标准模型下 CCA2 安全且固定密文长度的模糊基于身份加密方案

葛爱军[1],马传贵[1],程庆丰[2]
(1.解放军信息工程大学数学工程与先进计算国家重点实验室,河南郑州 450002;
2.解放军外国语学院基础部,河南洛阳 471003)

摘 要: 模糊基于身份加密体制为基于身份密码提供了检错能力,并且可以把消息加密后同时发送给多个具有相同属性的用户.本文提出了一种在标准模型下能抵抗适应性选择密文攻击,并且密文长度达到了固定值的模糊基于身份加密方案.与现有方案相比,本方案占用通信带宽低,计算效率高,具有更高的安全性,因此能更好的满足应用要求.

关键词: 模糊基于身份加密; 适应性选择密文攻击; 双线性对; 标准模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013) 10-1948-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.10.012

CCA2 Secure Fuzzy Identity-Based Encryption with Constant Size Ciphertexts in the Standard Model

GE Ai-jun[1], MA Chuan-gui[1], CHENG Qing-feng[2]
(1. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University of PLA, Zhengzhou, Henan*, 450002, *China*; 2. *Deparment of Basic Courses, PLA University of Foreign Languages, Luoyang, Henan*, 471003, *China*)

Abstract: Fuzzy identity-based encryption can provide an error-tolerance property for identity-based systems, and it allows a sender to encrypt a message to all users who have a certain set of attributes. In this paper, we proposed a fuzzy identity-based encryption scheme with constant size of ciphertexts that is indistinguishable against adaptive chosen ciphertexts attacks (CCA2) in the standard model. Compared with other existing schemes, this construction can satisfy the application requirements, as it can provide better efficiency in terms of the communication and computation cost as well as a stronger security guarantee.

Key words: fuzzy identity-based encryption; chosen ciphertexts attack; bilinear pairing; standard model

1 引言

基于身份公钥密码体制最早是由 Shamir[1]提出,其核心思想是用户采用自己的身份信息(如电子邮箱地址、身份证号码等)作为公钥,用户的私钥由一个称为私钥生成器的可信第三方产生.Boneh 和 Franklin[2]在 2001 年首次将椭圆曲线上双线性对引入到公钥密码体制,并构造了第一个实用的基于身份加密体制.Sahai 和 Waters[3]在 2005 年欧密会首次提出了模糊基于身份加密方案,在传统基于身份加密基础上提供了检错能力:如果身份 *ID* 与 *ID'*在一定范围接近的话,一个用 *ID'*加密的密文用身份 *ID* 的私钥也能解密.模糊基于身份加密这种容错性质,使其可以应用在无线传感网络[4]以及保密数据库[5]中.

随着公钥密码体制的迅速发展,对模糊基于身份加密的研究也成为当前一个热点问题.近年来,一系列模糊基于身份加密方案[6~9]相继被提出.但是这些方案或者密文的长度与用户的身份线性相关[6~8],导致效率不高;或者只能在随机预言模型下可证安全[6,8,9].然而,随机预言模型把哈希函数作为一个完全随机的理想模型,而真正的哈希函数与随机预言的问答模式是有区别的,同时也有学者指出某些在随机预言模型下可证安全的方案在哈希函数实例化后并不安全[10].因此在不借助于随机预言的标准模型下设计固定密文长度的模糊基于身份加密方案更有意义.

抗适应性选择密文攻击(CCA2)安全性是公钥密码中一个很重要的安全概念,其对存在主动攻击的许多加密应用都是充分的,并且已成为目前公钥加密体制的标

收稿日期:2012-09-07;修回日期:2013-01-30;责任编辑:马兰英
基金项目:信息工程大学博士研究生学位论文创新基金;国家自然科学基金(No.61072047);国家 863 高技术研究发展计划(No.2011AA010803)

准性安全要求之一.最近,Ren 等人[7]首次在标准模型下构造了一个 CCA2 安全的模糊基于身份加密方案,随后,Yang 等人[9]在随机预言模型下给出了一种 CCA2 安全的模糊基于身份加密方案,且密文长度达到了固定值.但是,已有文献[11,12]分析表明 Ren 等人[7]和 Yang 等人方案[9]均存在安全缺陷,并不具有 CCA2 安全性,目前尚未存在标准模型下 CCA2 安全且固定密文长度的模糊基于身份加密方案.本文在现有研究基础上,利用椭圆曲线上双线性对,首次提出了一个标准模型下 CCA2 安全的模糊基于身份加密方案,并且其密文长度达到了固定值.与现有方案相比,本方案占用通信带宽低,计算效率高,具有更高的安全性,因此能更好的满足应用要求.

2　预备知识

2.1　双线性映射及复杂性假设

设 G_1, G_2 是阶为素数 p 的乘法群,g 是 G_1 的生成元,若一个映射 $e: G_1 \times G_1 \to G_2$ 满足以下三条性质,我们称这个映射为双线性映射:

(1)**双线性性**　对于任何的 $a, b \in \mathbb{Z}_p^*$ 都有 $e(g^a, g^b) = e(g,g)^{ab}$;(2)**非退化性**　$e(g,g) \neq 1$.(3)**可计算性**　对于任何的 $g, h \in G_1$,存在一个有效的算法来计算 $e(g,h)$ 的值.

下面介绍本文模糊基于身份加密方案安全性所基于的复杂性假设:

定义 1　Decision q-Bilinear Diffie-Hellman Exponentiation(判定性 q-BDHE)问题[13]:设 G_1 是阶为素数 p 的乘法群,且存在双线性映射 $e: G_1 \times G_1 \to G_2$,给定 $2q+1$ 元组 $(g, h, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^q}, g^{\alpha^{q+2}}, \cdots, g^{\alpha^{2q}}) \in G_1^{2q+1}$ 以及 $T \in G_2$,其中未知,要求判断等式 $e(g,h)^{\alpha^{q+1}} = T$ 是否成立.如果对于任意多项式时间敌手 $\mathcal{A}$,其优势均小于一个可忽略的值,则称判定性 q-BDHE 假设成立.

2.2　模糊基于身份加密的一般化模型

根据文献[3],一个模糊基于身份加密体制一般是由如下四个多项式时间算法组成:

(1)**系统建立(Setup)**　该算法是由 PKG 完成的概率多项式时间算法,输入安全参数 λ,输出主密钥 msk 和系统公开参数 params 以及纠错距离 d,其中公开参数 params 和纠错距离 d 公开,主密钥 msk 保密.

(2)**密钥提取(Extract)**　该算法亦是由 PKG 完成的概率多项式时间算法,输入一个用户的身份 ID(这里用户的身份 ID 代表其拥有的一组属性集合)和主密钥 msk,算法输出对应 ID 的私钥 sk_{ID},并通过秘密信道安全的传送给该用户.

(3)**加密算法(Encrypt)**　该算法是由消息发送者完成的概率多项式时间算法,输入系统公开参数 params、消息以及用户的身份 ID',发送者生成消息对应的密文 C.

(4)**解密算法(Decrypt)**　该算法是由解密者完成的确定性多项式时间算法,输入系统公开参数 params、用户的身份 ID 及私钥 sk_{ID} 以及一个用身份 ID' 加密的密文 C,只要 ID 满足 $|ID' \cap ID| \geqslant d$,身份为 ID 用户就能解密密文 C 得到明文 M.

2.3　模糊基于身份加密方案的安全模型

我们提出的模糊基于身份加密方案在选择身份及适应性选择密文攻击下是不可区分的(IND-sID-CCA2),其正式定义用如下一系列游戏来刻画,这些游戏由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 共同进行:

(1)**初始化(Init)**　敌手 $\mathcal{A}$ 首先声明一个他要攻击的身份 ID^*,此 ID^* 即为在挑战阶段要使用到的身份.

(2)**系统建立(Setup)**　接收到敌手 $\mathcal{A}$ 的挑战身份 ID^* 之后,挑战者 $\mathcal{C}$ 输入安全参数 λ,运行系统建立算法得到主密钥 msk 和系统公开参数 params 以及纠错距离 d.挑战者 $\mathcal{C}$ 发送公开参数 parmas 以及纠错距离 d 给敌手 $\mathcal{A}$,并秘密保存主密钥 msk.

(3)**询问阶段 1(Phase 1)**　敌手 $\mathcal{A}$ 可以进行多项式次数的适应性**私钥提取询问和解密询问**,挑战者 $\mathcal{C}$ 利用自己掌握的主密钥 msk 相应的回答.

私钥提取询问　敌手 $\mathcal{A}$ 任意选择用户的身份 ID,要求 $|ID^* \cap ID| < d$,$\mathcal{C}$ 输出对应 ID 的私钥 sk_{ID}.

解密询问　敌手 $\mathcal{A}$ 任意选择一个利用身份 ID_i 对消息 M 加密的密文 C_i,要求挑战者 $\mathcal{C}$ 输出密文 C_i 对应的明文 M.

(4)**挑战阶段(Challenge)**　敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提供两个等长的消息 (M_0, M_1),挑战者 $\mathcal{C}$ 随机选择 $\beta \in \{0,1\}$,利用初始化阶段敌手 $\mathcal{A}$ 给定的 ID^* 对消息 M_β 进行加密得到密文 C^*,并将密文 C^* 发送给敌手 $\mathcal{A}$.

(5)**询问阶段 2(Phase 2)**　同询问阶段 1 类似,敌手 $\mathcal{A}$ 仍可进行多项式次数的适应性私钥提取询问和解密询问,但是敌手 $\mathcal{A}$ 不能询问被挑战的密文 C^*.

(6)**猜测阶段(Guess)**　最后,敌手 $\mathcal{A}$ 对于 β 的值给出一个猜测 β'.如果敌手 $\mathcal{A}$ 给出了正确的猜测我们称 $\mathcal{A}$ 赢得了游戏,而敌手的优势定义为 $|Pr[\beta' = \beta] - 1/2|$.

定义 2　如果一个敌手 $\mathcal{A}$ 能够在多项式时间 t 内最多进行了 q_k 次私钥提取询问,q_D 次解密询问后能有 ε 的优势赢得上述游戏,我们就称该模糊基于身份加密方案是 $(t, \varepsilon, q_K, q_D)$-IND-sID-CCA2 安全的.

3 固定长度且 CCA2 安全的模糊基于身份加密方案

本部分首先回顾一下 Lagrange 插值公式:设 $f(x)$是一个次数为 $d-1$ 次的单变元多项式,给定 d 个不同的值$(i, f(i))$,其中 S 是含 d 个不同元素的集合且 $i\in S$,利用 Lagrange 插值公式可求出 $f(x)=\sum_{i\in S}f(i)\Delta_{i,S}(x)$,其中 Lagrange 系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{(x-j)}{(i-j)}$.

假定系统属性全体为 U,$|U|=n$,简单起见我们用 $U=\{1,2,\cdots,n\}$来表示这 n 个属性.用户身份 $ID=(ID_1,\cdots ID_k)$,其中 $ID_i\in U$ 为其拥有的属性,d 代表最小的纠错距离且 $d\leqslant n$.我们构造了一个 CCA2 安全且密文长度为固定值的模糊基于身份加密方案,如果 $|ID'\cap ID|\geqslant d$,一个用身份 ID'加密的密文用 ID 的私钥也能解密.具体构造如下:

系统建立(Setup):设 G_1, G_2 都是阶为素数 p 的乘法群且 G_1 的生成元为 g,双线性映射 $e:G_1\times G_1\rightarrow G_2$,$H:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$是抗碰撞的哈希函数.密钥生成中心 PKG 从 G_1 中随机选择$(h_0,h_1,\cdots,h_n,\delta_1,\delta_2,\delta_3)$以及一个随机数 $a\in\mathbb{Z}_p^*$并令 $Z=e(g,g)^a$.则系统公开参数 $\text{params}=(g,Z,d,H,h_0,h_1,\cdots,h_n,\delta_1,\delta_2,\delta_3)$,系统主密钥 $\text{msk}=a$.

密钥提取(Extract):给定用户的身份 $ID=(ID_1,\cdots,ID_k)$,PKG 随机选择一个 $d-1$ 次的多项式 $f(x)$且满足 $f(0)=a$.对每个属性 $i\in ID$,PKG 选择随机数 $r_i\in\mathbb{Z}_p^*$计算用户的私钥 $sk_{ID}=(sk_{ID,1},sk_{ID,2},\cdots,sk_{ID,k})$,其中 $sk_{ID,i}=(g^{f(i)}(h_0h_i)^{r_i},g^{r_i},h_1^{r_i},\cdots,h_{i-1}^{r_i},h_{i+1}^{r_i},\cdots,h_n^{r_i})=(a_i,b_i,c_{i,1},\cdots,c_{i,i-1},c_{i,i+1},\cdots,c_{i,n})$.

加密算法(Encrypt):对于消息 $M\in G_2$ 以及身份 $ID'=(ID'_1,\cdots ID'_{k'})$,加密者随机选择 $r,s\in\mathbb{Z}_p^*$并计算密文 $C=(C_0,C_1,C_2,C_3,r)$,其中 $C_0=M\cdot Z^s$, $C_1=g^s$, $C_2=(h_0\prod_{i\in ID'}h_i)^s$, $C_3=(\delta_1^c\delta_2^r\delta_3)^s$, $c=H(ID',C_0,C_1,C_2)$.

解密算法(Decrypt):假定密文 $C=(C_0,C_1,C_2,C_3,r)$使用身份 ID'加密,而解密者拥有身份 ID 的私钥,且 $|ID'\cap ID|\geqslant d$.解密者选择 $S\subseteq(ID'\cap ID)$且满足 $|S|=d$,首先验证如下两等式是否成立:

$$e(g,C_2)=e(C_1,(h_0\prod_{i\in ID'}h_i)),$$

$$e(g,C_3)=e(C_1,(\delta_1^c\delta_2^r\delta_3)).$$

如果上式至少有一个不成立,表明密文 C 不是有效密文,解密者拒绝解密或返回错误消息;否则,解密者计算 $D_1=\prod_{i\in S}(a_i\prod_{j\in ID',j\neq i}(c_{i,j}))^{\Delta_{i,S}(0)}$, $D_2=\prod_{i\in S}(b_i)^{\Delta_{i,S}(0)}$,进而解密:

$$M=C_0\cdot e(C_2,D_2)/e(C_1,D_1).$$

4 方案的安全性与效率分析

4.1 正确性分析

正确性验证如下:

$$\begin{aligned}D_1&=\prod_{i\in S}(a_i\prod_{j\in ID',j\neq i}(c_{i,j}))^{\Delta_{i,S}(0)}\\&=\prod_{i\in S}(g^{f(i)}(h_0h_i)^{r_i}\prod_{j\in ID',j\neq i}(h_j)^{r_i})^{\Delta_{i,S}(0)}\\&=\prod_{i\in S}(g^{f(i)}(h_0\prod_{j\in ID'}(h_j))^{r_i})^{\Delta_{i,S}(0)}\\&=g^{\sum_{i\in S}f(i)\Delta_{i,S}(0)}\cdot(h_0\prod_{j\in ID'}(h_j))^{\sum_{i\in S}r_i\Delta_{i,S}(0)}\\&=g^a\cdot(h_0\prod_{j\in ID'}(h_j))^{\sum_{i\in S}r_i\Delta_{i,S}(0)}\end{aligned}$$

$$\begin{aligned}e(C_1,D_1)&=e(g^s,g^a\cdot(h_0\prod_{j\in ID'}(h_j))^{\sum_{i\in S}r_i\Delta_{i,S}(0)})\\&=e(g,g^a)^s\cdot e(g^{\sum_{i\in S}r_i\Delta_{i,S}(0)},(h_0\prod_{j\in ID'}(h_j))^s)\\&=Z^s\cdot e(D_2,C_2)\end{aligned}$$

故明文 $M=C_0\cdot e(C_2,D_2)/e(C_1,D_1)$ 成立.

4.2 方案的安全性

定理 1 如果在双线性群(G_1,G_2)内(t',ε',q)-BDHE 假设成立,并且假设攻击者最多 q_K 次私钥提取询问,q_D 次解密询问,那么本文提出的模糊基于身份加密方案在标准模型下对选择身份及 CCA2 攻击者是(t,ε,q_K,q_D)不可区分的,其中 $\varepsilon'=(\varepsilon-q_D/p)/2$, $t'=t+O(q_D\cdot P)$, P 表示一次双线性对运算的时间.

证: 设敌手 $\mathcal{A}$ 能以 ε 的优势攻击成功本文方案,给定挑战者 $\mathcal{C}$ 一个 q-BDHE 问题实例$(g,h,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}})\in G_1^{2q+1}$ 以及 $T\in G_2$,以下我们将演示 $\mathcal{C}$ 如何利用 $\mathcal{A}$ 来判定等式 $e(g,h)^{\alpha^{q+1}}=T$ 是否成立,进而解决判定性 q-BDHE 问题.

(1)**初始化** 在游戏开始之前,攻击者 $\mathcal{A}$ 首先给出要出要攻击的身份 ID^*.

(2)**系统建立** 挑战者 $\mathcal{C}$ 首先定义系统中使用到的属性为 $U=\{1,2,\cdots,n\}$,不失一般性,我们假定 $n=q$.$\mathcal{C}$ 再随机从$\mathbb{Z}_p^*$ 中选取 $\gamma_j(0\leqslant j\leqslant q)$并令 $h_0=g^{\gamma_0}\prod_{i\in ID^*}h_i^{-1}$, $h_i=g^{\gamma_i}g^{\alpha^{q-i+1}}$.进一步,$\mathcal{C}$ 随机选$\alpha'\in\mathbb{Z}_p^*$并令 $Z=e(g^{\alpha'},g)\cdot e(g^\alpha,g^{\alpha^q})$,这也就意味着主密钥 $a=\alpha'+\alpha^{q+1}$是 $\mathcal{C}$ 所未知的.此外,$\mathcal{C}$ 随机选 $d_2,d_3,e_1,e_2,e_3\in\mathbb{Z}_p^*$并令 $\delta_1=g_1g^{e_1}$, $\delta_2=g_1^{d_2}g^{e_2}$, $\delta_3=g_1^{d_3}g^{e_3}$,其中 $g_1=g^\alpha$.$\mathcal{C}$ 将公开参数 $\text{params}=(g,Z,d,H,h_0,h_1,\cdots,h_n,\delta_1,\delta_2,\delta_3)$发送给攻击者 $\mathcal{A}$,这里 $d<n$ 是纠错距离,$H:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$是抗碰撞哈希函数.

(3)**询问阶段 1** 敌手 $\mathcal{A}$ 可以进行多项式次数的适应性私钥提取询问和解密询问,挑战者 $\mathcal{C}$ 分别给出相应的回答.

(a)**私钥提取询问** 假设 $\mathcal{A}$ 最多 q_K 次私钥提取询

问,$\mathcal{A}$ 任意选择一个用户的身份 ID 满足 $|ID^* \cap ID| < d$,$\mathcal{A}$ 要求挑战者 $\mathcal{C}$ 输出 ID 对应的私钥.$\mathcal{C}$ 分别定义三个集合 T, T', T'' 如下:$T = ID \cap ID^*$, $T \subseteq T' \subseteq ID^*$ 且 $|T'| = d-1$, $T'' = T' \cup \{0\}$,并可令 $d-1$ 次多项式 $f(x)$ 满足 $f(0) = a = \alpha' + \alpha^{n+1}$($C$ 未知).对应每个属性 $i \in ID$,$\mathcal{C}$ 计算私钥 $sk_{ID,i}$ 如下:

①若 $i \in T'$,$\mathcal{C}$ 随机选 $t_i, r'_i \in \mathbb{Z}_p^*$ 并令 $f(i) = t_i$, $r_i = r'_i + \alpha^i$,可计算私钥

$$\begin{aligned} sk_{ID,i} &= (g^{f(i)}(h_0h_i)^{r_i}, g^{r_i}, h_1^{r_i}, \cdots, h_{i-1}^{r_i}, h_{i+1}^{r_i}, \cdots, h_n^{r_i}) \\ &= (g_i^t(h_oh_i)^{r'_i+\alpha^i}, g^{r'_i+\alpha^i}, h_1^{r'_i+\alpha^i}, \cdots h_{i-1}^{r'_{i-1}+\alpha'}, h_{i+1}^{r'_{i+1}+\alpha'}, \cdots, h_n^{r'_1+\alpha'}) \\ &= (g_i^t(h_oh_i)^{r'_i} \cdot (g^{\gamma_0}\prod_{j\in ID^*, j\neq i} h_j^{-1})^{\alpha i}, \\ &\quad g^{r'_i+\alpha^i}, h^{r'_i+\alpha^i}, \cdots h_{i+1}^{r'_i+\alpha^i}, h_{i+1}^{r'_{i+1}+\alpha} \cdots h_n^{r'_i+\alpha^i}) \end{aligned}$$

②若 $i \notin T'$,$\mathcal{C}$ 随机选 $r'_i \in \mathbb{Z}_p^*$ 并令 $r_i = r'_i - \Delta_{0,T''}(i)\alpha^i$,利用 Lagrange 公式:$f(i) = f(0)\Delta_{0,T''}(i) + \sum_{j\in T'} f(j)\Delta_{j,T''}(i)$,$\mathcal{C}$ 计算私钥:

$$\begin{aligned} sk_{ID,i} &= (g^{f(i)}(h_0h_i)^{r_i}, g^{r_i}, h_1^{r_i}, \cdots, h_{i-1}^{r_i}, h_{i+1}^{r_i}, \cdots, h_n^{r_i}) \\ &= (g^{\Delta_{0,T''}(i)f(0)+\sum_{j\in T'}\Delta_{j,T''}(i)\cdot f(j)}(h_0h_i)^{r'_i-\Delta_{0,T''}(i)\alpha^i}), \\ &\quad g^{r'_i-\Delta_{0,T''}(i)\alpha^i}, h_1^{r'_i-\Delta_{0,T''}(i)\alpha^i}, \cdots, h_{i-1}^{r'_i-\Delta_{0,T''}(i)\alpha^i}, \\ &\quad h_{i+1}^{r'_i-\Delta_{0,T''}(i)\alpha^i}, \cdots, h_n^{r'_i-\Delta_{0,T''}(i)\alpha^i}) \\ &= (g^{\Delta_{0,T''}(i)\alpha'+\sum_{j\in T'}\Delta_{j,T''}(i)t_j}(h_0h_i)^{r'_i}(h_0)^{-\Delta_{0,T''}(i)\alpha^i} \\ &\quad (g^{\alpha^i})^{-\Delta_{0,T''}(i)\gamma_i}, g^{r'_i-\Delta_{0,T''}(i)\alpha^i}, h_1^{r'_i-\Delta_{0,T''}(i)\alpha^i}, \cdots, \\ &\quad h_{i-1}^{r'_i-\Delta_{0,T''}(i)\alpha^i}, h_{i+1}^{r'_i-\Delta_{0,T''}(i)\alpha^i}, \cdots, h_n^{r'_i-\Delta_{0,T''}(i)\alpha^i}) \end{aligned}$$

(*b*)**解密询问**　攻击者 $\mathcal{A}$ 提交对身份 ID' 加密的密文 $C = (C_0, C_1, C_2, C_3, r)$,$\mathcal{C}$ 首先计算 $c = H(ID', C_0, C_1, C_2)$,并验证如下两等式是否成立:

$$e(g, C_2) = e(C_1, (h_0\prod_{i\in ID'} h_i));$$

$$e(g, C_3) = e(C_1, (\delta_1^c\delta_2^r\delta_3)).$$

如果上面两个等式至少有一个不成立,则表明密文 C 不是有效密文,这时解密者拒绝解密或返回一错误消息;否则,$\mathcal{C}$ 计算 $M = C_0/e(C_3/C_1^{e_1+re_2+e_3}, g_2^{(c+rd_2+d_3)^{-1}})$ 并发送给 $\mathcal{A}$,其中 $g_2 = g^{\alpha'} \cdot g^{\alpha^q}$.

(4)**挑战阶段**　敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提供两个等长的消息 (M_0, M_1),挑战者 $\mathcal{C}$ 随机选择 $\beta \in \{0,1\}$,并利用初始化阶段敌手 $\mathcal{A}$ 给定的 ID^* 对消息 M_β 进行加密得到密文 $C^* = (C_0^*, C_1^*, C_2^*, C_3^*, r^*)$ 如下,并将密文 C^* 发送给敌手 $\mathcal{A}$:

$$C_0^* = M_\beta T \cdot e(h, g^{\alpha'}), C_1^* = h, C_2^* = h^{\gamma_0},$$

$$C_3^* = h^{e_1c^*+r^*e_2+e_3}, r^* = -(c^*+d_3)/d_2,$$

$$c^* = H(ID^*, C_0^*, C_1^*, C_2^*).$$

如果 $\mu = 0$,则 $T = e(g^{\alpha^{q+1}}, h)$,挑战密文 C^* 是对 M_β 的有效密文;如果 $\mu = 1$, T 是 G_T 中随机元素,则对于敌手 $\mathcal{A}$ 来说,挑战密文 C^* 是与 β 无关的随机值.

(5)**询问阶段 2**　同询问阶段 1 类似,敌手 $\mathcal{A}$ 进行多项式次数的适应性**私钥提取询问和解密询问**,$\mathcal{C}$,分别给出相应的回答.

(6)**猜测阶段**:　最后,敌手 $\mathcal{A}$ 对于 M_β 的值给出一个猜测 β'.如果敌手 $\mathcal{A}$ 给出了正确的猜测,即 $\beta' = \beta$,挑战者 $\mathcal{C}$ 输出 $\mu' = 0$ 猜测 $T = e(g^{\alpha^{q+1}}, h)$;否则 $\mu' = 1$ 猜测 T 是 G_2 中随机元素.

概率分析　上述过程成功,即挑战者解决判定性 q-BDHE 问题的成功概率分析如下:

如果 $\mu = 1$,即 T 是 G_T 中随机元素,则对于敌手 $\mathcal{A}$ 来说,$\mathcal{A}$ 从挑战密文 C^* 中不会获得关于 β 任何信息,因此有 $Pr[\beta' \neq \beta | \mu = 1] = Pr[\beta' = \beta | \mu = 1] = 1/2$.

如果 $\mu = 0$,此时 $T = e(g^{\alpha^{q+1}}, h)$,挑战密文 C^* 是对 M_β 的有效密文,而敌手 $\mathcal{A}$ 有 ε 的概率成功解密.注意到在游戏模拟过程 $\mathcal{C}$ 可能会有 q_D/p 的概率失败,故此时有 $Pr[\beta' = \beta | \mu = 0] = \varepsilon + (1/2) - (q_D/p)$.

综上可得,挑战者能够成功解决判定性 q-*BDHE* 问题的优势为:

$(1/2)Pr[\beta' = \beta | \mu = 0] + (1/2)Pr[\beta' = \beta | \mu = 1] - (1/2) = (\varepsilon - (q_D/p))/2$　　证毕.

4.3　性能比较

在本节我们主要通过计算开销和通信开销两方面来综合分析本方案的性能,并给出了我们的方案与已有的模糊基于身份加密方案进行了性能对比.其中,计算开销主要由加密运算和解密运算两部分组成,通信开销为密文长度.此外,我们还对私钥长度,安全性等进行了比较,具体如表 1 所示:

表 1　与已有的模糊基于身份加密体制的性能比较

方案	密文长度	加密复杂度	解密复杂度	私钥长度	安全性
[3]	$(n)G_1 + G_2$	$(d+1)E$	$(d)P$	$(k)G_1$	CPA
[6]	$(n+1)G_1 + G_2$	$(n+2)E$	$(d+1)P$	$(2k)G_1$	CPA
本文	$3G_1 + G_2 + \mathbb{Z}_p$	$6E$	$6P$	$k(n+1)G_1$	CCA

不失一般性,在性能比较中,我们仅考虑最耗时的双线性对运算(用 P 表示一个双线性对运算时间)和次耗时的幂指数运算(用 E 表示一个幂指数运算所花费的时间).在表 1 中,n 表示系统属性个数,d 为纠错距离,$k(1 \leq k \leq n)$为用户拥有的属性数目.通过表 1 可以看出,文献[3,6]中的方案密文长度以及解密算法所需双线性对运算的个数都与系统属性数目 n 以及纠错距离 d 线性相关,而本文方案密文长度达到了固定值(3 个群 G_1、1 个群 G_2 以及 1 个 $\mathbb{Z}_p$ 中的元素),并且只需要 6 个双线性对运算,通信量和计算效率都有了很大改进.此外,文献[3,6]方案不能抵抗选择密文攻击,而本

文方案在选择密文攻击下仍然可证安全,安全性也有明显提高.但是,与文献[3,6]方案相比,本文方案私钥长度较大,通过在私钥中嵌入系统公开参数的方法,使得密文长度达到了固定值.即本文方案通过牺牲用户存储代价来达到降低通信带宽,提高运算效率的目的.但是,在网络环境中,系统的通信带宽通常会成为瓶颈,要提高系统的通信带宽往往需要很高的代价,而增加存储量相对比较容易,也即本文方案是可行的.

5 结论

最近提出的两个模糊基于身份加密方案[7,9]均存在安全缺陷[11,12],目前尚未构造出固定密文长度且能够达到 CCA2 安全的模糊基于身份加密方案,为此我们构造了一个新的模糊基于身份加密方案,在标准模型下基于判定性 q-BDHE 困难假设证明了其对适应性选择密文攻击是不可区分的(也即达到了 CCA2 安全性).新方案密文长度以及双线性对运算都首次达到了固定值,具有较高的运算效率.但是,本文方案只能在弱的敌手(选择身份)模型下证明其安全性,如何在标准模型下构造一个完全安全的固定密文长度的模糊基于身份加密方案,这是当前研究的公开难题,也是下一步我们要继续研究的问题.

参考文献

[1] Shamir A. Identity-based cryptosystems and signature schemes [A]. Proceedings of the CRYPTO 1984 [C]. LNCS 196. Berlin: Springer-Verlag, 1984. 47 – 53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [A]. Proceedings of the CRYPTO 2001 [C]. LNCS 2139. Berlin: Springer-Verlag, 2001. 213 – 229.

[3] Sahai A, Waters B. Fuzzy identity-based encryption [A]. Proceedings of the EUROCRYPT 2005 [C]. LNCS 3494. Berlin: Springer-Verlag, 2005. 166 – 180.

[4] 杨庚,等.基于身份加密的无线传感器网络密钥分配方法[J].电子学报,2007,35 (1):180 – 184.
Yang Gong, et al. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms [J]. Acta Electronica Sinica, 2007, 35 (1): 180 – 184. (in Chinese)

[5] 袁春,文振,张基宏,钟玉琢.基于密码学的访问控制和加密安全数据库[J].电子学报,2006,:2043 – 2046.
Yuan Chun, et al. Progress of cryptographic access control and encryption security database [J]. Acta Electronica Sinica, 2006, 34(11): 2043 – 2046. (in Chinese)

[6] Baek J, Susilo W, Zhou J. New constructions of fuzzy identity-based encryption [A]. Proceedings of the ACM Symposium on Information Computer and Communication Security 2007 [C]. New York: ACM, 2007. 368 – 370.

[7] Ren Y, et al. New fuzzy identity-based encryption in the standard model [J]. Informatica, 2010, 21(3): 393 – 4074.

[8] Sarier N. A new biometric identity based encryption scheme secure against DoS attacks [J]. Security and Communication Networks, 2011, 4(1): 23 – 32.

[9] Yang Y, Hu Y, Zhang L, Sun C. CCA2 secure biometric identity based encryption with constant-size ciphertext [J]. Journal of Zhejiang University-Science C (Computers & Electronics), 2011, 12(10): 819 – 827.

[10] Canetti R, et al. The random oracle methodology revisited [J]. Journal of the ACM, 2004, 51(4): 557 – 594.

[11] Tian M, Yang W, Huang L. Security of a biometric identity-based encryption scheme [J/OL]. http://arxiv.org/abs/1110.2653v2, 2013-01-24.

[12] Tian M, Huang L, Yang W. Secruity analysis of a fuzzy identity-based encryption scheme [J/OL]. http://eprint.iacr.org/2011/523, 2013-01-24.

[13] Boneh D, Boyen X, Goh E. Hierarchical identity based encryption with constant size ciphertext [A]. Proceedings of the EUROCRYPT 2005 [C]. LNCS 3494. Berlin: Springer-Verlag, 2005: 166 – 180.

作者简介

葛爱军 男,1985 年出生,山东潍坊人,解放军信息工程大学博士生,主要研究方向为公钥加密、数字签名等.
E-mail: geaijun@163.com

马传贵(通讯作者) 男 1962 年出生,山东菏泽人,博士,解放军信息 工程大学教授,博士生导师,主要研究方向为公网络与信息安全等.
E-mail: chuanguima@sina.com

程庆丰 男,1979 年出生,辽宁朝阳人,博士,解放军外国语学院讲师,主要研究方向为密码学、信息安全等.
E-mail: qingfengc2008@sina.com