(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 107437993 A
(43)申请公布日 2017.12.05

(21)申请号 201610362863.2

(22)申请日 2016.05.26

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 刘勇 张家明 陆小慧

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李红爽 凌齐文

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

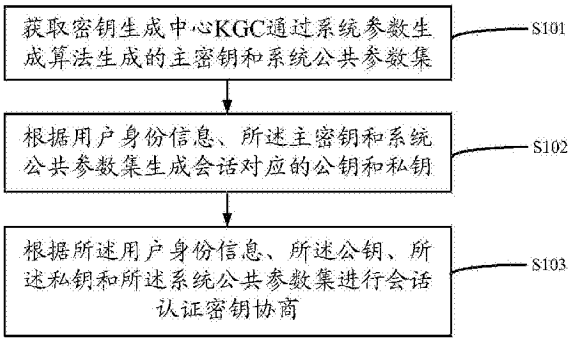
权利要求书4页 说明书12页 附图2页

(54)发明名称

一种基于无证书两方认证密钥协商方法和装置

(57)摘要

本发明公开了一种基于无证书的两方认证密钥协商的方法和装置，该装置包括参数模块和协商模块，通过生成系统公开参数集和密钥生产中心(KGC)的主密钥、部分密钥、秘密值、私钥、公钥、两方密钥协商的步骤，能够克服了传统公钥密码体制下复杂的证书管理问题和基于身份的密码体制所固有的密钥托管问题，而且不依赖于双线性对运算，提高了系统的效率，特别适用于计算能力受限的无线移动设备。



CN 107437993 A

1.一种基于无证书两方认证密钥协商的方法，其特征在于，应用于会话参与用户，所述方法包括：

获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk和系统公共参数集params；

根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥；

根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

2.根据权利要求1所述的方法，其特征在于，通过系统参数生成算法生成主密钥msk和系统公共参数集params包括：

根据预定的安全参数$k\in Z^+$，选择两个k比特的大素数p和q且满足$q|p-1$，生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G，从所述循环群G确定一个生成元P，并在密钥集合$Z_q^*=\{1,2,...,q-1\}$中随机确定一个整数s作为系统主密钥msk；

根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数$H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开参数集为$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$，其中，$H_1$是$\{0,1\}^*$到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积$\{0,1\}^*\times\{0,1\}^*\times G^4$到集合$Z_q^*$的密码学哈希函数，安全参数k表示安全参数的比特长度，$k>0$，$\{0,1\}^*$表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G^4分别表示4个加法循环群G的笛卡尔积，$\{0,1\}^*\times\{0,1\}^*\times G^4$表示$\{0,1\}^*$、$\{0,1\}^*$和$G^4$的笛卡尔积，$q|p-1$表示p-1能被q整除，$E/F_P$表示$E:y^2=x^3+ax+b$为有限域$F_P$上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

3.根据权利要求2所述的方法，其特征在于，根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥包括：

根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值；

根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥。

4.根据权利要求3所述的方法，其特征在于，根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值包括：

在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

5.根据权利要求4所述的方法，其特征在于，根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥包括：

根据生成的所述秘密值x_i，按照公式$P_i=x_iP$计算获得所述用户的公钥P_i。

6.根据权利要求5所述的方法，其特征在于，根据所述系统公共参数集params和用户身

份信息，生成所述用户的部分私钥包括：

在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式$R_i=r_iP$计算获得所述用户的公钥第一参数R_i，按照公式$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$计算获得所述用户的公钥第二参数$s_i$，将$(s_i,R_i)$作为部分私钥$D_i$，$ID_i$表示用户身份信息，mod表示取余。

7.根据权利要求6所述的方法，其特征在于，根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥包括：

根据公式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立确定所述部分私钥$D_i$是否有效；

当所述部分私钥D_i有效时，将(x_i,s_i,R_i)作为私钥S_i。

8.根据权利要求7所述的方法，其特征在于，根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商包括：

会话发起方在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式$T_A=t_AP$计算发起方会话密钥元素T_A，将(ID_A,R_A,T_A)作为发起方会话密钥参数M_A发送给会话响应方；

会话响应方收到所述发起方会话密钥参数M_A后，在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式$T_B=t_BP$计算响应会话密钥元素T_B，将(ID_B,R_B,T_B)作为响应方会话密钥参数M_B发送给会话发起方；会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

并通过下面的等式验证：

$$\begin{aligned}K_{AB}^1&=(x_A+s_A+t_A)(P_B+W_B)\\&=(x_A+s_A+t_A)(x_B+s_B)P\\&=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,\\K_{AB}^2&=(x_A+s_A+t_A)(T_B+W_B)\\&=(x_A+s_A+t_A)(t_B+s_B)P\\&=(t_B+s_B)W_A=K_{BA}^2,\end{aligned}$$

$K_{AB}=K_{BA}=K$，用户A和用户B生成了相同的会话密钥。

9.一种基于无证书两方认证密钥协商的装置，其特征在于，所述装置包括：

获取模块，设置为获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk和系统公共参数集params；

生成模块，设置为根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥；

协商模块，设置为根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

10.根据权利要求9所述的装置，其特征在于，所述获取模块获得的通过系统参数生成算法生成主密钥msk和系统公共参数集params是指：

根据预定的安全参数$k\in Z^+$，选择两个k比特的大素数p和q且满足$q|p-1$，生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G，从所述循环群G确定一个生成元P，并在密钥集合$Z_q^*=\{1,2,...,q-1\}$中随机确定一个整数s作为系 统主密钥msk；

根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开参数集为$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$，其中，$H_1$是$\{0,1\}^*$到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积$\{0,1\}^*\times\{0,1\}^*\times G^4$到集合$Z_q^*$的密码学哈希函数，安全参数k表示安全参数的比特长度，$k>0$，$\{0,1\}^*$表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G^4分别表示4个加法循环群G的笛卡尔积，$\{0,1\}^*\times\{0,1\}^*\times G^4$表示$\{0,1\}^*$、$\{0,1\}^*$和$G^4$的笛卡尔积，$q|p-1$表示p-1能被q整除，$E/F_P$表示$E:y^2=x^3+ax+b$为有限域$F_P$上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

11.根据权利要求10所述的装置，其特征在于，所述生成模块根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥包括：

根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值；

根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥。

12.根据权利要求11所述的装置，其特征在于，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值包括：

在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

13.根据权利要求12所述的装置，其特征在于，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥包括：

根据生成的所述秘密值x_i，按照公式$P_i=x_iP$计算获得所述用户的公钥P_i。

14.根据权利要求13所述的装置，其特征在于，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的部分私钥包括：

在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式$R_i=r_iP$计算获得所述用户的公钥第一参数R_i，按照公式$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$ 计算获得所述用户的公钥第二参数s_i，将(s_i,R_i)作为部分私钥D_i，ID_i表示用户身份信息，mod表示取余。

15.根据权利要求14所述的装置，其特征在于，所述生成模块根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥包括：

根据公式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立确定所述部分私钥$D_i$是否有效；

当所述部分私钥D_i有效时，将(x_i,s_i,R_i)作为私钥S_i。

16.根据权利要求15所述的装置，其特征在于，所述协商模块根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商包括：

会话发起方在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式$T_A=t_AP$计算发起方会话密钥元素T_A，将(ID_A,R_A,T_A)作为发起方会话密钥参数M_A发送给会话响应方；

会话响应方收到所述发起方会话密钥参数M_A后，在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式$T_B=t_BP$计算响应会话密钥元素T_B，将(ID_B,R_B,T_B)作为响应方会话密钥参数M_B发送给会话发起方；

会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

并通过下面的等式验证：

$$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$

$$=(x_A+s_A+t_A)(x_B+s_B)P$$

$$=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,$$

$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

$$=(x_A+s_A+t_A)(t_B+s_B)P$$

$$=(t_B+s_B)W_A=K_{BA}^2,$$

$K_{AB}=K_{BA}=K$，用户A和用户B生成了相同的会话密钥。

一种基于无证书两方认证密钥协商方法和装置

技术领域

[0001] 本发明涉及信息安全技术领域，尤指一种基于无证书的两方认证密钥协商的方法和装置。

背景技术

[0002] 目前，密钥协商作为一个重要的密码学原语，它可以保证两个或多个用户在公开的网络环境中通过交互信息建立一个共享的会话密钥，参与通信的用户通过共享的会话密钥来加解密通信数据从而保证网络通信的安全。其中，认证密钥协商是一种带有认证(显式认证或隐式认证)功能的密钥协商，它可以提供对通信用户的身份和密钥的认证功能，从而可以有效的抵抗第三者的攻击。

[0003] 现有技术中，认证密钥协商方法大多是在传统公钥密码体制下或基于身份密码体制下所提出的，其中，对于基于无证书密码体制是Al-Riyami和Paterson等人在2003年所提出的一种新型公钥密码体制，该体制有机结合了基于身份密码体制和传统公钥密码体制的优点，并有效克服了这两种密码体制中存在的缺陷。因此，基于无证书密码体制是一个性能优良，便于开放网络环境中应用的新型公钥密钥体制。

[0004] 但是，采用现有技术中的认证密钥协商方法可以有效解决了复杂的证书管理问题及密钥托管问题，然而这些基于Al-Riyami和Paterson等人提出的密钥协商方法都依赖于双线性对运算，计算代价很大，导致计算能力受限的无线移动设备在开放网络环境中的安全应用受到威胁。

发明内容

[0005] 为了解决上述技术问题，本发明提供了一种基于无证书的两方认证密钥协商的方法和装置，能够克服了传统公钥密码体制下复杂的证书管理问题和基于身份的密码体制所固有的密钥托管问题，而且不依赖于双线性对运算，提高了系统的效率，特别适用于计算能力受限的无线移动设备。

[0006] 本发明提供一种基于无证书两方认证密钥协商的方法，应用于会话参与用户，所述方法包括：

[0007] 获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk和系统公共参数集params；

[0008] 根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥；

[0009] 根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

[0010] 优选地，通过系统参数生成算法生成主密钥msk和系统公共参数集params包括：

[0011] 根据预定的安全参数$k\in Z^{+}$，选择两个k比特的大素数p和q且满足$q|p-1$，生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G，从所述循环群G确定一个生成元P，并在密钥

集合$Z_q^*=\{1,2,\ldots,q-1\}$中随机确定一个整数s作为系统主密钥msk；

[0012] 根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数$H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开参数集为params＝{$F_P$,E/$F_P$,G,k,P,$P_{pub}$,$H_1$,$H_2$}，其中，$H_1$是{0,1}*到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积{0,1}*×{0,1}*×$G^4$到集合$Z_q^*$的密码学哈希函数，安全参数k表示安全参数的比特长度，k＞0，{0,1}*表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G^4分别表示4个加法循环群G的笛卡尔积，{0,1}*×{0,1}*×G^4表示{0,1}*、{0,1}*和G^4的笛卡尔积，q|p-1表示p-1能被q整除，E/F_P表示E：$y^2=x^3+ax+b$为有限域F_P上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

[0013] 优选地，根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥包括：

[0014] 根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密 值；

[0015] 根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

[0016] 获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

[0017] 根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥。

[0018] 优选地，根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值包括：

[0019] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

[0020] 优选地，根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥包括：

[0021] 根据生成的所述秘密值x_i，按照公式$P_i=x_iP$计算获得所述用户的公钥P_i。

[0022] 优选地，根据所述系统公共参数集params和用户身份信息，生成所述用户的部分私钥包括：

[0023] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式$R_i=r_iP$计算获得所述用户的公钥第一参数R_i，按照公式$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$计算获得所述用户的公钥第二参数$s_i$，将($s_i$,$R_i$)作为部分私钥$D_i$，$ID_i$表示用户身份信息，mod表示取余。

[0024] 优选地，根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥包括：

[0025] 根据公式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立确定所述部分私钥$D_i$是否有效；

[0026] 当所述部分私钥D_i有效时，将(x_i,s_i,R_i)作为私钥S_i。

[0027] 优选地，根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商包括：

[0028] 会话发起方在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式$T_A=t_AP$计算发起方会话密钥元素T_A，将(ID_A,R_A,T_A)作为发起方会话密钥参数M_A发送给会话

响应方；

[0029] 会话响应方收到所述发起方会话密钥参数M_A后，在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式$T_B=t_BP$计算响应会话密钥 元素T_B，将(ID_B,R_B,T_B)作为响应方会话密钥参数M_B发送给会话发起方；

[0030] 会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

[0031] 会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$， $K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式 $K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

[0032] 并通过下面的等式验证：

$$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$

[0033]
$$=(x_A+s_A+t_A)(x_B+s_B)P$$

$$=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,$$

$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

[0034]
$$=(x_A+s_A+t_A)(t_B+s_B)P$$

$$=(t_B+s_B)W_A=K_{BA}^2。$$

[0035] $K_{AB}=K_{BA}=K$，用户A和用户B生成了相同的会话密钥。

[0036] 本发明还提供一种基于无证书两方认证密钥协商的装置，所述装置包括：

[0037] 获取模块，设置为获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk和系统公共参数集params；

[0038] 生成模块，设置为根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥；

[0039] 协商模块，设置为根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

[0040] 优选地，所述获取模块获得的通过系统参数生成算法生成主密钥msk和系统公共参数集params是指：

[0041] 根据预定的安全参数$k\in Z^+$，选择两个k比特的大素数p和q且满足$q|p-1$，生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G，从所述循环群G确定一个生成元P，并在密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中随机确定一个整数s作为系 统主密钥msk；

[0042] 根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开参数集为$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$，其中，$H_1$是$\{0,1\}^*$到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积$\{0,1\}^*\times\{0,$

1}*×G⁴到集合Z_q^*的密码学哈希函数，安全参数k表示安全参数的比特长度，k>0，{0,1}*表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G⁴分别表示4个加法循环群G的笛卡尔积，{0,1}*×{0,1}*×G⁴表示{0,1}*、{0,1}*和G⁴的笛卡尔积，q|p-1表示p-1能被q整除，E/Fp表示E：$y^2=x^3+ax+b$为有限域Fp上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

[0043] 优选地，所述生成模块根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥包括：

[0044] 根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值；

[0045] 根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

[0046] 获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

[0047] 根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥。

[0048] 优选地，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值包括：

[0049] 在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

[0050] 优选地，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥包括：

[0051] 根据生成的所述秘密值xi，按照公式Pi=xiP计算获得所述用户的公钥Pi。

[0052] 优选地，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的部分私钥包括：

[0053] 在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式Ri=riP计算获得所述用户的公钥第一参数Ri，按照公式si=ri+sH1(IDi,Ri,Pi)(mod q)计算获得所述用户的公钥第二参数si，将(si,Ri)作为部分私钥Di，IDi表 示用户身份信息，mod表示取余。

[0054] 优选地，所述生成模块根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥包括：

[0055] 根据公式siP=Ri+H1(IDi,Ri,Pi)Ppub是否成立确定所述部分私钥Di是否有效；

[0056] 当所述部分私钥Di有效时，将(xi,si,Ri)作为私钥Si。

[0057] 优选地，所述协商模块根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商包括：

[0058] 会话发起方在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式TA=tAP计算发起方会话密钥元素TA，将(IDA,RA,TA)作为发起方会话密钥参数MA发送给会话响应方；

[0059] 会话响应方收到所述发起方会话密钥参数MA后，在所述密钥集合$Z_q^*=\{1,2,...,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式TB=tBP计算响应会话密钥元素TB，将(IDB,RB,TB)作为响应方会话密钥参数MB发送给会话发起方；

[0060] 会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

[0061] 会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

[0062] 并通过下面的等式验证：

$$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$

[0063] $$=(x_A+s_A+t_A)(x_B+s_B)P$$

$$=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,$$

$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

[0064] $$=(x_A+s_A+t_A)(t_B+s_B)P$$

$$=(t_B+s_B)W_A=K_{BA}^2。$$

[0065] $K_{AB}=K_{BA}=K$，用户A和用户B生成了相同的会话密钥。

[0066] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0067] 附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

[0068] 图1为本发明实施例提供的一种基于无证书的两方认证密钥协商的方法的流程示意图；

[0069] 图2为本发明实施例提供的一种基于无证书的两方认证密钥协商的装置的结构示意图；

[0070] 图3为本发明实施例一提供的一种基于无证书的两方认证密钥协商的方法的流程示意图。

具体实施方式

[0071] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0072] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0073] 本发明实施例涉及的方法可以应用于开放的网络环境，需要进行信息安全保护的通信或者互联网络，但并不以此为限。

[0074] 本发明实施例涉及的方法，旨在解决现有技术中基于无证书的密钥协商方法都依赖于双线性对运算，其运算过程复杂，导致计算能力受限的无线移动设备在开放网络环境中的安全应用受到威胁的技术问题。

[0075] 下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0076] 图1为本发明提供的一种基于无证书的两方认证密钥协商的方法实施例一的流程示意图。本实施例涉及的是基于无证书不依赖双线性对运算的两方认证密钥协商的具体过程。如图1所示，该方法包括：

[0077] S101、获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk(Master Session Key)和系统公共参数集params；

[0078] S102、根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥；

[0079] S103、根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

[0080] 其中，步骤S101具体包括：

[0081] 根据预定的安全参数$k\in Z^+$，选择两个k比特的大素数p和q且满足$q|p-1$，生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G，从所述循环群G确定一个生成元P，并在密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中随机确定一个整数s作为系统主密钥msk；

[0082] 根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数$H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开参数集为$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$，其中，$H_1$是$\{0,1\}^*$到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积$\{0,1\}^*\times\{0,1\}^*\times G^4$到集合$Z_q^*$的密码学哈希函数，安全参数k表示安全参数的比特长度，$k>0$，$\{0,1\}^*$表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G^4分别表示4个加法循环群G的笛卡尔积，$\{0,1\}^*\times\{0,1\}^*\times G^4$表示$\{0,1\}^*$、$\{0,1\}^*$和$G^4$的笛卡尔积，$q|p-1$表示$p-1$能被q整除，$E/F_P$表示$E:y^2=x^3+ax+b$为有限域$F_P$上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

[0083] 根据上述过程，生成KGC保存的主密钥为$msk=s$，系统公开参数集$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$。

[0084] 步骤S102具体包括：

[0085] S1021、根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值；

[0086] S1022、根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

[0087] S1023、获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

[0088] S1024、根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所

述用户的私钥。

[0089] 步骤S1021包括：

[0090] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

[0091] 步骤S1022包括：

[0092] 根据生成的所述秘密值x_i，按照公式$P_i=x_iP$计算获得所述用户的公钥P_i。

[0093] 步骤S1023包括：

[0094] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式$R_i=r_iP$计算获得所述用户的公钥第一参数R_i，按照公式$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$计算获得所述用户的公钥第二参数$s_i$，将$(s_i,R_i)$作为部分私钥$D_i$，$ID_i$表示用户身份信息，mod表示取余。

[0095] 步骤S1024包括：

[0096] 根据公式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立确定所述部分私钥$D_i$是否有效；

[0097] 当所述部分私钥D_i有效时，将(x_i,s_i,R_i)作为私钥S_i。

[0098] 步骤S103具体包括：

[0099] 会话发起方在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式$T_A=t_AP$计算发起方会话密钥元素T_A，将(ID_A,R_A,T_A)作为发起方会话密钥参数M_A发送给会话响应方；

[0100] 会话响应方收到所述发起方会话密钥参数M_A后，在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式$T_B=t_BP$计算响应会话密钥元素T_B，将(ID_B,R_B,T_B)作为响应方会话密钥参数M_B发送给会话发起方；

[0101] 会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

[0102] 会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

[0103] 验证过程如下：

$$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$

[0104]
$$=(x_A+s_A+t_A)(x_B+s_B)P$$
$$=(x_B+s_B)W_A=K_{BA}^1,$$
$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

[0105]
$$=(x_A+s_A+t_A)(t_B+s_B)P$$
$$=(t_B+s_B)W_A=K_{BA}^2。$$

[0106] 具体的，会话参与用户包括会话发起方A和会话响应方B，。

[0107] 1)用户A随机选择一个整数$t_A\in Z_q^*$，计算$T_A=t_AP$并把$M_A=(ID_A,R_A,T_A)$发送给用户

B。

[0108] 2)当用户B收到$M_A=(ID_A,R_A,T_A)$后,会随机选择一个整数$t_B \in Z_q^*$,计算$T_B=t_BP$并把$M_B=(ID_B,R_B,T_B)$发送给用户A。

[0109] 3)当用户A收到$M_B=(ID_B,R_B,T_B)$后,用户A会依次计算:$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$,$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$,其中,$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$,然后用户A计算并获得会话密钥:$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$。

[0110] 用户B依次计算:$K_{BA}^1=(x_B+s_B)W_A$, $K_{BA}^2=(t_B+s_B)W_A$,其中,$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$;然后用户B计算并获得会话密钥:$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$。

[0111] 本方法的正确性很容易通过下面的等式验证:

[0112] $$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$
$$=(x_A+s_A+t_A)(x_B+s_B)P$$

[0113]
$$=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,$$
$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

[0114] $$=(x_A+s_A+t_A)(t_B+s_B)P$$
$$=(t_B+s_B)W_A=K_{BA}^2。$$

[0115] 因此,$K_{AB}=K_{BA}=K$,用户A和用户B生成了相同的会话密钥。

[0116] 本发明实施例提供的一种基于无证书的两方认证密钥协商的方法,该方法通过生成系统公开参数集和密钥生产中心(KGC)的主密钥、部分密钥、秘密值、私钥、公钥、两方密钥协商的步骤,能够克服了传统公钥密码体制下复杂的证书管理问题和基于身份的密码体制所固有的密钥托管问题,而且不依赖于双线性对运算,提高了系统的效率,特别适用于计算能力受限的无线移动设备。

[0117] 图2为本发明提供的一种基于无证书的两方认证密钥协商的装置实施例一的结构示意图,如图2所示,该装置包括:

[0118] 获取模块,设置为获取密钥生成中心KGC通过系统参数生成算法生成的主密钥msk和系统公共参数集params;

[0119] 生成模块,设置为根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥;

[0120] 协商模块,设置为根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商。

[0121] 其中,所述获取模块获得的通过系统参数生成算法生成主密钥msk和系统公共参数集params是指:

[0122] 根据预定的安全参数$k \in Z^+$,选择两个k比特的大素数p和q且满足$q|p-1$,生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G,从所述循环群G确定一个生成元P,并在密钥

集合$Z_q^*=\{1,2,\ldots,q-1\}$中随机确定一个整数s作为系统主密钥msk；

[0123] 根据公式$P_{pus}=sP$计算公开生成元P_{pus}，并根据第一哈希函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$和第二哈希函数$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$，获取所述系统公开 参数集为params＝{$F_P$，$E/F_P$，G，k，P，$P_{pub}$，$H_1$，$H_2$}，其中，$H_1$是{0，1}*到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积{0，1}*×{0，1}*×$G^4$到集合$Z_q^*$的密码学哈希函数，安全参数k表示安全参数的比特长度，k＞0，{0，1}*表示长度不确定的二进制串的集合，Z_q^*表示长度为k的二进制串的集合，G^4分别表示4个加法循环群G的笛卡尔积，{0，1}*×{0，1}*×G^4表示{0，1}*、{0，1}*和G^4的笛卡尔积，q|p-1表示p-1能被q整除，E/F_P表示E：$y^2=x^3+ax+b$为有限域F_P上的椭圆曲线，x为横轴坐标，y为纵轴坐标，a、b为常数。

[0124] 其中，所述生成模块根据用户身份信息、所述主密钥msk和系统公共参数集params生成会话对应的公钥和私钥包括：

[0125] 根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值；

[0126] 根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥；

[0127] 获取所述KGC根据所述系统公共参数集params和用户身份信息生成的所述用户的部分私钥；

[0128] 根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥。

[0129] 其中，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的秘密值包括：

[0130] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$x_i\in Z_q^*$作为秘密值。

[0131] 其中，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的公钥包括：

[0132] 根据生成的所述秘密值x_i，按照公式$P_i=x_iP$计算获得所述用户的公钥P_i。

[0133] 其中，所述生成模块根据所述系统公共参数集params和用户身份信息，生成所述用户的部分私钥包括：

[0134] 在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$r_i\in Z_q^*$，按照公式$R_i=r_iP$计算获得所述用户的公钥第一参数R_i，按照公式$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$计算获得所述用户的公钥第二参数$s_i$，将$(s_i,R_i)$作为部分私钥$D_i$，$ID_i$表示用户身份信息，mod表示取余。

[0135] 其中，所述生成模块根据所述系统公共参数集params、用户身份信息和所述部分私钥，生成所述用户的私钥包括：

[0136] 根据公式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立确定所述部分私钥$D_i$是否有效；

[0137] 当所述部分私钥D_i有效时，将(x_i,s_i,R_i)作为私钥S_i。

[0138] 其中，所述协商模块根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集params进行会话认证密钥协商包括：

[0139] 会话发起方在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_A\in Z_q^*$，按照公式

$T_A=t_AP$计算发起方会话密钥元素T_A，将(ID_A,R_A,T_A)作为发起方会话密钥参数M_A发送给会话响应方；

[0140] 会话响应方收到所述发起方会话密钥参数M_A后，在所述密钥集合$Z_q^*=\{1,2,\ldots,q-1\}$中选择一个整数$t_B\in Z_q^*$，按照公式$T_B=t_BP$计算响应会话密钥元素T_B，将(ID_B,R_B,T_B)作为响应方会话密钥参数M_B发送给会话发起方；

[0141] 会话发起方收到所述响应方会话密钥参数M_B后，计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$和$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，按照公式$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$计算并获得发起方会话密钥$K_{AB}$；

[0142] 会话响应方计算：$K_{BA}^1=(x_B+s_B)W_A$，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$；按照公式$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{BA}^1,K_{BA}^2)$计算并获得响应方会话密钥$K_{BA}$；

[0143] 并通过下面的等式验证：

$$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$$

[0144] $$=(x_A+s_A+t_A)(x_B+s_B)P$$

$$=(x_A+s_A+t_A)(x_B+s_B)P=K_{BA}^1,$$

$$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$$

[0145] $$=(x_A+s_A+t_A)(t_B+s_B)P$$

$$=(t_B+s_B)W_A=K_{BA}^2。$$

[0146] $K_{AB}=K_{BA}=K$，用户A和用户B生成了相同的会话密钥。

[0147] 本发明实施例提供的装置，可以执行上述方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0148] 下面具体的列举实施例来进行详细说明：

[0149] 实施例一

[0150] 本实施例系统中所涉及的实体如下：

[0151] (1)KGC：负责系统参数生成，即KGC主密钥和系统公开参数集，并生产用户部分私钥的可信第三方；

[0152] (2)用户A：会话的原始发起实体；

[0153] (3)用户B：会话的响应实体；

[0154] 图3为本发明提供的一种基于无证书的两方认证密钥协商的方法实施例二的流程示意图，具体步骤如下：

[0155] 步骤A，生成KGC的主密钥和系统公开参数集；具体步骤如下：

[0156] 步骤1：KGC运行系统参数生产算法：KGC根据设定的安全参数$k\in Z^+$，选择两个k比特的大素数p和q且满足$q|p-1$，并生成一个素数域椭圆曲线E/F_P上阶为q的加法循环群G。

[0157] 步骤2：KGC从循环群G中选择一个生成元P并在集合Z_q^*中随机选择一个整数s，并计

算$P_{pub}=sP$，其中：集合$Z_q^*=\{1,2,\ldots,q-1\}$。

[0158] 步骤3：定义两个哈希函数$H_1:\{0,1\}^*\rightarrow Z_q^*$、$H_2:\{0,1\}^*\times\{0,1\}^*\times G^4\rightarrow Z_q^*$；其中：$H_1$是$\{0,1\}^*$到$Z_q^*$的密码学哈希函数，$H_2$是笛卡尔积$\{0,1\}^*\times\{0,1\}^*\times G^4$到集合$Z_q^*$的密码学哈希函数，整数$k>0$，k表示系统安全参数的比特长度，$\{0,1\}^*$表示长度不确定的二进制串的集合，$Z_q^*$表示长度为k的二进制串的集合，$G^4$分别表示4个群G的笛卡尔积，$\{0,1\}^*\times\{0,1\}^*\times G^4$表示$\{0,1\}^*$、$\{0,1\}^*$和$G^4$的笛卡尔积。

[0159] 步骤4：根据步骤1，步骤2及步骤3的执行结果，生成KGC秘密保存的主密钥为$msk=s$，系统公开参数集为$params=\{F_P,E/F_P,G,k,P,P_{pub},H_1,H_2\}$。

[0160] 步骤B，根据所述系统公开参数集，用户身份信息，生成用户的秘密值；具体过程为：

[0161] 步骤5：用户ID_i在集合Z_q^*中随机选择一个整数$x_i\in Z_q^*$作为自己的秘密值。

[0162] 步骤C，根据所述系统公开参数集，用户身份信息，生成用户的公钥；具体过程为：

[0163] 步骤6：用户ID_i根据已选择的秘密值x_i计算并获得自己的公钥$P_i=x_iP$。

[0164] 步骤D，根据所述系统公开参数集，用户身份信息，生成用户的部分密钥；具体过程为：

[0165] 步骤7：身份为ID_i的用户i把身份信息ID_i和公钥P_i提交给KGC。

[0166] 步骤8：KGC随机选择$r_i\in Z_q^*$，计算$R_i=r_iP$和$s_i=r_i+sH_1(ID_i,R_i,P_i)(\mathrm{mod}\ q)$。

[0167] 步骤9：KGC通过安全信道把用户ID_i的部分私钥$D_i=D_i=(s_i,R_i)$发送给用户。

[0168] 步骤E，根据所述系统公开参数集，用户身份信息，生成用户的私钥；具体过程为：

[0169] 步骤10：用户ID_i通过判断等式$s_iP=R_i+H_1(ID_i,R_i,P_i)P_{pub}$是否成立来验证部分私钥$D_i=(s_i,R_i)$是否有效。

[0170] 步骤11：用户ID_i将自己的私钥设置为$S_i=(x_i,s_i,R_i)$。

[0171] 步骤F，根据所述系统公开参数集，会话发起方和会话响应方的身份信息、公钥、私钥，生成两方的会话密钥；具体过程为：

[0172] 步骤12：会话发起方A随机选择一个整数$t_A\in Z_q^*$，计算$T_A=t_AP$。

[0173] 步骤13：会话发起方A把$M_A=(ID_A,R_A,T_A)$发送给会话响应方B，其中，ID_A是会话发起方A的身份信息，R_A是会话发起方A的部分私钥。

[0174] 步骤14：收到$M_A=(ID_A,R_A,T_A)$后，会话响应方B随机选择一个整数$t_B\in Z_q^*$，计算$T_B=t_BP$。

[0175] 步骤15：会话响应方B把$M_B=(ID_B,R_B,T_B)$发送给会话响应方A，其中，ID_B是会话响应方B的身份信息，R_B是会话发起方B的部分私钥。

[0176] 步骤16：会话发起方A收到$M_B=(ID_B,R_B,T_B)$后，会话发起方A依次计算：$K_{AB}^1=(x_A+s_A+t_A)(P_B+W_B)$，$K_{AB}^2=(x_A+s_A+t_A)(T_B+W_B)$，其中，$W_B=R_B+H_1(ID_B,R_B,P_B)P_{pub}$，$x_A$是会话发起方A的秘密值，$s_A$是会话发起方A的部分私钥，$ID_B$是会话响应方B的身份信息，$R_B$是会话响应方B的部分私钥，$P_B$是会话响应方B的公钥；然后A计算并获得会话密

钥：$K_{AB}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$。

[0177] 步骤17：会话响应方B依次计算：$K_{BA}^1=(x_B+s_B)W_A$ ，$K_{BA}^2=(t_B+s_B)W_A$，其中，$W_A=P_A+R_A+H_1(ID_A,R_A,P_A)P_{pub}+T_A$，$x_B$是会话响应方B的秘密值，$s_B$是会话响应方B部分私钥，$ID_A$是会话发起方A的身份信息，$P_A$是会话发起方A的公钥，$R_A$是会话发起方A的部分私钥；然后B计算并获得会话密钥：$K_{BA}=H_2(ID_A,ID_B,T_A,T_B,K_{AB}^1,K_{AB}^2)$。

[0178] 该实施例通过生成系统公开参数集和密钥生产中心(KGC)的主密钥、部分密钥、秘密值、私钥、公钥、两方密钥协商的步骤，能够克服了传统公钥密码体制下复杂的证书管理问题和基于身份的密码体制所固有的密钥托管问题，而且不依赖于双线性对运算，提高了系统的效率，特别适用于计算能力受限的无线移动设备。

[0179] 虽然本发明所揭露的实施方式如上，但所述的内容仅为便于理解本发明而采用的实施方式，并非用以限定本发明。任何本发明所属领域内的技术人员，在不脱离本发明所揭露的精神和范围的前提下，可以在实施的形式及细节上进行任何的修改与变化，但本发明的专利保护范围，仍须以所附的权利要求书所界定的范围为准。

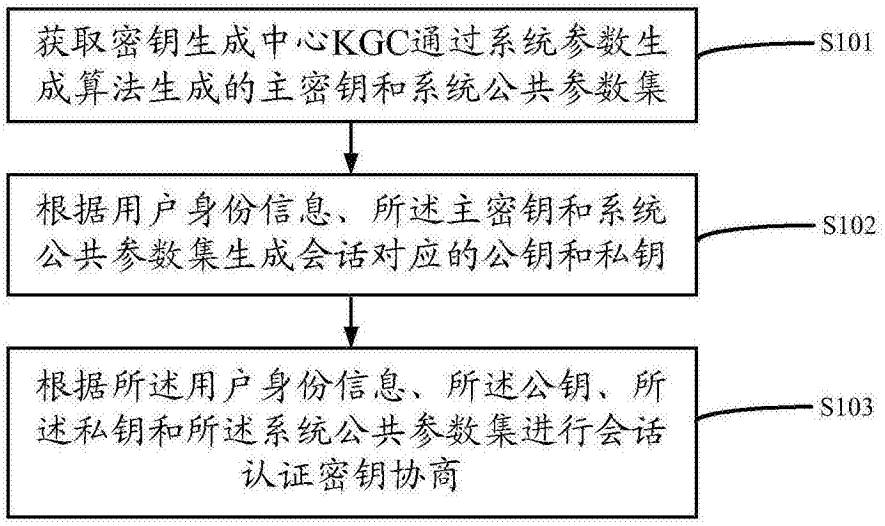

获取密钥生成中心KGC通过系统参数生成算法生成的主密钥和系统公共参数集
S101
根据用户身份信息、所述主密钥和系统公共参数集生成会话对应的公钥和私钥
S102
根据所述用户身份信息、所述公钥、所述私钥和所述系统公共参数集进行会话认证密钥协商
S103

图1


获取模块
生成模块
协商模块

图2

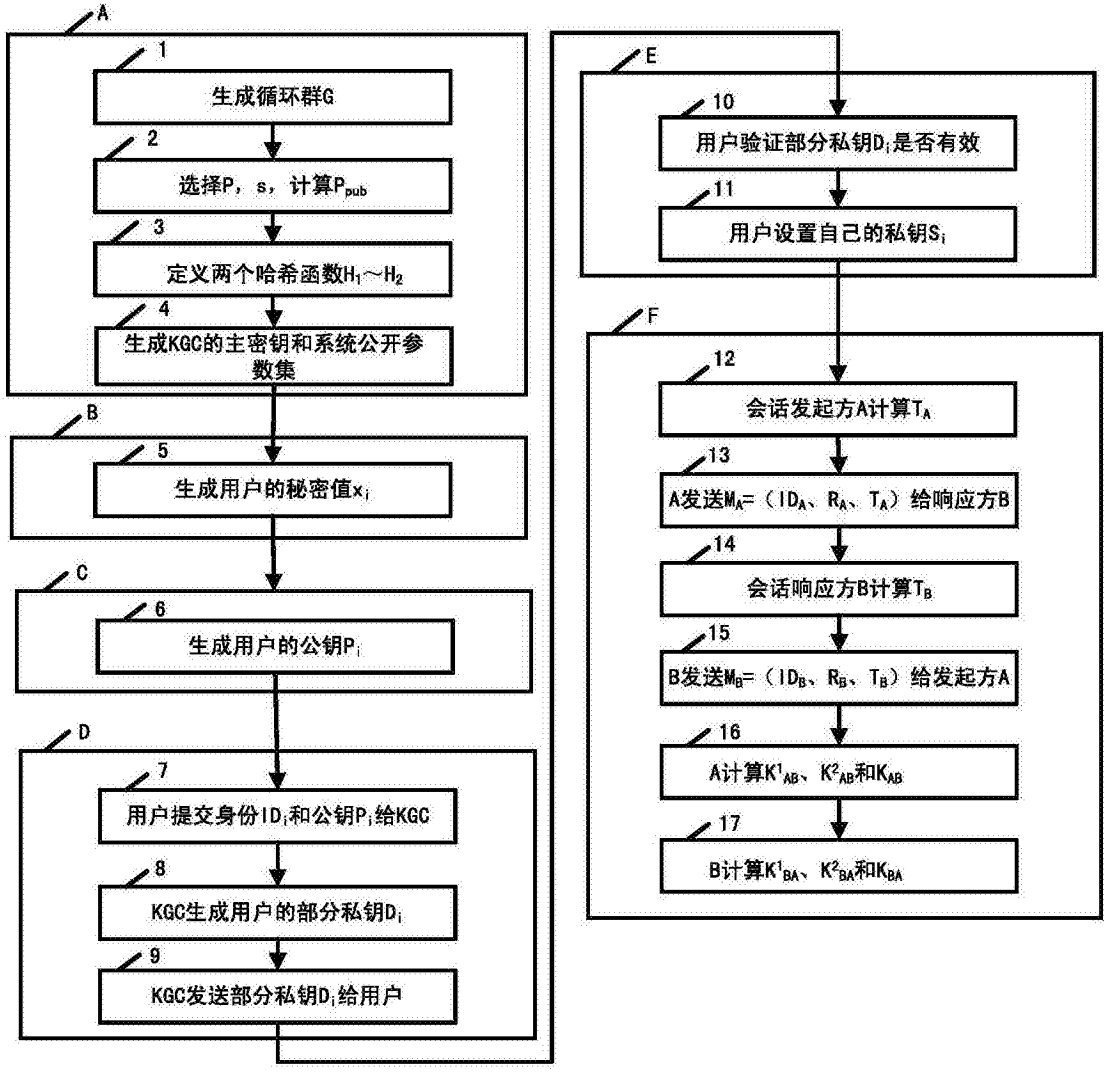

A
1
生成循环群G
2
选择P，s，计算P_{pub}
3
定义两个哈希函数H_1～H_2
4
生成KGC的主密钥和系统公开参数集
B
5
生成用户的秘密值x_i
C
6
生成用户的公钥P_i
D
7
用户提交身份ID_i和公钥P_i给KGC
8
KGC生成用户的部分私钥D_i
9
KGC发送部分私钥D_i给用户
E
10
用户验证部分私钥D_i是否有效
11
用户设置自己的私钥S_i
F
12
会话发起方A计算T_A
13
A发送M_A=（ID_A、R_A、T_A）给响应方B
14
会话响应方B计算T_B
15
B发送M_B=（ID_B、R_B、T_B）给发起方A
16
A计算K^1_{AB}、K^2_{AB}和K_{AB}
17
B计算K^1_{BA}、K^2_{BA}和K_{BA}

图3