的秘密指数生成新中间值;

步骤 303: 上述多个用户用新中间值加密会话密钥, 并将加密后的密文发送给此特定用户; 此特定用户收到该密文后, 用新中间值对密文解密, 得到会话密钥;

步骤 304: 多个用户和此特定用户用会话密钥加密新中间值, 并广播加密后的新中间值;

5 步骤 305: 此特定用户和新的组群内的每个用户根据新中间值和会话密钥生成新的组群密钥。

下面以  $n$  (这里设  $n$  为奇数) 个用户 ( $U_1, U_2, \dots, U_n$ ) 为例, 其中,  $U(n+1)=U_1, U(n+2)=U_2, U(-1)=U(n-1), U(0)=U(n)$ , 这样就构成了一个由  $n$  个用户构成的首尾相接的用户链。参见图 4, 协商组群密钥的方法如下:

10 步骤 401: 用户  $U_i$  选择随机数, 并将选择的随机数作为秘密指数, 根据秘密指数和系统参数  $g$  计算公开值, 将该公开值发送给她左侧相邻最近的两个用户和右侧相邻最近的两个用户。此步骤具体为:

用户  $U_i$  选择随机数  $x_i \in Z_q^*$ , 其中,  $q$  是  $g$  的阶, 星号表示除去 0。计算公开值  $X_i = g^{x_i}$ , 并将  $X_i$  发送给用户  $U(i-2)$ 、 $U(i-1)$ 、 $U(i+1)$  及  $U(i+2)$ , 即分别发送给她左侧相邻最近的两个  
15 用户和右侧相邻最近的两个用户。

步骤 402: 用户  $U_i$  接收其右边两个用户  $U(i+1)$  和  $U(i+2)$  的两个值  $X(i+1)$  和  $X(i+2)$ , 左边两个用户  $U(i-1)$  和  $U(i-2)$  的两个值  $X(i-1)$  和  $X(i-2)$  后, 用户  $U_i$  通过  $X(i+1)$ ,  $X(i+2)$  和  $X_i$  计算右侧共享密钥  $R_i = Q^{x(i+1)x(i+2)x_i}$ , 以及左侧共享密钥  $L_i = Q^{x(i-1)x(i-2)x_i}$ 。

20 步骤 403: 用户  $U_i$  计算中间值  $K_i = R_i/L_i$ , 然后通过网络将携带该中间值的中间消息发送给其它用户。

步骤 404: 用户  $U_i$  收到所有其它用户发送的中间消息后, 提取中间值  $K_1, K_2, \dots, K(i-1), K(i+1), \dots, K_n$  后, 验证中间值  $K_1, K_2, \dots, K_n$  是否正确。具体验证过程如下:

因为  $R_i = Q^{x(i+1)x(i+2)x_i}$ ,  $L(i+2) = Q^{x(i+1)x_i x(i+2)}$ , 所以  $R_i = L(i+2)$ 。又因为  $K_i = R_i/L_i$ , 所以用户  $U_i$  可以通过计算  $K(i+2)$  与  $R_i$  的乘积得到  $R(i+2)$ , 因为  $R(i+2) = L(i+4)$ , 所以用户  $U_i$   
25 又可以通过计算  $K(i+4)$  与  $R(i+2)$  的乘积得到  $R(i+4)$ , 也就是  $L(i+6)$ 。以此类推最后得到  $L_i$ , 也就是  $R(i-2)$  的值。如果用户  $U_i$  通过上述方法计算得到的  $L_i$  与其在步骤 202 中计算得到的相同, 则说明他收到的中间值  $K_1, K_2, \dots, K_n$  正确, 否则不正确, 不进行组群密钥的协商。

步骤 405: 验证中间值  $K_1, K_2, \dots, K_n$  正确后, 根据步骤 404 中的递推方法, 将得到  
30  $R_1, R_2, \dots, R_n$ 。例如, 以当前用户  $U_i$  为  $U_1$  为例, 则由  $R_1 \rightarrow R_3$ , 由  $R_3 \rightarrow R_5, \dots, R(n-2) \rightarrow R(n)$ , 然后, 由  $R(n) \rightarrow R_2$ , 由  $R_2 \rightarrow R_4, \dots, R(n-3) \rightarrow R(n-1)$ , 其它用户的推

导过程类似。用户  $U_i$  计算组群的会话密钥  $S=R_1R_2 \dots R_n$ 。

上述方法中的用户个数  $n$  为奇数，如果组群内用户个数是偶数个时，设此时有  $n+1$  个用户，根据上述步骤 404 中的递推方法，奇数用户  $U_1, U_3, \dots, U(n)$  将会推导出  $R_1, R_3, \dots, R(n)$ ，偶数用户  $U_2, U_4, \dots, U(n+1)$  将会推导出  $R_2, R_4, \dots, R(n+1)$ ，所以奇数用户计算出的会话密钥  $S=R_1R_3 \dots R(n)$ ，偶数用户计算出的会话密钥  $S=R_2R_4 \dots R(n+1)$ ，所以，当组群内的用户个数为偶数个时，参见图 5，执行以下步骤：

步骤 501：从  $n+1$  个用户中选择  $n$  个用户，分别为用户  $U_1, U_2, \dots, U_n$ 。

步骤 502 至步骤 506 与上述步骤 401 至步骤 405 相同，这里不再赘述。

步骤 507：用户  $U_1, U_2, \dots, U_n$  通过上述方法得到  $(U_1, U_2, \dots, U_n)$  的组群会话密钥  $S$  后，从用户  $U_1, U_2, \dots, U_n$  中选择多个用户与用户  $U(n+1)$  进行信息交互，本实施例选择用户  $U_1$  和  $U_n$ ，用户  $U_1$  和  $U_n$  分别将公开值  $X_1$  和  $X_n$  发送给  $U(n+1)$ 。同时， $U(n+1)$  随机选择  $x(n+1) \in Z_q^*$ ，计算公开值  $X(n+1)=g^{x(n+1)}$ ，并将公开值  $X(n+1)$  分别发送给  $U_1$  和  $U_n$ 。

步骤 508：用户  $U_1, U_n$  和  $U(n+1)$  通过双线性对计算中间值  $K(n+1)=Q^{x_1x_nx(n+1)}$ 。

步骤 509：用户  $U_1$  和  $U_n$  分别将中间值  $K(n+1)$  作为密钥加密会话密钥  $S$ ，并将加密后的密文发送给用户  $U(n+1)$ ；

步骤 510：用户  $U(n+1)$  收到密文后，用中间值  $K(n+1)$  解密得到会话密钥  $S$ 。

步骤 511：用户  $U_1, U_n$  和  $U(n+1)$  分别用  $S$  作为密钥加密中间值  $K(n+1)$ ，并将加密后的密文广播给其它用户；

步骤 512：用户  $U_1, U_2, \dots, U(n+1)$  共享组群会话密钥  $S$  和中间值  $K(n+1)$ ，将组群会话密钥  $S$  和中间值  $K(n+1)$  进行连接，然后进行 Hash 运算得到当前的组群密钥  $KK$ ，即  $KK=H(S||K(n+1))$ 。

当有一群用户加入时，不失一般性，假设有  $j$  个用户  $C_1, C_2, \dots, C_j$  加入当前组群  $(U_1, U_2, \dots, U_n)$ ，具体群组密钥协商过程如下：

首先，构造  $(U_n, C_1, C_2, \dots, C_j, U_1)$  的用户群，并为组群中的用户按照由小到大的顺序编号形成组群  $(T_1, T_2, \dots, T_{j+2})$ ，其中， $T_1=U_n, T_{j+2}=U_1$ 。然后在该组群中按以上的组群密钥协商方法得到该组群密钥  $KT$ 。

用户  $U_1$  和  $U_n$  以  $S$  为密钥加密组群密钥  $KT$ ，并将密文以广播的形式发送给  $(U_2, \dots, U(n-1))$ 。这样在用户  $(U_1, \dots, U_n)$  中共享了两个秘密值：组群会话密钥  $S$  和组群密钥  $KT$ 。

用户  $U_1, \dots, U_n$  将组群会话密钥  $S$  和组群密钥  $KT$  进行连接, 然后进行 Hash 运算得到当前的组群密钥  $KK$ 。同时,  $U_1$  和  $U_n$  用  $KT$  为组群密钥加密  $KK$ , 并将其发送给用户  $C_1, C_2, \dots, C_j$ , 使该组用户拥有组群密钥  $KK$ 。

在完成上述加入算法之后, 也可以对用户进行排序, 对于新加入的成员  $C_1, C_2, \dots, C_j$ , 令  $C_1=U(n+1), C_2=U(n+2), \dots, C_j=U(n+j)$ 。

如果上述加入的用户为单个用户时, 即  $C_1$  要求加入组群  $(U_1, \dots, U_n)$  中, 具体过程如下:

首先, 令  $C_1$  为  $U(n+1)$ ,  $C_1$  随机选取随机数  $x(n+1)$ , 计算公开值  $X(n+1)=g^{x(n+1)}$ , 并将公开值  $X(n+1)$  发送给用户  $U_1$  和  $U_n$ 。同时,  $U_1$  和  $U_n$  将公开值  $X_1$  和  $X_n$  发送给  $U(n+1)$ 。  
10 然后,  $U_1, U_n$  和  $U(n+1)$  计算组群密钥  $KT=Q^{x_1x_nx(n+1)}$ 。

接着,  $U_1$  和  $U_n$  以组群会话密钥  $S$  为密钥加密  $KT$ , 并将密文以广播的形式发送给  $(U_2, \dots, U(n-1))$ 。这样在用户  $(U_1, \dots, U_n)$  中共享了两个秘密值组群会话密钥  $S$  和组群密钥  $KT$ 。

用户  $(U_1, \dots, U_n)$  将组群会话密钥  $S$  和组群密钥  $KT$  进行连接, 然后进行 Hash 运算,  
15 得到当前的组群密钥  $KK$ , 即  $KK=\text{Hash}(S||KT)$ 。同时,  $U_1$  和  $U_n$  用  $KT$  为密钥加密  $KK$ , 并将其发送给用户  $C_1$ , 使得该用户拥有密钥  $KK$ 。

如果日前用户群由  $(U_1, U_2, \dots, U_n)$  构成, 当用户  $U_i, \dots, U_j$  要退出该组群时, 则将剩余的用户组成新的组群, 根据新组群中用户个数的奇偶数, 执行上述组群密钥的协商方法的步骤 401 至步骤 405 或步骤 501 至步骤 512。

20 针对上述组群密钥的协商方法, 以 5 个用户构成的组群  $U_1, U_2, U_3, U_4, U_5$  为例, 参见图 6, 具体过程如下:

步骤 601: 用户  $U_1, U_2, U_3, U_4, U_5$  分别选择随机数, 并根据选择的随机数和系统参数  $g$  分别计算公开值, 然后将公开值发送给她左侧的两个相邻用户和右侧的两个相邻用户。具体为:

25 用户  $U_1$  选择随机数  $x_1 \in Z_q^*$ , 计算公开值  $X_1=g^{x_1}$ , 并将  $X_1$  发送给用户  $U_2, U_3$  和  $U_4, U_5$ ; 同理, 用户  $U_2$  将  $X_2$  发送给  $U_1, U_5$  和  $U_3, U_4$ ; 用户  $U_3$  将  $X_3$  发送给  $U_1, U_2$  和  $U_4$  和  $U_5$ ; 用户  $U_4$  将  $X_4$  发送给  $U_2, U_3$  和  $U_5, U_1$ ; 用户  $U_5$  将  $X_5$  发送给  $U_3, U_4$  和  $U_1, U_2$ , 这样就构成了一个由 5 个用户构成的首尾相接的用户链。

步骤 602: 用户  $U_1$  收到了其它四个用户发送的公开值, 分别是  $U_2$  的  $X_2, U_3$  的  $X_3, U_4$  的  $X_4$  和  $U_5$  的  $X_5$ , 用户  $U_1$  计算右侧密钥  $R_1=Q^{x_1x_2x_3}$  和左侧密钥  $L_1=Q^{x_1x_4x_5}$ 。同理, 其它用户也进行类似计算。

步骤 603: 用户 U1 计算中间值  $K1=R1/L1$ , U2 计算中间值  $K2=R2/L2$ , U3 计算中间值  $K3=R3/L3$ , U4 计算中间值  $K4=R4/L4$ , U5 计算中间值  $K5=R5/L5$ , 然后分别通过网络将中间值 K1, K2, K3, K4, K5 发布给组内其它用户。

步骤 604: 用户 U1 收到其它用户发送的中间值 K2, K3, K4, K5 后, 对中间值 K2, K3, K4, K5 进行验证。

因为有  $R1$  等于  $L3$ ,  $R2$  等于  $L4$ ,  $R3$  等于  $L5$ ,  $R4$  等于  $L1$ ,  $R5$  等于  $L2$ , 所以, 用户 U1 可以通过  $R1$  与  $K3$  的乘积得到  $R3$ ,  $R3$  与  $K5$  的乘积得到  $R5$ ,  $R5$  与  $K2$  的乘积得到  $R2$ ,  $R2$  与  $K4$  的乘积得到  $R4$ ,  $R4$  与  $K1$  的乘积得到  $R1$ 。用户 U1 将本步骤计算得到  $R1$  与步骤 302 中计算的  $R1$  进行比较, 如果相同, 则 K2、K3、K4 和 K5 正确, 否则错误。

其它用户也用上述方法对收到的中间值进行验证。

步骤 605: 验证通过后, 用户 U1 根据 K1、K2、K3、K4 和 K5 得到  $R1$ 、 $R2$ 、 $R3$ 、 $R4$  和  $R5$ , 计算会话密钥  $S=R1R2R3R4R5$ , 同理, 其它用户也计算出会话密钥  $S=R1R2R3R4R5$ 。

当用户 U6 要加入以上的组群时, 可以采用如下方法生成组群密钥:

用户 U6 随机选择  $x6 \in Z_q^*$ , 计算公开值  $X6=g^{x6}$ , 然后用户 U6 与 U1 和 U5 交换公开值。U1、U5 以及 U6 计算共享的密钥  $KT=Q^{x1x5x6}$ 。

U1 和 U5 以会话密钥  $S$  为密钥加密  $KT$ , 并将密文以广播的形式发送给 U2, U3 和 U4。这样用户 U1, U2, U3, U4 和 U5 就共享了秘密  $S$  和  $KT$ 。

用户 U1, U2, U3, U4 和 U5 将  $S$  和  $KT$  进行连接, 然后进行 Hash 运算, 得到当前的组群密钥  $KK$ , 即  $KK=(S||KT)$ 。同时, U1 和 U5 用  $KT$  为密钥加密  $KK$ , 并将其发送给用户 U6, 使 U6 也拥有组群密钥  $KK$ 。

当用户 U6, U7 要求加入由用户 U1, U2, U3, U4, U5 构成的组群时, 组群密钥协商过程如下:

首先, 用户 U6 随机选择  $x6 \in Z_q^*$ , 计算公开值  $X6=g^{x6}$ ; U7 随机选择  $x7 \in Z_q^*$ , 计算公开值  $X7=g^{x7}$ 。用户 U6 与 U7, U1 和 U5 交换公开值, 同时, 用户 U7 与 U1, U5 和 U6 交换公开值。

然后, 用户 U5, U6 和 U7 计算得到  $S'=Q^{x5x6x7}$ 。用户 U6, U7 和 U1 计算得到  $KT'=Q^{x6x7x1}$ 。用户 U6, U7 以  $S'$  为密钥加密  $KT'$ , 并将加密后的密文发送给用户 U5。

接着, 用户 U5, U6 和 U7 分别计算  $KT=Hash(S'||KT')$ 。用户 U6, U7 以  $KT'$  为密钥加密  $KT$  并将加密后的密文发送给用户 U1, 使用户 U1 也拥有了  $KT$ 。

用户 U1 和 U5 以 S 为密钥加密 KT，并将密文以广播的形式发送给用户 U2，U3，U4，这样在用户 U1，U2，U3，U4，U5 中就共享了两个秘密值 S 和 KT。

这五个用户将秘密 S 和 KT 进行连接，然后进行 Hash 运算，得到当前的组群密钥 KK，即  $KK = H(S || KT)$ 。同时，用户 U1 和 U5 以 KT 为密钥加密 KK，并将密文其发送给用户 U6 和 U7，使得这两个用户也拥有组群密钥 KK。

当 U3 要退出由用户 U1，U2，U3，U4，U5 构成的组群。则将剩余的用户 U1，U2，U4，U5 组成新的组群，新组群中用户个数为偶数，执行上述组群密钥的协商方法的步骤 501 至步骤 512，生成组群密钥 KK。

### 实施例 2

10 参见图 7，本实施例提供了一种协商组群密钥的设备，包括：

信息交互模块 701，用于根据秘密指数生成公开值，分别与左侧的两个相邻设备和右侧的两个相邻设备交换公开值，以及与其它设备进行信息交互；

中间值生成模块 702，用于提取信息交互模块 701 收到的公开值中的秘密指数，根据公开值中的秘密指数和设备自身的秘密指数生成中间值，并通知信息交互模块 701 广播携带中间值的中间消息；

组群密钥生成模块 703，用于验证信息交互模块 701 收到的中间消息中的中间值，验证通过后，根据其它设备的中间值和自身的中间值生成会话密钥，将会话密钥作为组群密钥。

### 实施例 3

参见图 8，本实施例提供了一种协商组群密钥的设备，包括：

20 信息交互模块 801，用于根据秘密指数生成公开值，分别与左侧的两个相邻设备和右侧的两个相邻设备交换公开值，以及与其它设备进行信息交互；

中间值生成模块 802，用于提取信息交互模块 801 收到的公开值中的秘密指数，根据公开值中的秘密指数和设备自身的秘密指数生成中间值，并通过信息交互模块 801 广播携带中间值的中间消息；

25 会话密钥生成模块 803，用于验证信息交互模块 801 收到的中间消息中的中间值，验证通过后，根据收到的中间值和自身的中间值生成会话密钥；

新中间值生成模块 804，用于通知信息交互模块 801 与特定设备交换携带秘密指数的公开值，并根据接收到的特定设备的公开值中的秘密指数和设备自身的秘密指数生成新中间值；

30 组群密钥生成模块 805，用于根据新中间值生成模块 504 生成的新中间值和会话密钥生成新的组群密钥。

进一步地，上述设备还包括：

会话密钥加密模块，用于用新中间值生成模块 804 生成的新中间值加密会话密钥，并通过信息交互模块 801 将加密后的密文发送给特定设备；

中间值加密模块，用于用会话密钥对新中间值生成模块 804 生成的新中间值加密，并  
5 通过信息交互模块 801 广播加密后的新中间值。

#### 实施例 4

参见图 9，本实施例提供了一种协商组群密钥的设备，包括：

信息交互模块 901，用于根据秘密指数生成公开值，分别与组群中的多个设备交换公开值，以及与其它设备进行信息交互；

10 中间值生成模块 902，用于提取信息交互模块 901 收到的公开值中的秘密指数，根据公开值中的秘密指数和设备自身的秘密指数生成中间值；

会话密钥解密模块 903，用于用中间值生成模块 902 生成的中间值解密信息交互模块 901 收到的密文，得到会话密钥；

中间值加密模块 904，用于用会话密钥解密模块 903 解密出的会话密钥对中间值生成模  
15 块 902 生成的中间值加密，并通过信息交互模块 901 广播加密后的中间值。

上述方案中的全部或部分步骤可以通过指令控制相应的硬件完成，该指令可以存储于存储介质中，存储介质如计算机或服务器的硬盘或内存。

20 以上实施例提供的技术方案基于椭圆曲线的密码体制，基于椭圆曲线的密码体制与 RSA 和 El Gamal 等密码体制相比，具有很高的单比特安全性，并且在未来计算能力逐渐提升的情况下与 RSA 和 El Gamal 的体制相比具有更强的竞争力。

该体制可以在固定的通信轮数下完成密钥协商过程，也就是说该密钥协商的通信轮数与组群中成员的人数无关。相对于现有技术，本发明有如下优点：

25 a) 在多个用户加入的过程中，首先计算了要求加入的用户组群的共享密钥，然后将此密钥与原始组群的密钥进行合并得到更新的组群密钥，提高了协议的效率。

b) 密钥协商过程中用的通信轮数较少。例如，组群中有  $n$  个用户，如果应用现有技术，完成密钥协商过程需要进行  $\text{Log}(n)$  轮的通信，而使用本发明实施例提供的方案，只需要两轮的通信就可以完成，提高了通信的实时性。

30 c) 通信量小。由于密钥协商的轮数与成员的人数无关，使得在成员较多，即  $n$  比较大的情况下，可以明显的减小密钥协商的通信量。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

# 权 利 要 求 书

1. 一种协商组群密钥的方法，其特征在于，当组群内的用户总数为奇数时，所述方法包括：

5       步骤 A：用户根据秘密指数生成公开值，分别与左侧的两个相邻用户和右侧的两个相邻用户交换公开值；

      步骤 B：所述用户收到四个相邻用户发送的公开值后，根据所述公开值中的秘密指数和自身的秘密指数生成中间值，广播携带所述中间值的中间消息；

      步骤 C：所述用户收到其它用户的中间消息后，验证所述中间消息中的中间值是否正确，  
10   验证通过后，根据所述其它用户的中间值和自身的中间值生成会话密钥，将所述会话密钥作为组群密钥；

      当组群内的用户总数为偶数时，所述方法包括：

      步骤 A1：从组群中分离出一个用户，将所分离出的用户作为特定用户；将组群内的其余用户组成新的组群，所述新的组群内每个用户执行所述步骤 A 至所述步骤 C；

15       步骤 B1：所述特定用户与所述新的组群内的多个用户交换携带秘密指数的公开值；所述特定用户与所述多个用户根据收到的公开值中的秘密指数生成新中间值；

      步骤 C1：所述多个用户用所述新中间值加密所述会话密钥，并将加密后的密文发送给所述特定用户；所述特定用户收到所述密文后，用所述新中间值对所述密文解密，得到所述会话密钥；

20       步骤 D1：所述多个用户和所述特定用户用所述会话密钥加密所生成的新中间值，并广播加密后的所述新中间值；

      步骤 E1：所述特定用户和所述新的组群内的每个用户根据所述新中间值和所述会话密钥生成新的组群密钥。

25       2. 如权利要求 1 所述的协商组群密钥的方法，其特征在于，所述方法基于椭圆曲线的双线性对映射，系统参数包括两个阶为  $q$ ，且建立在椭圆曲线上的循环乘群  $G1$  和  $G2$ ， $g$  是所述循环乘群  $G1$  的生成子，所述  $G1$  和  $G2$  有可计算的双线性映射， $g$  与  $g$  的双线性映射为  $Q$ 。

3. 如权利要求 2 所述的协商组群密钥的方法，其特征在于，所述步骤 A 包括：

30       用户从  $Z_q^*$  中选择一个随机数作为秘密指数，以所述系统参数中的  $g$  为底数，所述秘密指数为指数得到公开值，并将所述公开值发送给左侧相邻的两个用户和右侧相邻的两个用

户。

4. 如权利要求 2 所述的协商组群密钥的方法，其特征在于，所述步骤 B 包括：

所述用户收到所述相邻用户发送的公开值后，以所述系统参数中的  $Q$  为底数，以左侧  
5 相邻用户发送的公开值中的秘密指数和自身的秘密指数的乘积为指数生成左侧共享密钥；  
以右侧相邻用户发送的公开值中的秘密指数和自身的秘密指数的乘积为指数生成右侧共享  
密钥；

所述用户将所述右侧共享密钥除以左侧共享密钥，得到中间值，广播携带所述中间值  
的中间消息。

10

5. 如权利要求 4 所述的协商组群密钥的方法，其特征在于，所述步骤 C 包括：

所述用户收到其它用户的中间消息后，根据所收到的中间消息中的中间值计算左侧共  
享密钥，比较计算的所述左侧共享密钥与所述步骤 B 中生成的左侧共享密钥是否相等，如  
果相等，则判断所收到的中间消息中的中间值正确；

15

验证通过后，根据所述其它用户的中间值和自身的中间值计算其它用户的右侧共享密  
钥，将每个右侧共享密钥相乘得到会话密钥；

将所述会话密钥作为组群密钥。

6. 如权利要求 1 所述的协商组群密钥的方法，其特征在于，所述步骤 E1 包括：

20

所述特定用户和所述新的组群内的每个用户将所述新中间值和所述会话密钥进行连  
接，对连接后的结果进行哈希运算得到新的组群密钥。

7. 如权利要求 1 所述的协商组群密钥的方法，其特征在于，当有多个新用户加入原组  
群时，所述方法还包括：

25

从所述原组群中选出多个用户，将所选出的多个用户与所述多个新用户组成新的组群，  
根据新的组群中用户的总数执行所述步骤 A 至所述步骤 C 或所述步骤 A1 至所述步骤 E1，  
得到所述新的组群的组群密钥；

所述选出的多个用户用所述会话密钥加密所述新组群的组群密钥，并广播加密后的密  
文；

30

所述原组群中用户收到所述密文后，用所述会话密钥解密得到所述新组群的组群密钥；  
所述原组群中的用户根据所述会话密钥和所述新组群的组群密钥生成当前组群的组群密

钥;

所述选出的多个用户用所述新组群的组群密钥加密所述当前组群的组群密钥, 并将加密后的密钥发送给所述多个新用户;

所述多个新用户对加密后的密钥进行解密, 得到所述当前组群的组群密钥。

5

8. 如权利要求 1 所述的协商组群密钥的方法, 其特征在于, 当有多个用户退出原组群时, 所述方法还包括:

将所述原组群中剩余的用户组成新的组群, 根据新的组群中用户的总数执行所述步骤 A 至所述步骤 C 或所述步骤 A1 至所述步骤 E1, 得到所述新的组群的组群密钥。

10

9. 一种协商组群密钥的设备, 其特征在于, 所述设备包括:

信息交互模块 (701), 用于根据秘密指数生成公开值, 分别与左侧的两个相邻设备和右侧的两个相邻设备交换公开值, 以及与其它设备进行信息交互;

15 中间值生成模块 (702), 用于提取所述信息交互模块 (701) 收到的公开值中的秘密指数, 根据所述公开值中的秘密指数和本地设备自身的秘密指数生成中间值, 并通知所述信息交互模块 (701) 广播携带所述中间值的中间消息;

组群密钥生成模块 (703), 用于验证所述信息交互模块 (701) 收到的中间消息中的中间值, 验证通过后, 根据所述其它设备的中间值和自身的中间值生成会话密钥, 将所述会话密钥作为组群密钥。

20

10. 一种协商组群密钥的设备, 其特征在于, 所述设备包括:

信息交互模块 (801), 用于根据秘密指数生成公开值, 分别与左侧的两个相邻设备和右侧的两个相邻设备交换公开值, 以及与其它设备进行信息交互;

25 中间值生成模块 (802), 用于提取所述信息交互模块 (801) 收到的公开值中的秘密指数, 根据所述公开值中的秘密指数和本地设备自身的秘密指数生成中间值, 并通过所述信息交互模块广播携带所述中间值的中间消息;

会话密钥生成模块 (803), 用于验证所述信息交互模块 (801) 收到的中间消息中的中间值, 验证通过后, 根据收到的中间值和自身的中间值生成会话密钥;

30 新中间值生成模块 (804), 用于通知所述信息交互模块 (801) 与特定设备交换携带秘密指数的公开值, 并根据接收到的所述特定设备的公开值中的秘密指数和设备自身的秘密指数生成新中间值;

组群密钥生成模块（805），用于根据所述新中间值生成模块（804）生成的新中间值和所述会话密钥生成新的组群密钥。

11. 如权利要求 10 所述的协商组群密钥的设备，其特征在于，所述设备还包括：

会话密钥加密模块，用于利用所述新中间值生成模块生成的新中间值加密所述会话密  
5 钥，并通过所述信息交互模块将加密后的密文发送给所述特定设备；

中间值加密模块，用于利用所述会话密钥对所述新中间值生成模块生成的新中间值加密，并通过所述信息交互模块广播加密后的所述新中间值。

12. 一种协商组群密钥的设备，其特征在于，所述设备包括：

10 信息交互模块（901），用于根据秘密指数生成公开值，分别与组群中的多个设备交换公开值，以及与其它设备进行信息交互；

中间值生成模块（902），用于提取所述信息交互模块（801）收到的公开值中的秘密指数，根据所述公开值中的秘密指数和设备自身的秘密指数生成中间值；

会话密钥解密模块（903），用于利用所述中间值生成模块（902）生成的中间值解密所  
15 述信息交互模块收到的密文，得到会话密钥；

中间值加密模块（904），用于利用所述会话密钥解密模块（903）解密出的会话密钥对所述中间值生成模块（902）生成的中间值加密，并通过所述信息交互模块（901）广播加密后的所述中间值。

说明书附图

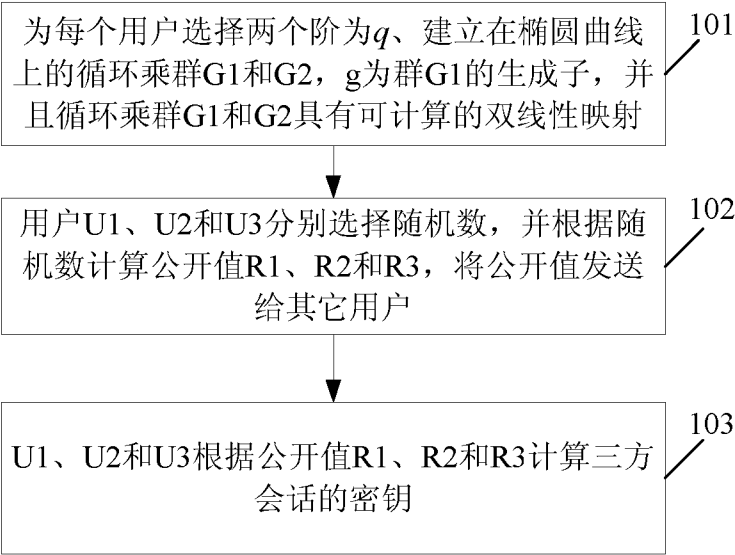


图 1

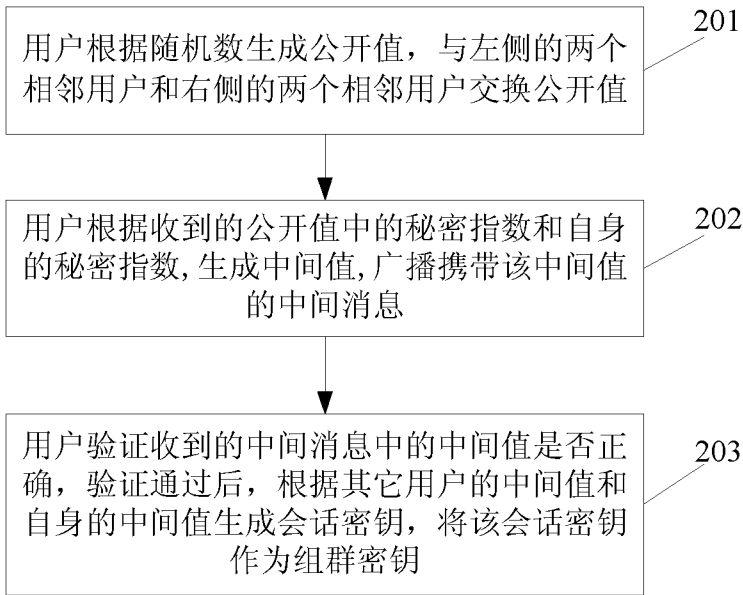


图 2

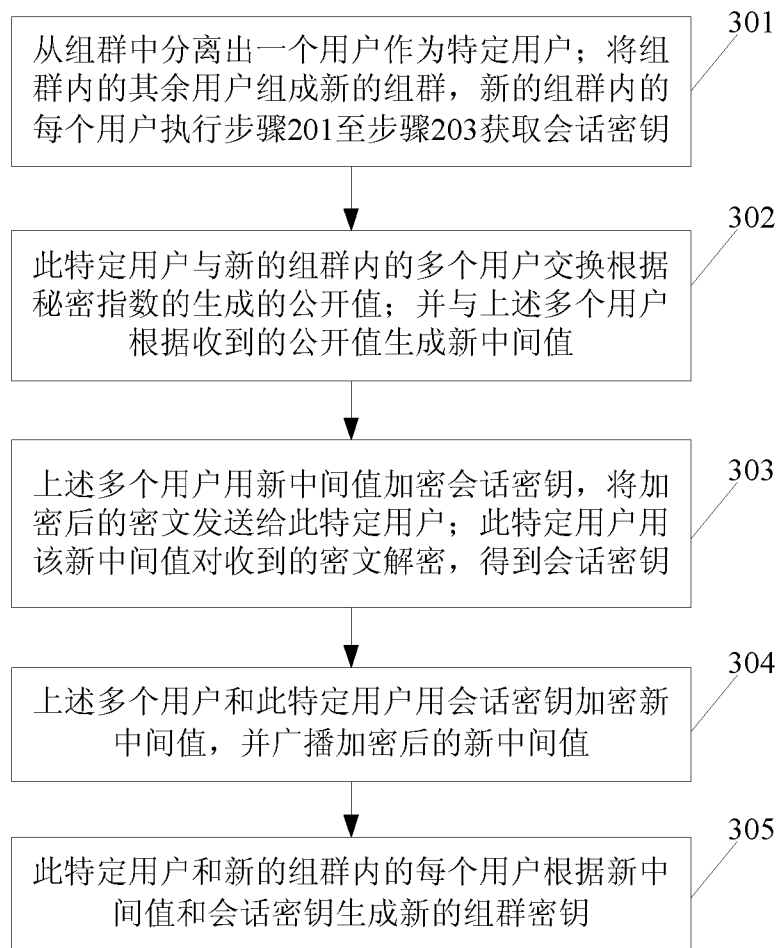


图 3

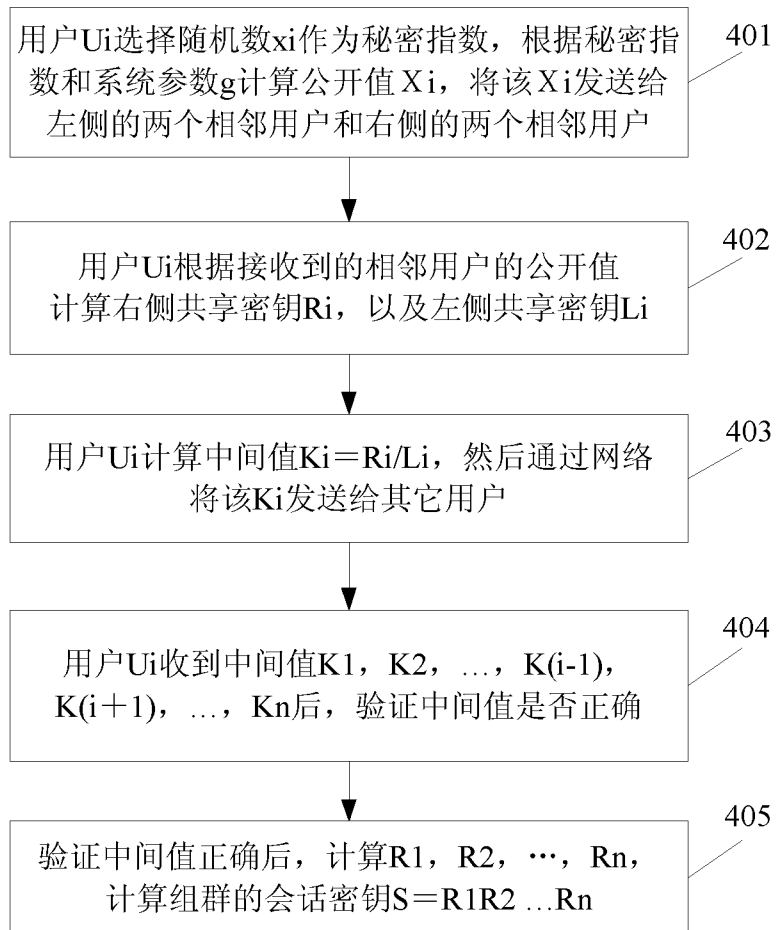


图 4



图 5

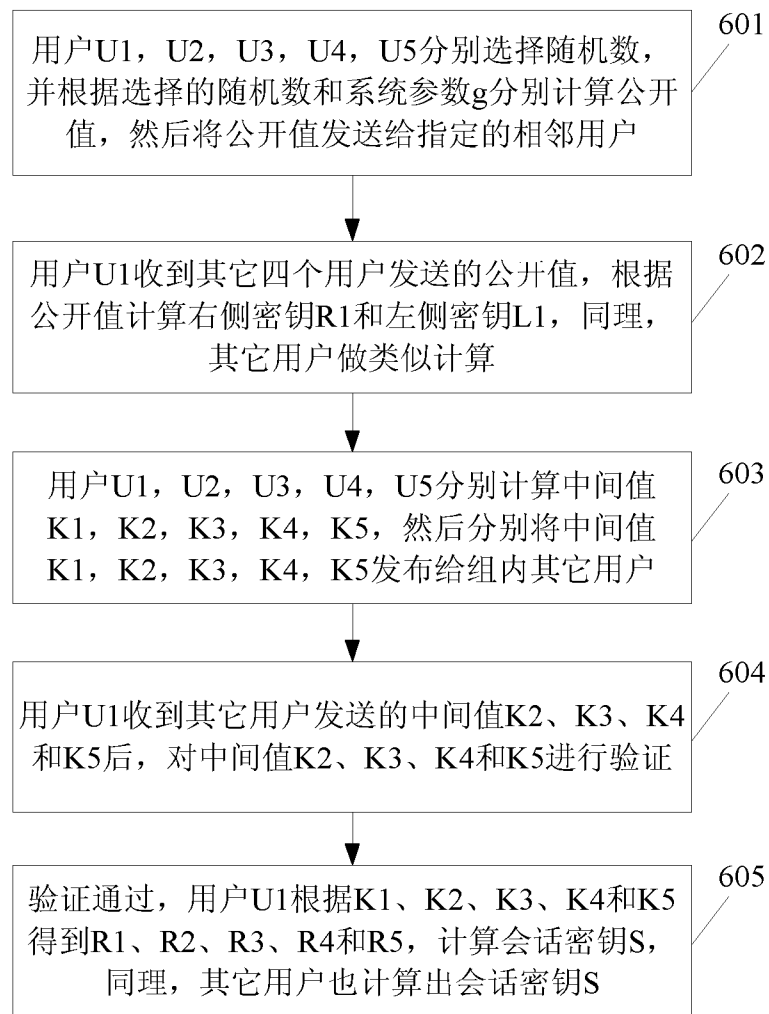


图 6

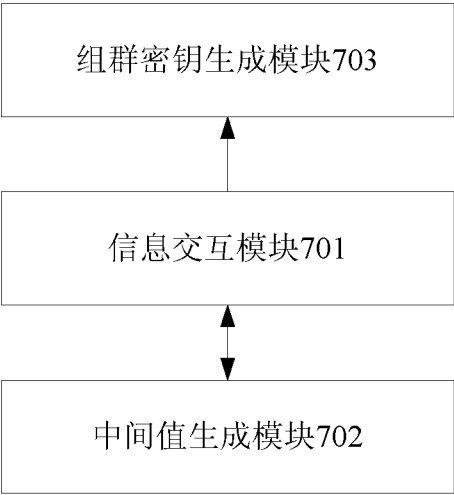


图 7

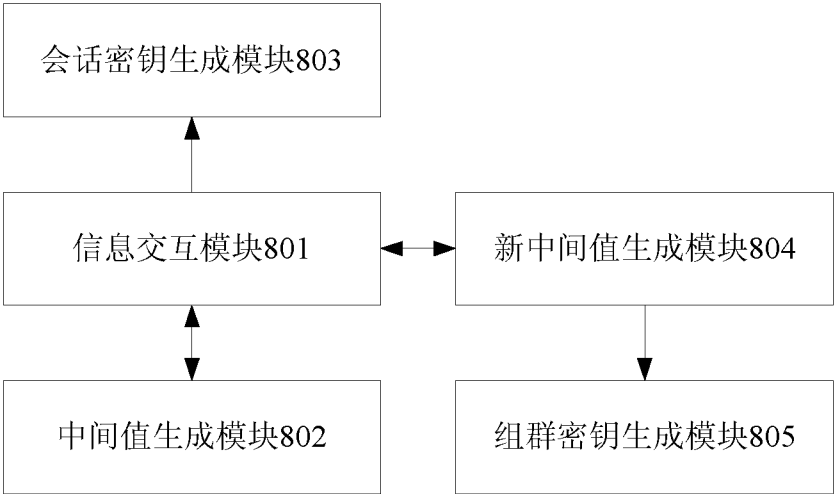


图 8

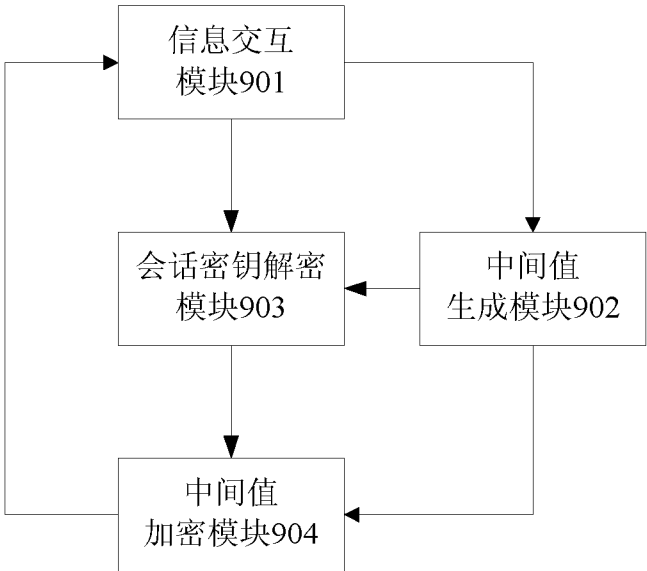


图 9

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2008/072434

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; H04M; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT;CNKI;WPI;EPODOC;PAJ

key; clear; middle; group; agreement; dynamic; ellipse; curve; mapping; neighbor; odd; even; bilinear; dual linear

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                               | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | LI Xin, ZHANG Peng, YE Chengqing An efficient dynamic group key agreement protocol<br>Journal of Zhejiang University 28 Feb. 2007(28.02.2007) the whole document | 1-12                  |
| A         | XIAO Youan, LI Layuan Research on the Xiao's Key Agreement Scheme<br>Journal of Wuhan University of Technology 31 Dec. 2003(31.12.2003) the whole document       | 1-12                  |
| A         | CN1984077A (ALCATEL) 20 Jun. 2007 (20.06.2007) the whole document                                                                                                | 1-12                  |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

|                                                                                                                                                                          |                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Special categories of cited documents:                                                                                                                                 | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention                                              |
| "A" document defining the general state of the art which is not considered to be of particular relevance                                                                 | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone                                                                     |
| "E" earlier application or patent but published on or after the international filing date                                                                                | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family                                                                                                                                                                                                    |
| "O" document referring to an oral disclosure, use, exhibition or other means                                                                                             |                                                                                                                                                                                                                                                  |
| "P" document published prior to the international filing date but later than the priority date claimed                                                                   |                                                                                                                                                                                                                                                  |

|                                                                                                                                                                                                              |                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Date of the actual completion of the international search<br>16 Dec. 2008(16.12.2008)                                                                                                                        | Date of mailing of the international search report<br><b>15 Jan. 2009 (15.01.2009)</b> |
| Name and mailing address of the ISA/CN<br>The State Intellectual Property Office, the P.R.China<br>6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China<br>100088<br>Facsimile No. 86-10-62019451 | Authorized officer<br><b>ZHANG, Yan</b><br>Telephone No. (86-10)62411651               |

International application No.  
PCT/CN2008/072434

Form PCT/ISA/210 (patent family annex) (April 2007)

## 国际检索报告

国际申请号  
**PCT/CN2008/072434****A. 主题的分类**

H04L 9/08(2006.01)i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

**B. 检索领域**

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L ; H04M; H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT;CNKI;WPI;EPODOC;PAJ 密钥; 公开; 中间; 组; 协商; 协定; 动态; 群; 椭圆; 曲线; 映射; 相邻; 奇数; 偶数; 双线性; key; clear; middle; group; agreement; dynamic; ellipse; curve; mapping; neighbor; odd; even; bilinear; dual linear

**C. 相关文件**

| 类 型* | 引用文件, 必要时, 指明相关段落                                               | 相关的权利要求 |
|------|-----------------------------------------------------------------|---------|
| A    | 李欣, 张鹏, 叶澄清 一个有效的动态组密钥协商协议 浙江大学学报<br>28.2 月 2007(28.02.2007) 全文 | 1-12    |
| A    | 肖攸安, 李腊元 一类高效密钥协商方案的研究 武汉理工大学学报 31. 12<br>月 2003(31.12.2003) 全文 | 1-12    |
| A    | CN1984077A (阿尔卡特公司) 20. 6 月 2007(20.06.2007)全文                  | 1-12    |

☐ 其余文件在 C 栏的续页中列出。☒ 见同族专利附件。

\* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇  
引用文件的公布日而引用的或者因其他特殊理由而引  
用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了  
理解发明之理论或原理的在后文件“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的  
发明不是新颖的或不具有创造性“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件  
结合并且这种结合对于本领域技术人员为显而易见时,  
要求保护的发明不具有创造性

“&amp;” 同族专利的文件

国际检索实际完成的日期

16. 12 月 2008(16.12.2008)

国际检索报告邮寄日期

**15.1 月 2009 (15.01.2009)**

中华人民共和国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

授权官员

**张妍**电话号码: (86-10) **62411651**

### 关于同族专利的信息

PCT/CN2008/072434

PCT/ISA/210 表(同族专利附件) (2008 年 7 月)