(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105187205 A
(43)申请公布日 2015.12.23

(21)申请号 201510475808.X

(22)申请日 2015.08.05

(71)申请人 北京航空航天大学
地址 100191 北京市海淀区学院路37号

(72)发明人 刘建伟 苏航 陶芮 冯伯昂
宋晨光 夏丹枫

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张大威

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/08(2006.01)

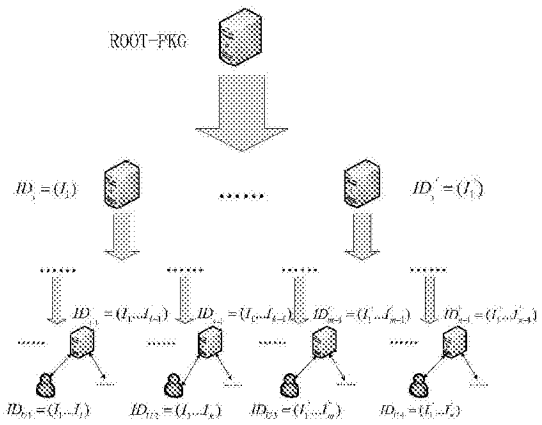
权利要求书3页 说明书8页 附图2页

(54)发明名称

无证书的基于层次身份基的认证密钥协商方法和协商系统

(57)摘要

本发明公开了一种无证书的基于层次身份基的认证密钥协商方法和协商系统，所述方法包括：根据输入的安全常数，得出椭圆曲线循环加法群，选取主私钥和两个安全的哈希函数，计算系统公钥；根据主私钥、第一用户身份和选取的一组随机数，计算第一用户的部分私钥和部分公钥；根据第一用户的部分私钥和选取的一个随机数，计算第一用户的私钥；根据所述第一用户上层用户身份、所述上层用户的部分私钥和部分公钥和一个随机数，计算第一用户的部分私钥和部分公钥；根据第二用户和第三用户选取的临时信息、私钥、公钥，计算会话密钥。本发明具有如下优点：适用于大型系统；效率高；无密钥托管问题；满足密钥协商的安全需求。



CN 105187205 A

1.一种无证书的基于层次身份基的认证密钥协商方法，其特征在于，包括以下步骤：

A：根据输入的安全常数 λ，得出阶数为 q 的椭圆曲线循环加法群$\mathbb{G}$、其生成元为 P，选取主私钥 msk，计算公钥 P_{pub}，选取安全的哈希函数 H_1和哈希函数 H_2；

B：根据第一用户的身份向量 ID = $(I_1, I_2, \ldots, I_t)$，可以通过两种算法生成所述第一用户的私钥 d：

B1：根据所述主私钥 msk、所述第一用户身份向量 ID = $(I_1, I_2, \ldots, I_t)$ 和随机选取的$g_1, \ldots, g_t \in \mathbb{Z}_q^*$，根 PKG 计算所述第一用户的部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，所述第一用户验证所述部分私钥 k 是否满足验证条件，如果所述部分私钥 k 满足验证条件，所述第一用户接受所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$；

B2：根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及第一用户随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥 d 和公钥 pk；

或

B′ 1：根据所述第一用户的身份向量 ID = $(I_1, I_2, \ldots, I_t)$、所述第一用户的上层用户的身份向量 ID_{PKG} = $(I_1, I_2, \ldots, I_{t-1})$、所述上层用户的部分私钥 k′、部分公钥 $\{g_1P, \ldots, g_{t-1}P\}$ 和随机选取的$g_t \in \mathbb{Z}_q^*$，所述上层用户的 PKG 为所述第一用户生成部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，所述第一用户验证所述部分私钥 k 是否满足验证条件，如果所述部分私钥 k 满足验证条件，所述第一用户接受所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$；

B′ 2：根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及第一用户随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥 d 和公钥 pk。

2.根据权利要求 1 所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，所述步骤 A 进一步包括：

所述椭圆曲线循环加法群$\mathbb{G}$为满足安全常数 λ 的阶为 q 的椭圆曲线循环加法群；

所述公钥 P_{pub} = sP，其中主私钥 msk = s；

所述哈希函数$H_1 : \{0,1\}^* \times \mathbb{G} \to \mathbb{Z}_q^*$；以及

所述哈希函数$H_2 : \mathbb{G} \times \mathbb{G} \to \mathcal{K}$，其中$\mathcal{K}$为会话密钥空间。

3.根据权利要求 2 所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，所述步骤 B1 进一步包括：

根据所述主私钥 msk、所述第一用户身份向量 ID = $(I_1, I_2, \ldots, I_t)$ 和所述根 PKG 随机选取的$g_1, \ldots, g_t \in \mathbb{Z}_q^*$，计算 $r_i = H_1(I_i || g_iP)$，其中 $1 \leqslant i \leqslant t$，所述第一用户的部分私钥 k 为：

$$k = s + \sum_{i=1}^{t} (g_i r_i)$$

如果 k = 0，则需要重新选取$g_1, \ldots, g_t \in \mathbb{Z}_q^*$，通过安全信道将 $\{g_1P, \ldots, g_tP, k\}$ 发送给所述第一用户，其中 $g_1P, \ldots, g_tP$ 为所述第一用户的部分公钥，所述第一用户验证下列等式：

$$kP = P_{pub} + \sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

若等式不成立，则拒绝所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$。

4. 根据权利要求 3 所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，所述步骤 B2 进一步包括：

随机选取$x \in \mathbb{Z}_q^*$，生成所述第一用户的的私钥 d，

d = k+x

如果 d = 0，重新选取$x \in \mathbb{Z}_q^*$计算所述第一用户的私钥 d，所述第一用户的公钥为 pk = {ID, $g_1P, \ldots, g_tP$, xP}。

5. 根据权利要求 2 所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，所述步骤 B′ 1 进一步包括：

根据所述第一用户的身份向量 ID = $(I_1, I_2, \ldots, I_t)$、所述第一用户的上层用户 ID_{PKG} = $(I_1, I_2, \ldots, I_{t-1})$、所述上层用户的部分私钥$k' = s + \sum_{i=1}^{t-1}(g_ir_i)$，所述上层用户的部分公钥 $\{g_1P, \ldots, g_{t-1}P\}$ 和随机选取$g_t \in \mathbb{Z}_q^*$，计算 $r_t = H_1(I_t||g_tP)$，所述上层用户的 PKG 为所述第一用户生成所述部分私钥 k，所述部分私钥 k 通过以下公式得到：

$$k = k' + g_tr_t = s + \sum_{i=1}^{t-1}(g_ir_i) + g_tr_t = s + \sum_{i=1}^{t}(g_ir_i),$$

如果 k = 0，则重新选取$g_t \in \mathbb{Z}_q^*$并计算所述部分私钥 k，通过安全信道将 $\{g_1P, \ldots, g_tP, k\}$ 发送给所述第一用户，其中 $g_1P, \ldots, g_tP$ 为所述第一用户的部分公钥，所述第一用户验证下列等式：

$$kP = P_{pub} + \sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

若等式不成立，所述第一用户拒绝所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$。

6. 根据权利要求 5 所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，所述步骤 B′ 2 进一步包括：

随机选取$x \in \mathbb{Z}_q^*$，生成所述第一用户的的私钥 d，

d = k+x

如果 d = 0，重新选取$x \in \mathbb{Z}_q^*$计算所述第一用户的私钥 d，所述第一用户的公钥为 pk = {ID, $g_1P, \ldots, g_tP$, xP}。

7. 根据权利要求 1-6 任一所述的无证书的基于层次身份基的认证密钥协商方法，其特征在于，在步骤 B 还包括以下步骤：

C：随机选择第二用户 A 和第三用户 B，根据所述第二用户 A 的身份向量 $ID=(I_1, I_2, \ldots, I_{l_A})$、第二用户私钥 d_A、第二用户公钥 pk_A和所述第三用户 B 的身份向量 $ID = (I_1', I_2', \ldots, I_{l_B}')$、第三用户私钥 d_B、第三用户公钥 pk_B，以及第二用户和第三用户分别随机选取的$a \in \mathbb{Z}_q^*$和$b \in \mathbb{Z}_q^*$，计算所述第二用户 A 向所述第三用户 B 发消息使用的第一会

话密钥 sk_A和所述第三用户 B 向所述第二用户 A 发消息使用的第二会话密钥 sk_B，如果所述第一会话密钥 sk_A和所述第二会话密钥 sk_B相同，所述第二用户 A 和所述第三用户 B 之间可进行安全通信。

8. 一种无证书的基于层次身份基的认证密钥协商系统，其特征在于，包括：

系统建立模块，用于根据输入的安全常数 λ，得出阶数为 q 椭圆曲线循环加法群$\mathbb{G}$、其生成元为 P，选取主私钥 msk，计算公钥 P_{pub}，选取安全的哈希函数 H_1和哈希函数 H_2；

私钥生成模块，所述私钥生成模块用于根据所述主私钥 msk、所述第一用户身份向量 $ID = (I_1, I_2, \ldots, I_t)$ 和随机选取的$g_1, \ldots, g_t \in \mathbb{Z}_q^*$，计算所述第一用户的部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，通过验证模块验证后，并根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥 d 和公钥 pk，其中，$\mathbb{Z}_q^*$表示整数集合 {1, 2, ..., q-2, q-1}；

私钥委托模块，所述私钥委托模块用于根据所述第一用户的身份向量 $ID = (I_1, I_2, \ldots, I_t)$、所述第一用户的上层用户 $ID_{PKG} = (I_1, I_2, \ldots, I_{t-1})$、所述上层用户的部分私钥 k′、部分公钥 $\{g_1P, \ldots, g_{t-1}P\}$ 和随机选取的$g_t \in \mathbb{Z}_q^*$生成所述第一用户的部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，通过所述验证模块验证后，并根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥 d 和公钥 pk，其中，$\mathbb{Z}_q^*$表示整数集合 {1, 2, ..., q-2, q-1}；

验证模块，所述验证模块用于对所述私钥生成模块生成的所述部分私钥 k 和所述私钥委托模块生成的所述部分私钥 k 进行验证。

9. 根据权利要求 8 所述的无证书的基于层次身份基的认证密钥协商系统，其特征在于，还包括：

密钥协商模块，所述密钥协商模块用于任意第二用户 A 和第三用户 B，根据所述第二用户 A 的身份向量$ID = (I_1, I_2, \ldots, I_{l_A})$、第二用户私钥 d_A、第二用户公钥 pk_A和所述第三用户 B 的身份向量$ID = (I'_1, I'_2, \ldots, I'_{l_B})$、第三用户私钥 d_B、第三用户公钥 pk_B，以及第二用户和第三用户分别随机选取的$a \in \mathbb{Z}_q^*$和$b \in \mathbb{Z}_q^*$，计算所述第二用户 A 向所述第三用户 B 发送消息使用的第一会话密钥 sk_A和所述第三用户 B 向所述第二用户 A 发消息使用的第二会话密钥 sk_B，如果所述第一会话密钥 sK_A和所述第二会话密钥 sk_B相同，所述第二用户 A 和所述第三用户 B 之间可进行安全通信。

无证书的基于层次身份基的认证密钥协商方法和协商系统

技术领域

[0001] 本发明涉及无证书的密码体制，具体涉及一种无证书的基于层次身份基的认证密钥协商方法和协商系统。

背景技术

[0002] 公钥密码体制是保证网络和信息安全的重要技术。在传统的公钥基础设施(PKI，Public Key Infrastructure)中，需要可信第三方为用户颁发证书来证明用户的合法身份，因此涉及到很多证书管理的问题，占用了大量系统相关资源。为了简化传统公钥基础设施对证书的管理过程，Shamir在1984年提出了一种身份基密码体制(IBC，Identity Based Cryptosystem)。该体制不使用证书，直接将用户的身份作为公钥，私钥由可信的私钥生成中心PKG(Public Key Generator)生成。

[0003] 然而在Shamir提出的IBC体制中，用户的私钥完全由PKG生成，若PKG受到攻击造成信息泄露，则攻击者可以获得用户的长期私钥，以此来假冒用户。这就是IBC体制固有的密钥托管问题。为了解决这一问题，Al-Riyami和Paterson在2003年提出了无证书的身份基密码体制(CLIBC，CertificatelessIdentity Based Cryptosystem)。在这一体制中，PKG只为用户生成部分私钥，完整的私钥由用户结合PKG生成的部分私钥以及自身选定的私有秘密值共同生成。因此，无证书密码体制既解决了传统公钥密码体制中的证书管理问题，又解决了身份基密码体制中的密钥托管问题。

[0004] 在IBE和CLIBE体制中均只含有一个PKG。PKG不仅承担着验证用户身份及为用户生成私钥的任务，还要承担维护安全信道以便把私钥安全的发送给用户的任务，同时PKG还要负责用户私钥的更新，撤销等工作。显然，单一PKG将不能承担起大型系统繁重的工作。为了解决这一问题，密码学家Gentry和Silverberg与2002年第一次提出了层次身份基密码体制(HIBC，Hierarchical Identity Based Cryptography)。该体制中包含一个根PKG及多层的域PKG，根PKG验证域PKG并为其生成私钥，上层域PKG验证下层域PKG并为其生成私钥，直至用户的上一层域。不过在HIBC体制中仍然存在密钥托管问题。2008年，Chow、Roth和Rieffel则首次对无证书的分层密码体制(HCLC，Hierarchical Certificateless Cryptography)进行了研究。这一体制既保留了HIBC体制的优点，又避免了HIBC体制中的密钥托管问题。

[0005] 密钥协商作为密码学中的基础部分，在安全通信中有至关重要的作用。它允许两个实体在开放信道上协商安全的会话密钥，以保证双方通信的安全。基于无证书的身份基密码体制，学者们提出了大量的无证书的身份基认证密钥协商协议。然而，大多数无证书身份基认证密钥协商协议都是在单一PKG环境下提出的。同时，椭圆曲线上的双线性对运算耗时大约是点乘运算的20倍，因此效率较低。针对这一问题，有学者提出了无双线性对运算的无证书的身份基密钥协商协议，不过这类协议也都是在单一PKG环境下提出的。

[0006] 椭圆曲线密码(ECC，Elliptic curve cryptography)与其他公钥密码体制相比，其主要优势是在相同的安全水平下系统参数更短，因此在身份基密码体制中运用最为广

泛。在无双线性对运算的密钥协商协议中，协议的安全性一是基于椭圆曲线离散对数困难假设，即$\mathbb{G}$为椭圆曲线上的q阶循环加法群，给定两个元素$P, aP \in \mathbb{G}$，其中$a \in \mathbb{Z}_q^*$，由P，aP计算a是困难的，但由P，a计算aP是容易的。二是基于计算性Diffie-Hellman困难假设，即$\mathbb{G}$为椭圆曲线上的q阶循环加法群，给定三个元素$P, aP, bP \in \mathbb{G}$，其中$a, b \in \mathbb{Z}_q^*$，计算abP是困难的。

发明内容

[0007] 本发明旨在至少解决上述技术问题之一。

[0008] 为此，本发明的第一个目的在于提出一种无证书的基于层次身份基的认证密钥协商方法。

[0009] 本发明的第二个目的在于提出一种无证书的基于层次身份基的认证密钥协商系统。

[0010] 为了实现上述目的，本发明的的实施例公开了一种无证书的基于层次身份基的认证密钥协商方法，包括以下步骤：A：根据输入的安全常数 λ，得出阶数为q的椭圆曲线循环加法群$\mathbb{G}$、其生成元为P，选取主私钥msk，计算公钥P_{pub}，选取安全的哈希函数H_1和哈希函数H_2；B：根据第一用户的身份向量ID＝(I_1，I_2，...，I_t)，可以通过两种算法生成所述第一用户的私钥d：B1：根据所述主私钥msk、所述第一用户身份向量ID＝(I_1，I_2，...，I_t)和随机选取的$g_1, \cdots, g_t \in \mathbb{Z}_q^*$，根PKG计算所述第一用户的部分私钥k和部分公钥$g_1P$，...，$g_tP$，所述第一用户验证所述部分私钥k是否满足验证条件，如果所述部分私钥k满足验证条件，所述第一用户接受所述部分私钥k和部分公钥g_1P，...，g_tP；B2：根据所述部分私钥k和部分公钥g_1P，...，g_tP及随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥d和公钥pk；或B′ 1：根据所述第一用户的身份向量ID＝(I_1，I_2，...，I_t)、所述第一用户的上层用户的身份向量ID_{PKG}＝(I_1，I_2，...，I_{t-1})、所述上层用户的部分私钥k′、部分公钥{g_1P，...，$g_{t-1}P$}和随机选取的$g_t \in \mathbb{Z}_q^*$，所述上层用户的PKG为所述第一用户生成部分私钥k和部分公钥g_1P，...，g_tP，所述第一用户验证所述部分私钥k是否满足验证条件，如果所述部分私钥k满足验证条件，所述第一用户接受所述部分私钥k和部分公钥g_1P，...，g_tP；B′ 2：根据所述部分私钥k和部分公钥g_1P，...，g_tP及随机选取的$x \in \mathbb{Z}_q^*$生成所述第一用户的私钥d和公钥pk。

[0011] 根据本发明实施例的无证书的基于层次身份基的认证密钥协商方法，基于无证书的层次身份基密码体制，适用于大型系统，而且方法在运算过程中不含双线性对运算，因此具有更高的效率。方法的安全性基于椭圆曲线离散对数困难假设及计算性Diffie-Hellman困难假设，满足密钥协商系统所需的基本安全需求。

[0012] 另外，根据本发明上述实施例的无证书的基于层次身份基的认证密钥协商方法，还可以具有如下附加的技术特征：

[0013] 进一步地，所述步骤A进一步包括：所述椭圆曲线循环加法群$\mathbb{G}$为满足安全常数 λ 的阶为q的椭圆曲线循环加法群；所述公钥P_{pub}＝ sP，其中主私钥msk ＝ s；所述哈希函

数$H_1:\{0,1\}^* \times \mathbb{G} \to \mathbb{Z}_q^*$；以及所述哈希函数$H_2:\mathbb{G} \times \mathbb{G} \to \mathcal{K}$，其中$\mathcal{K}$为会话密钥空间。

[0014] 进一步地，所述步骤B1进一步包括：根据所述主私钥msk、所述第一用户身份向量ID＝(I_1,I_2,...,I_t)和所述根PKG随机选取的$g_1,\dots,g_t \in \mathbb{Z}_q^*$，计算$r_i = H_1(I_i||g_iP)$，其中1≤i≤t，所述第一用户的部分私钥k为：

[0015] $$k = s + \sum_{i=1}^{t}(g_i r_i)$$

[0016] 如果k＝0，则需要重新选取$g_1,\dots,g_t \in \mathbb{Z}_q^*$，通过安全信道将{$g_1P$,...,$g_tP$,k}发送给所述第一用户，其中$g_1P$,...,$g_tP$为所述第一用户的部分公钥，所述第一用户验证下列等式：

[0017] $$kP = P_{pub} + \sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

[0018] 若等式不成立，则拒绝所述部分私钥k和部分公钥g_1P,...,g_tP。

[0019] 进一步地，所述步骤B2进一步包括：随机选取$x \in \mathbb{Z}_q^*$，生成所述第一用户的的私钥d，

[0020] d＝k+x

[0021] 如果d＝0，重新选取$x \in \mathbb{Z}_q^*$计算所述第一用户的私钥d，所述第一用户的公钥为pk＝{ID,g_1P,...,g_tP,xP}。

[0022] 进一步地，所述步骤B′ 1进一步包括：根据所述第一用户的身份向量ID＝(I_1,I_2,...,I_t)、所述第一用户上层用户ID_{PKG}＝(I_1,I_2,...,I_{t-1})、所述上层用户的部分私钥$k' = s + \sum_{i=1}^{t-1}(g_i r_i)$，所述上层用户的部分公钥{$g_1P$,...,$g_{t-1}P$}和随机选取$g_t \in \mathbb{Z}_q^*$，计算$r_t = H_1(I_t||g_tP)$，所述上层用户的PKG为所述第一用户生成所述部分私钥k，所述部分私钥k通过以下公式得到：

[0023] $$k = k' + g_t r_t = s + \sum_{i=1}^{t-1}(g_i r_i) + g_t r_t = s + \sum_{i=1}^{t}(g_i r_i),$$

[0024] 如果k＝0，则需要重新选取$g_t \in \mathbb{Z}_q^*$计算所述部分私钥k，通过安全信道将{g_1P,...,g_tP,k}发送给所述第一用户，其中g_1P,...,g_tP为所述第一用户的部分公钥，所述第一用户验证下列等式：

[0025] $$kP = P_{pub} + \sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

[0026] 若等式不成立，所述第一用户拒绝所述部分私钥k和部分公钥g_1P,...,g_tP。

[0027] 进一步地，所述步骤B′ 2进一步包括：随机选取$x \in \mathbb{Z}_q^*$，生成所述第一用户的的私钥d，

[0028] $d = k+x$

[0029] 如果 $d = 0$，重新选取 $x \in \mathbb{Z}_q^*$ 计算所述第一用户的私钥 d，所述第一用户的公钥为 $pk = \{ID, g_1P, \ldots, g_tP, xP\}$。

[0030] 进一步地，在步骤 B 还包括以下步骤：

[0031] C：随机选择第二用户 A 和第三用户 B，根据所述第二用户 A 的身份向量 $ID=(I_1, I_2, \ldots, I_{l_A})$、第二用户私钥 d_A、第二用户公钥 pk_A 和所述第三用户 B 的身份向量 $ID = (I'_1, I'_2, \ldots, I'_{l_B})$、第三用户私钥 d_B、第三用户公钥 pk_B，以及第二用户和第三用户随机选取的 $a \in \mathbb{Z}_q^*$ 和 $b \in \mathbb{Z}_q^*$，计算所述第二用户 A 向所述第三用户 B 发消息使用的第一会话密钥 sk_A 和所述第三用户 B 向所述第二用户 A 发消息使用的第二会话密钥 sk_B，如果所述第一会话密钥 sk_A 和所述第二会话密钥 sk_B 相同，所述第二用户 A 和所述第三用户 B 之间可进行安全通信。

[0032] 为了实现上述目的，本发明的的实施例公开了一种无证书的基于层次身份基的认证密钥协商系统，包括：系统建立模块，用于根据输入的安全常数 λ，得出阶数为 q 椭圆曲线循环加法群 $\mathbb{G}$、其生成元为 P，选取主私钥 msk，计算公钥 P_{pub}，选取安全的哈希函数 H_1 和哈希函数 H_2；私钥生成模块，所述私钥生成模块用于根据所述主私钥 msk、所述第一用户身份向量 $ID = (I_1, I_2, \ldots, I_t)$ 和随机选取的 $g_1, \ldots, g_t \in \mathbb{Z}_q^*$，计算所述第一用户的部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，通过验证模块验证后，并根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及随机选取的 $x \in \mathbb{Z}_q^*$ 生成所述第一用户的私钥 d 和公钥 pk，其中，$\mathbb{Z}_q^*$ 表示整数集合 $\{1, 2, \ldots, q-2, q-1\}$；私钥委托模块，所述私钥委托模块用于根据所述第一用户的身份向量 $ID = (I_1, I_2, \ldots, I_t)$、所述第一用户的上层用户 $ID_{PKG} = (I_1, I_2, \ldots, I_{t-1})$、所述上层用户的部分私钥 k′、部分公钥 $\{g_1P, \ldots, g_{t-1}P\}$ 和随机选取的 $g_t \in \mathbb{Z}_q^*$ 生成所述第一用户的部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$，通过所述验证模块验证后，并根据所述部分私钥 k 和部分公钥 $g_1P, \ldots, g_tP$ 及随机选取的 $x \in \mathbb{Z}_q^*$ 生成所述第一用户的私钥 d 和公钥 pk，其中，$\mathbb{Z}_q^*$ 表示整数集合 $\{1, 2, \ldots, q-2, q-1\}$；验证模块，所述验证模块用于对所述私钥生成模块生成的所述部分私钥 k 和所述私钥委托模块生成的所述部分私钥 k 进行验证。

[0033] 根据本发明实施例的无证书的基于层次身份基的认证密钥协商系统，基于无证书的层次身份基密码体制，适用于大型系统，而且方法在运算过程中不含双线性对运算，因此具有更高的效率。方法的安全性基于椭圆曲线离散对数困难假设及计算性 Diffie-Hellman 困难假设，满足密钥协商系统所需的基本安全需求。

[0034] 另外，根据本发明上述实施例的无证书的基于层次身份基的认证密钥协商系统，还可以具有如下附加的技术特征：

[0035] 进一步地，还包括：密钥协商模块，所述密钥协商模块用于任意第二用户 A 和第三用户 B，根据所述第二用户 A 的身份向量 $ID = (I_1, I_2, \ldots, I_{l_A})$、第二用户私钥为 d_A、第二用

户公钥 pk_A 和所述第三用户 B 的身份向量 $ID = (I'_1, I'_2, \ldots, I'_{l_B})$、第三用户私钥 d_B、第三用户公钥 pk_B，以及第二用户和第三用户随机选取的 $a \in \mathbb{Z}_q^*$ 和 $b \in \mathbb{Z}_q^*$，计算所述第二用户 A 向所述第三用户 B 发送消息使用的第一会话密钥 sk_A 和所述第三用户 B 向所述第二用户 A 发消息使用的第二会话密钥 sk_B，如果所述第一会话密钥 sk_A 和所述第二会话密钥 sk_B 相同，所述第二用户 A 和所述第三用户 B 之间可进行安全通信。

[0036] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0037] 本发明的上述和 / 或附加的方面和优点从结合下面附图对实施例的描述中将变得明显和容易理解，其中：

[0038] 图 1 是本发明一个实施例的无证书的基于层次身份基的认证密钥协商系统的结构示意图；

[0039] 图 2 是本发明一个实施例的密钥协商过程的示意图。

具体实施方式

[0040] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。

[0041] 在本发明的描述中，需要理解的是，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性。

[0042] 参照下面的描述和附图，将清楚本发明的实施例的这些和其他方面。在这些描述和附图中，具体公开了本发明的实施例中的一些特定实施方式，来表示实施本发明的实施例的原理的一些方式，但是应当理解，本发明的实施例的范围不受此限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0043] 以下结合附图描述根据本发明实施例的无证书的基于层次身份基的认证密钥协商方法和协商系统。

[0044] 主要的符号及椭圆曲线选取：

[0045] 1) p，q：大素数

[0046] 2) $\mathbb{F}_p$：阶数为 p 的有限域

[0047] 3) $E/\mathbb{F}_p$：有限域 $\mathbb{F}_p$ 上的椭圆曲线 E

[0048] 4) $\mathbb{G}$：椭圆曲线 E 上的点的集合，为 q 阶的循环加法群

[0049] 5) P：群 G 的生成元

[0050] 6) $\mathbb{Z}_q^*$：整数集合 {1，2，...，q-2，q-1}

[0051] 7) PKG：私钥生成中心

[0052] 8) H_1：安全的哈希函数，$H_1: \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$

[0053] 9)H_2:安全的哈希函数，$H_2:\mathbb{G}\times\mathbb{G}\to\mathcal{K}$

[0054] 10)$\mathcal{K}$:会话密钥空间

[0055] 椭圆曲线$E/\mathbb{F}_p$可用等式表示为：

[0056] $y^2\equiv x^3+ax+b \bmod p$，其中$a,b\in\mathbb{F}_p$且$4a^3+27b^2\neq 0 \bmod p$群$\mathbb{G}=\{(x,y)|x,y\in\mathbb{F}_p,(x,y)\in E/\mathbb{F}_p\}\cup\{O\}$，O为无穷远点群$\mathbb{G}$为循环加法群，群运算为加法运算（点乘运算），描述如下：

[0057]

$$kP=\underbrace{P+P+\cdots+P}_{k},\quad k\in\mathbb{Z}_q^*$$

[0058] 本发明可分为系统建立，部分私钥生成，私钥生成，私钥委托和密钥协商五个阶段。该方法具体构造如下：

[0059] (1)(pp,msk)←Root-Setup(λ)：系统建立算法由根PKG运行，选取满足安全常数λ的阶为q的椭圆曲线循环加法群$\mathbb{G}$，即|q|=λ，$\mathbb{G}$的生成元为P。选取安全的哈希函数：$H_1:\{0,1\}^*\times\mathbb{G}\to\mathbb{Z}_q^*$，$H_2:\mathbb{G}\times\mathbb{G}\to\mathcal{K}$，$\mathcal{K}$为会话密钥空间。选取主私钥msk=s，计算公钥$P_{pub}$=sP。输出共享的全局性系统参数：

[0060]

$$pp=\{\mathbb{G},q,P,P_{pub},H_1,H_2\}$$

[0061] (2)(k)←Partial-Private-KeyGen(msk,ID)：部分私钥生成算法由根PKG运行，给定主私钥msk和任意一个用户身份向量ID=(I_1,I_2,...,I_t)，PKG随机选取$g_1,\ldots,g_t\in\mathbb{Z}_q^*$，计算$r_i=H_1(I_i||g_iP)$，其中1≤i≤t。输出该用户所对应的部分私钥k：

[0062] $$k=s+\sum_{i=1}^{t}(g_ir_i)$$

[0063] 若k=0，则需要重新选取$g_1,\ldots,g_t\in\mathbb{Z}_q^*$。通过安全信道将{$g_1$P,...,$g_t$P,k}发送给用户($I_1$,$I_2$,...,$I_t$)，其中$g_1$P,...,$g_t$P为用户ID的部分公钥。用户验证等式：

[0064] $$kP=P_{pub}+\sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

[0065] 若等式不成立，则拒绝此部分私钥。

[0066] (3)(d)←Set-Private-Key(k,ID)：私钥生成算法由用户ID运行，随机选取$x\in\mathbb{Z}_q^*$，输出该用户的私钥d：

[0067] d=k+x

[0068] 若d=0，则需要重新选取$x\in\mathbb{Z}_q^*$，并计算用户私钥。该用户的公钥为pk={ID,

$g_1P,\ldots,g_tP,xP\}$。

[0069] (4)(k) ← Partial-Delegate(k′，ID)：部分私钥委托算法由用户 ID = $(I_1,I_2,\ldots,I_t)$ 的上层 PKG 运行，其中 $ID_{PKG}=(I_1,I_2,\ldots,I_{t-1})$，PKG 的部分私钥为 $k'=s+\sum_{i=1}^{t-1}(g_ir_i)$，部分公钥为 $\{g_1P,\ldots,g_{t-1}P\}$。随机选取 $g_t\in\mathbb{Z}_q^*$，计算 $r_t=H_1(I_t||g_tP)$。PKG 为用户 ID 生成部分私钥 k：

[0070] $$k=k'+g_tr_t=s+\sum_{i=1}^{t-1}(g_ir_i)+g_tr_t=s+\sum_{i=1}^{t}(g_ir_i)$$

[0071] 若 k = 0，则需要重新选取 $g_t\in\mathbb{Z}_q^*$。通过安全信道将 $\{g_1P,\ldots,g_tP,k\}$ 发送给用户 ID，其中 $g_1P,\ldots,g_tP$ 为用户的部分公钥。用户验证等式：

[0072] $$kP=P_{pub}+\sum_{i=1}^{t}(H_1(I_i||g_iP)g_iP)$$

[0073] 若等式不成立，则拒绝此部分私钥。若等式成立，用户可执行 Set-Private-Key 算法生成自己的私钥和公钥。

[0074] (5)(sk) ← Agreement(pk_1, T_1, pk_2, T_2)：密钥协商过程如图 2 所示。以用户 A 和 B 为例，其中用户 A 所处的层级为 l_A，$ID_A=(I_1,I_2,\ldots,I_{l_A})$，A 的私钥为 d_A，公钥 pk_A 为 $\{ID_A,g_1P,\ldots,g_{l_A}P,x_AP\}$。用户 B 所处的层级为 l_B，$ID_B=(I_1',I_2',\ldots,I_{l_B}')$，B 的私钥为 d_B，公钥 pk_B 为 $\{ID_B,g_1'P,\ldots,g_{l_B}'P,x_BP\}$。

[0075] A 随机选取 $a\in\mathbb{Z}_q^*$，计算 $T_A=ad_AP$，发送 $\{T_A,pk_A\}$ 给 B，B 随机选取 $b\in\mathbb{Z}_q^*$，计算 $T_B=bd_BP$，发送 $\{T_B,pk_B\}$ 给 A，A 与 B 分别计算会话密钥：

[0076] 用户 A 做如下计算：

$$k_{AB}=d_A(T_B+a(P_{pub}+x_BP+\sum_{i=1}^{l_B}(H_1(I_i'||g_i'P)g_i'P)))$$

[0077]

$$=d_A(bd_BP+ad_BP)=(a+b)d_Ad_BP$$

$$ad_AT_B=abd_Ad_BP$$

[0078] 会话密钥为：$sk_A=H_2(k_{AB}||abd_Ad_BP)$

[0079] 用户 B 做如下计算：

$$k_{BA} = d_B(T_A + b(P_{pub} + x_A P + \sum_{i=1}^{l_A}(H_1(I_i||g_i P)g_i P)))$$

[0080]

$$= d_B(ad_A P + bd_A P) = (a+b)d_A d_B P = k_{AB}$$

$$bd_B T_A = abd_A d_B P$$

[0081] 会话密钥为：$sk_B = H_2(k_{BA}||abd_A d_B P)$

[0082] 用户 A 与 B 得到相同的会话密钥，可进行安全通信。

[0083] 另外，本发明实施例的无证书的基于层次身份基的认证密钥协商方法和协商系统的其它构成以及作用对于本领域的技术人员而言都是已知的，为了减少冗余，不做赘述。

[0084] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0085] 尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同限定。

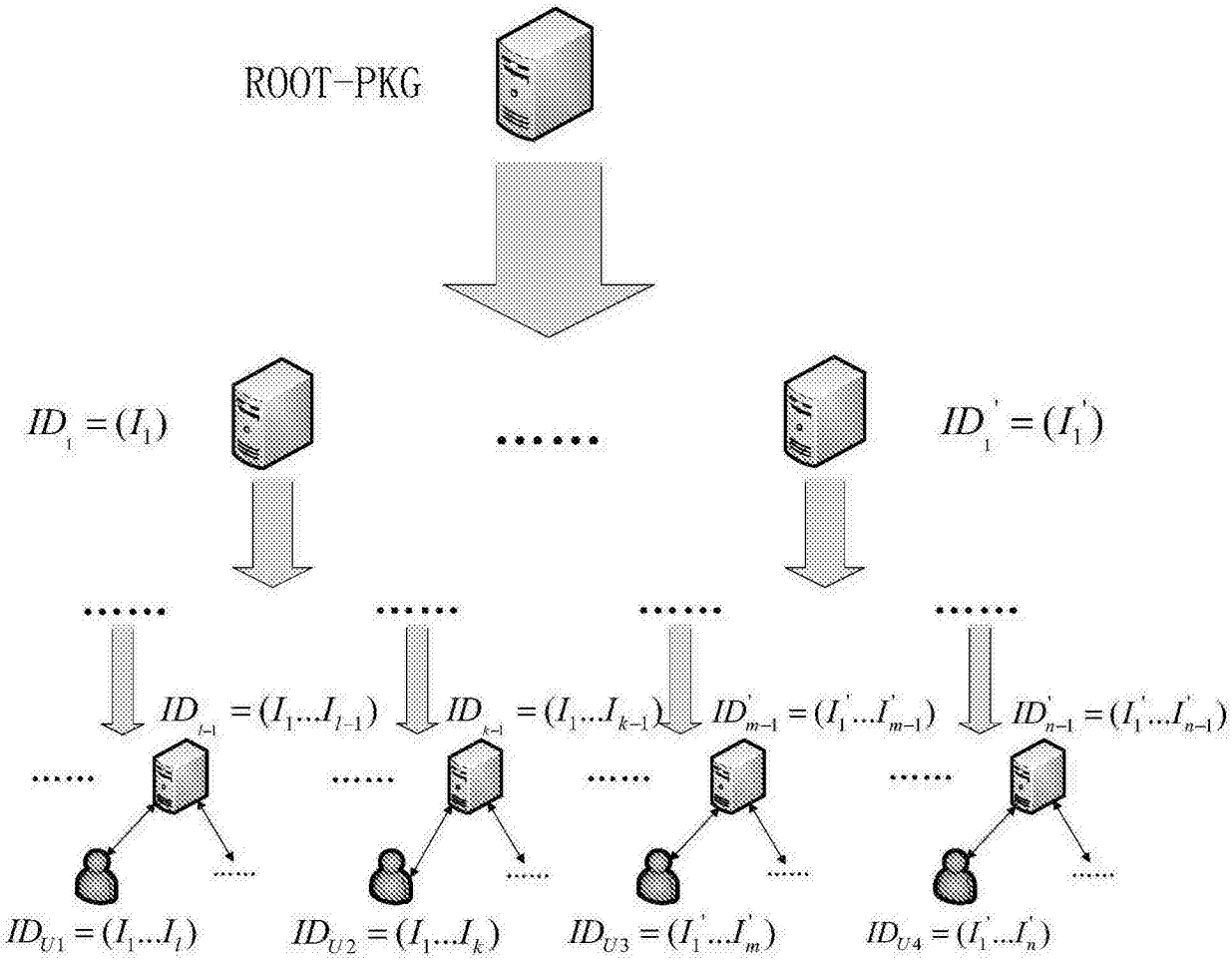

ROOT-PKG
$ID_1 = (I_1)$
$ID_1' = (I_1')$
$ID_{l-1} = (I_1 \ldots I_{l-1})$
$ID_{k-1} = (I_1 \ldots I_{k-1})$
$ID'_{m-1} = (I_1' \ldots I'_{m-1})$
$ID'_{n-1} = (I_1' \ldots I'_{n-1})$
$ID_{U1} = (I_1 \ldots I_l)$
$ID_{U2} = (I_1 \ldots I_k)$
$ID_{U3} = (I_1' \ldots I_m')$
$ID_{U4} = (I_1' \ldots I_n')$

图 1

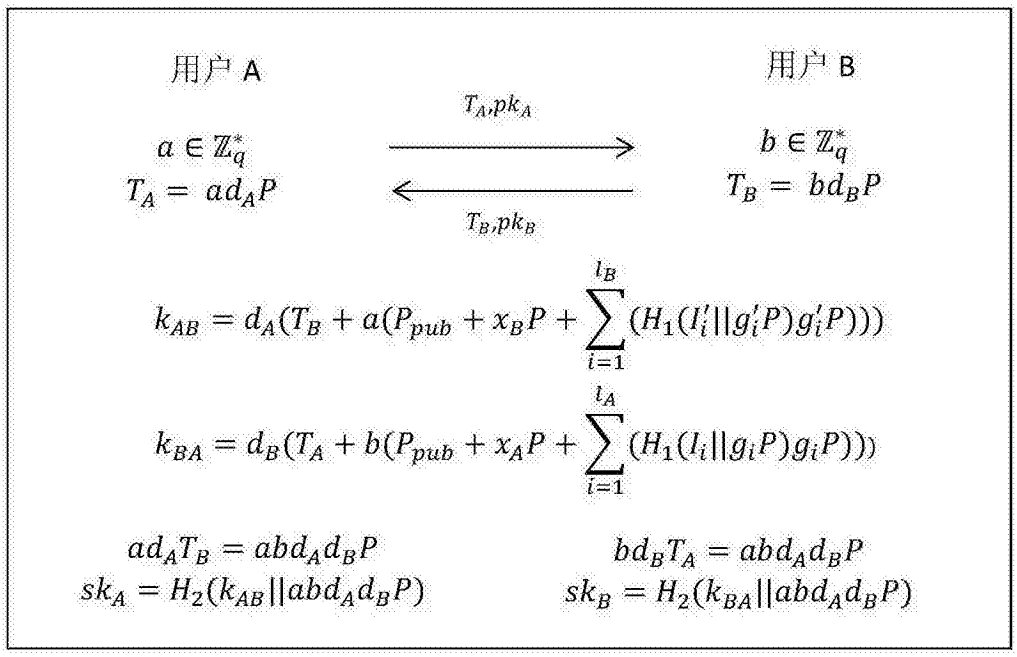

用户 A
用户 B
T_A, pk_A
$a \in \mathbb{Z}_q^*$
$T_A = aP$
$b \in \mathbb{Z}_q^*$
$T_B = bP$
T_B, pk_B
$k_{AB} = d_A(T_B + a(P_{pub} + x_B P + \sum_{i=1}^{l_B}(H_1(I_i' \| g_i' P) g_i' P)))$
$k_{BA} = d_B(T_A + b(P_{pub} + x_A P + \sum_{i=1}^{l_A}(H_1(I_i \| g_i P) g_i P)))$
$adT_B = abdd_BP$
$sk_A = H_2(k_{AB} \| abdd_BP)$
$bdT_A = abdd_BP$
$sk_B = H_2(k_{BA} \| abdd_BP)$

图 2