一个有效的多PKG环境下基于身份签密方案

赵秀凤[1),2)] 徐秋亮[2)]

[1)](信息工程大学电子技术学院 郑州 450004)

[2)](山东大学计算机科学与技术学院 济南 250101)

摘 要 多PKG环境下的签密机制是域间实体认证和保密通信的有效手段.文中提出了一个新的多PKG环境下基于身份的签密方案,方案使用了Waters基于身份加密体制及现有的基于身份签密体制的构造思想,并利用"⊕"运算和抗碰撞Hash函数消除了签密密文与明文之间的对应关系,从而保证了方案的语义安全.文中的方案实现了标准模型下的可证明CCA安全和存在不可伪造性;且当新方案退化为单个PKG环境时,与其它标准模型下的安全方案相比,该方案仍有稍高的效率.

关键词 基于身份签密;多PKG;双线性对;可证明安全;标准模型

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.00673

An Efficient Multi-PKG ID-Based Signcryption Scheme

ZHAO Xiu-Feng[1),2)] XU Qiu-Liang[2)]

[1)](*Institute of Electronic Technology, Information Engineering University, Zhengzhou* 450004)

[2)](*School of Computer Science and Technology, Shandong University, Jinan* 250101)

Abstract Signcryption with multiple private key generators (PKGs) can provide valid solution for authentication and confidential communication among entities in different domain. In this paper, a new identity-based signcryption scheme with multiple PKGs is proposed. We used the ideas of Waters IBE scheme and existing IBS scheme, we also employed "⊕" and hash function to eliminate the corresponding relation between plaintext message and ciphertext. Our scheme achieves CCA secure and existential unforgeability in the standard model. Moreover, when adapted in single PKG environment, our scheme is more efficient than the existing ones.

Keywords identity-based signcryption; multi-PKG; bilinear pairings; provably secure; standard model

1 引 言

随着新型网络计算背景的出现,跨域认证和保密通信技术成为一个关键和迫切需要解决的问题.签密能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能,而其所花费的代价,要远远低于传统的先签名后加密的方法,因此它是实现既保密又认证的传输信息的较为理想的方法.多PKG环境下基于身份的签密机制能够很好地解决域间实体的安全认证和保密通信问题.

签密技术于1997年由Zheng[1]首次提出,2002年Malone-Lee[2]利用双线性对构造了第一个基于身份的签密方案,随后,许多高效的签密方案被相继提出[3-11].其中,Yu等人[7]提出了第一个标准模型下可证安全的签密方案,但随后被Zhang[8]和Jin等

收稿日期:2011-06-28;最终修改稿收到日期:2011-12-14.本课题得到国家自然科学基金(61173139)、教育部博士点基金(20110131110027)和山东省自然科学基金重点项目(ZR2011FZ005)资助.**赵秀凤**,女,1977年生,博士研究生,讲师,主要研究兴趣为可证安全的公钥密码算法、认证及密钥协商协议的分析与设计.E-mail: zhao_xiu_feng@163.com. **徐秋亮**(通信作者),男,1960年生,博士,教授,博士生导师,主要研究领域为多方安全计算、数字签名、基于身份的密码体制等.E-mail: xql@sdu.edu.cn.

人[9]分别指出该方案不满足密文不可区分性和密文不可伪造性并给出了改进的方案. 但是我们发现,Zhang 改进的方案依然不满足密文不可区分性,原因是敌手获得挑战密文后,通过解签密的验证等式可以验证签密密文与明文消息的对应关系,从而可以进行密文区分. 最近,Li 等人[10]也指出 Zhang[8]给出的改进方案不满足 CCA 安全,同时指出 Jin 等人[9]的改进方案不满足不可伪造性,并基于 Kiltz 和 Vahlis 的 IBE 方案及 Paterson 和 Schuldt 的 IBS 方案给出了一个新的在标准模型下可证明安全的身份基签密方案. 2010 年,张波等人[11]给出了一个高效的基于身份多签密方案,但是在签密者对消息签密的过程中,不仅需要解签密者的身份信息,还需要解签密者的公钥参与运算,因此该方案涉及到公钥认证问题.

上述签密方案要求所有的通信实体都必须处在一个相同的 PKG(private key generator)的管理之下,极大地限制了方案的适用范围. 2007 年,Li 等人[12]提出了可用于多域的基于身份签密方案,很好地实现了域间秘密信息既保密又认证的安全传输. 该方案中域间通信的不同 PKG 共享相同的公共参数. 随后,Li 等人[13]对上述方案进行了优化,提高了计算效率,而且可以扩展到多个 PKG 拥有不同的系统参数. 但是,Zhang 等人[14]指出 Li 等人的两个方案在选择密文攻击下是不安全的. 与此同时,闻英友等人[15]也给出了一个可用于多域的可证明安全的签密方案,并且多个 PKG 拥有不同的系统参数和各自的公私钥. 但是上述签密方案的安全性都依赖于随机预言模型.

借助于 Waters 的 IBE 体制[16]及基于身份签密方案[8-11],本文提出了一个有效的多 PKG 环境下基于身份签密方案,并在标准模型下对方案的 CCA2 安全和存在性不可伪造性进行了证明,这是第一个在标准模型下可证安全的多 PKG 环境下基于身份签密方案,同时也适用于单个 PKG 环境.

2 背景知识

2.1 双线性对

设 G 和 G_T 为两个素数 p 阶的循环群,g 是群 G 的生成元,双线性对 e 是一个双线性映射 $e:G\times G\rightarrow G_T$,满足下面的特性:

(1) 双线性. 对所有的 $u,v\in G$, $a,b\in Z$,有 $e(u^a,v^b)=e(u,v)^{ab}$;

(2) 非退化性. $e(g,g)$ 不是 G_T 的生成元;

(3) 可计算性. 对于任何 $P,Q\in G$,存在有效的算法计算 $e(P,Q)$.

2.2 DBDH 假设

判定双线性 Diffie-Hellman(DBDH)问题. 挑战者随机选择 $a,b,c,z\in Z_p^*$ 和随机掷币 $\gamma\in\{0,1\}$. 如果 $\gamma=1$,则输出元组 $(g,A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc})$,否则输出 $(g,A=g^a,B=g^b,C=g^c,Z=e(g,g)^z)$,其中 g 为群 G 的生成元,攻击者输出对 γ 的猜测 γ'. 对于多项式时间的概率算法 $\mathcal{A}$,如果有

$$|Pr[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-Pr[\mathcal{A}(g,g^a,g^b,g^c,Z)=1]|\geq 2\varepsilon,$$

则称 $\mathcal{A}$ 至少以优势 ε 解决群 G 上的 DBDH 问题.

DBDH 假设. 对于所有的概率多项式时间算法 $\mathcal{A}$,优势 ε 是可以忽略的.

2.3 CDH 假设

计算性 Diffie-Hellman(CDH)问题. 群 G 中的 CDH 问题是指对于给定的随机的元组 (g,g^a,g^b) 计算出 g^{ab},其中 g 为群 G 的生成元,a,b 从 Z_p^* 中随机选取. 一个多项式时间内的概率算法 $\mathcal{A}$ 成功解决群 G 上的 CDH 问题的概率定义为

$$Adv_{\mathcal{A}}^{\mathrm{CDH}}=|Pr[\mathcal{A}(g,g^a,g^b)=g^{ab}:a,b\in Z_p^*]|.$$

CDH 假设. 对于所有的概率多项式时间算法 $\mathcal{A}$,$Adv_{\mathcal{A}}^{\mathrm{CDH}}$ 是可以忽略的.

3 多 PKG 基于身份签密的形式化模型

3.1 概念模型

多 PKG 环境下基于身份的签密方案由以下 5 个算法构成:全局建立 G-Setup,域建立 D-Setup,私钥提取 Extract,签密 Signcrypt,解签密 Unsigncrypt.

全局建立 G-Setup. 输入安全参数,输出全局公开的系统参数 *params*.

域建立 D-Setup. 输入全局公开的系统参数 *params*,每个域 PKG_x $(x=1,2,\cdots,l)$ 输出一个主密钥 s_x 和相应的域公钥 P_x(我们假设有 l 个域),公开域公钥 P_x,保存主密钥 s_x.

私钥提取 Extract. 输入域 PKG_x 中的身份 ID,PKG_x 计算相应的私钥 S_{ID} 并通过安全信道发送给用户 ID.

签密 Signcrypt. 假设签密者为 PKG_1 中的用户 A,解签密者为 PKG_2 中的用户 B. 输入全局公开的

系统参数 $params$、域公钥 P_1 和 P_2、签密者的私钥 S_{ID_A}、待签密明文消息 m 以及解签密者身份信息 ID_B，输出签密者对消息 m 的签密密文 σ，该算法由签密者运行.

解签密 Unsigncrypt. 输入全局公开的系统参数 $params$、域公钥 P_1 和 P_2、签密者身份 ID_A、解签密者私钥 S_{ID_B} 和签名 σ，输出明文消息 m 或者表示解签密失败的符号 $\perp$.

3.2　安全性定义

Li 等人[12-13]给出了多 PKG 环境下基于身份签密的安全性定义，包括自适应选择密文攻击下的密文不可区分性和自适应选择消息攻击下的密文存在性不可伪造性.

定义 1(机密性).　如果不存在多项式时间的敌手可以以不可忽略的概率赢得下面的游戏，则称多 PKG 环境下基于身份的签密方案(MPIDSC)在自适应选择密文攻击下具有密文不可区分性(IND-MPIDSC-CCA2).

游戏参与者包括挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$，游戏过程如下.

建立. 挑战者 $\mathcal{C}$ 选定安全参数 k，执行建立 G-Setup 算法和 D-Setup 算法，并将全局系统参数 $params$ 和域公钥 $P_x(x=1,2,\cdots,l)$ 发送给敌手 $\mathcal{A}$，秘密的持有主密钥 $s_x(x=1,2,\cdots,l)$.

第一阶段敌手执行多项式次数的询问，这些询问可以是自适应选择的，也就是说，每个询问都可以在前一个询问基础上进行. 敌手可以进行的询问包括：

私钥提取询问. 敌手可以发起对任意域 PKG_x 中任意身份 ID 的询问并获得与该身份信息相关的私钥 $S_{ID}=Extract(ID)$.

签密询问. 敌手可以发起对签密者身份 ID_A、接收者身份 ID_B 和消息 m 的签密询问. $\mathcal{C}$ 计算 $S_{ID_A}=Extract(ID_A)$ 和 $\sigma=Signcrypt(m,S_{ID_A},ID_B)$，并将签密密文 σ 发送给敌手.

解签密询问. 敌手可以产生对签密者身份信息 ID_A、接收者身份 ID_B 和签密密文 σ 的解签密询问. $\mathcal{C}$ 计算 $S_{ID_A}=Extract(ID_A)$，并将解签密结果 $\mathrm{Unsigncrypt}(\sigma,ID_A,S_{ID_B})$ 发送给敌手，这个结果可能是合法的明文消息 m 或在 σ 为不合法密文情况下的符号 $\perp$.

挑战. 敌手选择两个明文消息 m_0 和 m_1 以及他想挑战的签密者身份 ID_A^* 和接收者身份 ID_B^*. 注意到：他不能够在第一阶段中询问过与身份信息 ID_B^* 相关的私钥. $\mathcal{C}$ 选择随机比特 γ，计算签密密文 $\sigma^*=Signcrypt(m_\gamma,S_{ID_A^*},ID_B^*)$ 并将其发送给敌手.

第二阶段敌手可以进行和第一阶段相同的多项式次数询问，但是，他不能够发起对身份信息 ID_B^* 的私钥提取询问以及对签密密文 σ^* 在接收者身份为 ID_B^* 的解签密询问.

猜测. 最后，敌手输出对 γ 的猜测值 $\gamma'\in\{0,1\}$，如果 $\gamma'=\gamma$，则称敌手成功. 上述敌手被称为 IND-MPIDSC-CCA2 攻击者，敌手成功的概率优势定义为

$$Adv^{\text{IND-MPIDSC-CCA2}}=|Pr[\gamma'=\gamma]-1/2|.$$

定义 2(不可为造性).　如果不存在多项式时间的敌手可以以不可忽略的概率赢得下面的游戏，则称多 PKG 环境下基于身份签密方案在自适应选择消息攻击下具有密文的存在性不可伪造性(EUF-MPIDSC-CMA).

游戏过程如下：.

建立. 挑战者 $\mathcal{C}$ 选定安全参数 k，执行建立 G-Setup 算法和 D-Setup 算法，并将全局系统参数 $params$ 和域公钥 $P_x(x=1,2,\cdots,l)$ 发送给敌手 $\mathcal{A}$，秘密的持有主密钥 $s_x(x=1,2,\cdots,l)$.

询问. 如同定义 2 中一样，敌手可以自适应地发起多项式次数的询问.

伪造. 敌手产生新的元组 (σ,ID_A,S_{ID_B})(即不是由签密询问得到的元组)，如果解签密的结果 $Unsigncrypt(\sigma,ID_A,S_{ID_B})$ 不是符号 $\perp$，则称敌手成功，即敌手产生了合法的签密密文.

4　具体方案

4.1　方案描述

在下面的描述中，不妨设所有的身份信息都由具有固定长度 n_u 的字符串表示. 为保证方案的通用性，可以使用抗碰撞的 Hash 函数完成对任意长度身份信息的处理. 具体的多 PKG 环境下基于身份签密方案包括如下算法.

G-Setup. 选择素数 p 阶群 G 和 G_T，$e:G\times G\to G_T$ 为双线性对，g 为群 G 的生成元. 选定随机元素 $g_2\leftarrow_R G$，另外，选择群 G 中元素 u'，$m'\leftarrow_R G$ 和长度分别为 n_u 和 n_m 的向量 $\boldsymbol{\Lambda}_U=(u_i)$，$\boldsymbol{\Lambda}_M=(m_i)$，向量中的元素为群 G 中的随机元素. H 和 H_m 为密码学意义上的 Hash 函数，$H:G_T\to\{0,1\}^{l_t}$，其中 l_t 表示明文消息长度. $H_m:\{0,1\}^{l_t}\times G_T\to\{0,1\}^{n_m}$ 全局系统参数为 $params=\{G,G_T,e,g,g_2,u',\boldsymbol{\Lambda}_U,m',\boldsymbol{\Lambda}_M,$

$H, H_m\}$.

D-Setup. 每个 $PKG_x(x=1,2,\cdots,l)$ 选择一个随机元素 $\alpha_x \in Z_p$ 并计算域公钥 $P_x = g^{\alpha_x}$ 和相应的主密钥 $s_x = g_2^{\alpha_x}$.

Extract. 令 u 为具有长度 n_u 的表示身份的字符串，$u[i]$ 为 u 的第 i 比特，定义 $\mathcal{U} \subset \{1,2,\cdots,n_u\}$ 为 $u[i]=1$ 的位 i 的集合. 为构造与身份信息 u 相关的私钥 d_u，随机选择 $r_u \leftarrow Z_p$，并计算

$$d_u = (d_{u1}, d_{u2}) = (s_x (u' \prod_{i \in \mathcal{U}} u_i)^{r_u}, g^{r_u}).$$

这里不妨设签密者 Alice 为域 PKG_1 注册的用户，身份信息为 u_A，解签密者 Bob 为域 PKG_2 注册的用户，身份信息为 u_B. 他们的私钥分别由 PKG_1 和 PKG_2 生成：

$$d_A = (d_{A1}, d_{A2}) = \left(g_2^{\alpha_1} \left(u' \prod_{j \in \mathcal{U}_A} u_j\right)^{r_A}, g^{r_A}\right)$$

和

$$d_B = (d_{B1}, d_{B2}) = \left(g_2^{\alpha_2} \left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_B}, g^{r_B}\right).$$

Signcrypt. 令 m 为待签密消息，为发送消息 m 给接收者 Bob，签密者 Alice 选择随机数 $r_m \in Z_p$ 并执行以下步骤：

(1) 计算 $R = e(P_2, g_2)^{r_m}$，其中 $P_2 = g^{\alpha_2}$ 为 PKG_2 的域公钥，计算 $\sigma_1 = m \oplus H(R)$；

(2) 计算 $\sigma_2 = g^{r_m}$；

(3) 计算 $\sigma_3 = \left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_m}$；

(4) 计算 $M = H_m(m \| R)$ 和 $\sigma_4 = d_{A1} \cdot \left(m' \prod_{j \in \mathcal{M}} m_j\right)^{r_m}$，其中 $\mathcal{M} \subset \{1,2,\cdots,n_m\}$ 为 $M[i]=1$ 的位 i 的集合；

(5) $\sigma_5 = d_{A2}$.

最终的签密密文为 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

Unsigncrypt. 接收到签密密文 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ 后，Bob 执行以下步骤进行解签密：

(1) 计算 $R = e(d_{B1}, \sigma_2) e(d_{B2}, \sigma_3)^{-1}$；

(2) 计算 $m = \sigma_1 \oplus H(R)$；

(3) 计算 $M = H_m(m \| R)$.

当且仅当等式

$$e(\sigma_4, g) = e(P_2, g_2) e\left(u' \prod_{j \in \mathcal{U}_A} u_j, \sigma_5\right) e\left(m' \prod_{j \in \mathcal{M}} m_j, \sigma_2\right)$$

成立时 Bob 接受该签密密文.

4.2 正确性

方案的正确性可以由下面的等式验证

$$\begin{aligned}
&e(d_{B1}, \sigma_2) e(d_{B2}, \sigma_3)^{-1} \\
&= e\left(g_2^{\alpha_2} \left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_B}, g^{r_m}\right) e\left(g^{r_B}, \left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_m}\right)^{-1} \\
&= e(g_2^{\alpha_2}, g^r) e\left(\left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_B}, g^{r_m}\right) e\left(g^{r_B}, \left(u' \prod_{j \in \mathcal{U}_B} u_j\right)^{r_m}\right)^{-1} \\
&= e(g_2^{\alpha_2}, g^{r_m}) = e(g^{\alpha_2}, g_2)^{r_m} = e(P_2, g_2)^{r_m} = R, \\
&e(\sigma_4, g) = e\left(d_{A1} \cdot \left(m' \prod_{j \in \mathcal{M}} m_j\right)^{r_m}, g\right) \\
&= e\left(g_2^{\alpha_1} \left(u' \prod_{j \in \mathcal{U}_A} u_j\right)^{r_A}, g\right) e\left(\left(m' \prod_{j \in \mathcal{M}} m_j\right)^{r_m}, g\right) \\
&= e(g_2^{\alpha_1}, g) e\left(\left(u' \prod_{j \in \mathcal{U}_A} u_j\right)^{r_A}, g\right) e\left(\left(m' \prod_{j \in \mathcal{M}} m_j\right)^{r_m}, g\right) \\
&= e(g^{\alpha_1}, g_2) e\left(u' \prod_{j \in \mathcal{U}_A} u_j, g^{r_A}\right) e\left(m' \prod_{j \in \mathcal{M}} m_j, g^{r_m}\right) \\
&= e(P_2, g_2) e\left(u' \prod_{j \in \mathcal{U}_A} u_j, \sigma_5\right) e\left(m' \prod_{j \in \mathcal{M}} m_j, \sigma_2\right).
\end{aligned}$$

4.3 安全性

定理 1. 假设存在定义 1 中的 IND-MPIDSC-CCA2 敌手，经过至多 q_E 次私钥提取询问、q_S 次签密询问以及 q_U 次解签密询问，可以以优势 ε 区分两个合法密文，则存在一个区分者 $\mathcal{D}$，可以以

$$\frac{\varepsilon}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}$$

的优势解决判定双线性 Diffie-Hellman 问题.

证明. 假设区分器 $\mathcal{D}$ 获得随机双线性判定 Diffie-Hellman 问题实例 $(g, g^a, g^b, g^c, Z \in G_T)$，他的目标是判断等式 $Z = e(g,g)^{abc}$ 是否成立. 区分器 $\mathcal{D}$ 将把定义 1 中的 IND-MPIDSC-CCA2 敌手作为子过程同时充当游戏中的挑战者，具体的模拟过程如下.

建立. 该过程包括 G-Setup 和 D-Setup.

G-Setup. 令 $l_u = 2(q_E + q_S + q_U)$ 和 $l_m = 2q_S$，$\mathcal{D}$ 随机选择

(1) 两个整数 k_u 和 k_m $(0 \le k_u \le n_u, 0 \le k_m \le n_m)$；

(2) 整数 $x' \in Z_{l_u}$，一个 n_u 维向量 $\boldsymbol{X} = (x_i)$，$x_i \in Z_{l_u}$；

(3) 整数 $z' \in Z_{l_m}$，一个 n_m 维向量 $\boldsymbol{Z} = (z_j)$，$z_j \in Z_{l_m}$；

(4) 两个整数 $y', w' \in Z_p$，一个 n_u 长度的向量 $\boldsymbol{Y} = (y_i)$ $(y_i \in Z_p)$ 和一个 n_m 长度的向量 $\boldsymbol{W} = (w_j)$ $(w_j \in Z_p)$.

为方便分析，对身份 u 和消息 m 分别定义函数：

$$F(u) = -l_u k_u + x' + \sum_{i \in \mathcal{U}} x_i,\ J(u) = y' + \sum_{i \in \mathcal{U}} y_i,$$

$$K(m) = -l_m k_m + z' + \sum_{j \in \mathcal{M}} z_j,\ L(m) = w' + \sum_{j \in \mathcal{M}} w_j.$$

$\mathcal{D}$ 设定全局系统参数：

$$g_2 = g^b,$$

$$u' = g_2^{-n_u k_u + x'} g^{y'},\ u_i = g_2^{x_i} g^{y_i} (1 \le i \le n_u),$$

$m'=g_2^{-n_m k_m+z'}g^{w'}$，$m_j=g_2^{z_j}g^{w_j}(1\leq j\leq n_m)$.

因此对任意身份信息 u 和明文消息 m，有

$$u'\prod_{i\in\mathcal{U}}u_i=g_2^{F(u)}g^{J(u)},\quad m'\prod_{j\in\mathcal{M}}m_j=g_2^{K(u)}g^{L(u)}.$$

D-Setup. $\mathcal{D}$ 随机选择 $i^*\in\{1,2,\cdots,l\}$，设定域 PKG_{i^*} 的公钥为 $P_{i^*}=g^a$，并诚实地计算其他每个域 PKG_x 的公钥 g^{α_x} 和主密钥 $s_x=g_2^{\alpha_x}$，其中随机元素 $\alpha_x\in Z_p$.

第一阶段敌手执行多项式次数的询问，$\mathcal{D}$ 应答.

私钥提取询问. 当敌手对选择的身份信息 u 做私钥提取询问时，$\mathcal{D}$ 挑战者首先检查 u 所属的域，

(1) 如果 u 是域 $PKG_x(x\neq i^*)$ 的用户，则随机选择 $r_u\leftarrow Z_p$，并计算

$$d_u=(d_{u1},d_{u2})=\left(g_2^{\alpha_x}\left(u'\prod_{i\in\mathcal{U}}u_i\right)^{r_u},g^{r_u}\right).$$

(2) 如果 u 是域 PKG_{i^*} 的用户，则检查 $F(u)=0 \bmod l_u$ 是否成立，如果成立，则停止游戏，如果不成立，挑战者选择随机数 $r_u\leftarrow Z_p$，计算

$$d_u=(d_{u1},d_{u2})=\left(P_{i^*}^{-\frac{J(u)}{F(u)}}\cdot\left(u'\prod_{i\in\mathcal{U}}u_i\right)^{r_u},P_{i^*}^{-\frac{1}{F(u)}}g^{r_u}\right)$$

并将其返回给敌手.

当 $F(u)\neq 0 \bmod l_u$ 时挑战者可以产生 d_u，这个模拟是完美的，即 d_u 是身份信息 u 对应的合法私钥，这是因为令 $\hat{r}_u=r_u-\frac{a}{F(u)}$，有

$$\begin{aligned}d_{u1}&=P_{i^*}^{-\frac{J(u)}{F(u)}}\cdot(g_2^{F(u)}g^{J(u)})^{r_u}\\&=g^{-\frac{a\cdot J(u)}{F(u)}}\cdot(g_2^{F(u)}g^{J(u)})^{r_u}\\&=g_2^a(g_2^{F(u)}g^{J(u)})^{-\frac{a}{F(u)}}\cdot(g_2^{F(u)}g^{J(u)})^{r_u}\\&=g_2^a(g_2^{F(u)}g^{J(u)})^{r_u-\frac{a}{F(u)}}\\&=g_2^a(g_2^{F(u)}g^{J(u)})^{\hat{r}_u},\end{aligned}$$

$$d_{u2}=P_{i^*}^{-\frac{1}{F(u)}}g^{r_u}=g^{-\frac{a}{F(u)}}g^{r_u}=g^{r_u-\frac{a}{F(u)}}=g^{\hat{r}_u}.$$

如果 $F(u)=0 \bmod p$，上面的计算是无法进行的，挑战者 $\mathcal{D}$ 将退出游戏. 为使分析更加简单，不妨设 $l_u(n_u+1)<p$ 即 $0<l_u n_u<p$，容易得到

$$-p<F(u)=-l_u k_u+x'+\sum_{i\in\mathcal{U}}x_i<p$$

和

$$F(u)=0 \bmod p\Rightarrow F(u)=0 \bmod l_u.$$

因此 $F(u)\neq 0 \bmod l_u$ 蕴含 $F(u)\neq 0 \bmod p$，这样条件 $F(u)\neq 0 \bmod l_u$ 就足以保证 $\mathcal{D}$ 不会在私钥提取询问过程中退出.

签密询问. 在任意时刻，敌手可以发起对明文信息 m 和身份信息 u_A 与 u_B 的签密询问. 如果 u_A 是域 PKG_{i^*} 的用户且 $F(u_A)=0 \bmod l_u$，则 $\mathcal{D}$ 停止游戏；否则 $\mathcal{D}$ 首先调用私钥提取询问产生 u_A 对应的私钥，然后执行算法 $Signcrypt(m,d_A,ID_B)$ 应答敌手的询问.

解签密询问. 在任意时刻，敌手可以发起对签密密文 σ 和身份信息 u_A 与 u_B 的解签密询问. 如果 u_B 是域 PKG_{i^*} 的用户且 $F(u_B)=0 \bmod l_u$，则 $\mathcal{D}$ 停止游戏；否则，$\mathcal{D}$ 首先调用私钥提取询问产生 u_B 对应的私钥，然后执行算法 $\mathrm{Unsigncrypt}(\sigma,d_B,u_A)$ 应答敌手的询问.

挑战. 经过多项式轮数的询问后，敌手选择他想挑战的身份信息 u_A^* 和 u_B^*，注意到：敌手在第一阶段不能对 u_A^* 和 u_B^* 进行私钥提取询问. 接着敌手选择两条等长的明文消息 m_0 和 m_1，将其发送给挑战者 $\mathcal{D}$.

(1) 如果 u_A^* 不是域 PKG_{i^*} 的用户，$\mathcal{D}$ 停止游戏；

(2) 如果 u_A^* 是域 PKG_{i^*} 的用户，但是 $F(u_B^*)=0 \bmod l_u$，$\mathcal{D}$ 停止游戏；

(3) 如果 u_A^* 是域 PKG_{i^*} 的用户且满足 $F(u_B^*)=0 \bmod l_u$，$\mathcal{D}$ 选择随机比特 γ 和随机数 $r\in Z_p$，按下列方式构造 m_γ 对应的签密密文：

$\mathcal{D}$ 计算 $M=H_m(m_\gamma\|Z)$，令 $\mathcal{M}\subset\{1,2,\cdots,n_m\}$ 为 $M[i]=1$ 的位 i 的集合. 如果 $K(M)\neq 0 \bmod n_m$，则停止游戏. 否则设定签密密文为

$$\sigma^*=(m_\gamma\oplus H(Z),C,C^{J(u_B^*)},$$
$$P_{i^*}^{-\frac{J(u_A^*)}{F(u_B^*)}}(g_2^{F(u_A^*)}g^{J(u_A^*)})^{r_u}\cdot C^{L(M_\gamma)},P_{i^*}^{-\frac{1}{F(u_B^*)}}g^{r_u}).$$

当 $Z=e(g,g)^{abc}$，$C=g^c$ 时，这个模拟是完美的，这是因为

$$Z=e(g,g)^{abc}=e(g^a,g^b)^c=e(P_{i^*},g_2)^c,$$

$$C^{J(u_B^*)}=(g^{J(u_B^*)})^c=\left(u'\prod_{i\in\mathcal{U}_B^*}u_i\right)^c,$$

$$\begin{aligned}&P_{i^*}^{-\frac{J(u_A^*)}{F(u_B^*)}}(g_2^{F(u_A^*)}g^{J(u_B^*)})^{r_u}\cdot C^{L(M_\gamma)}\\&=P_{i^*}^{-\frac{J(u_A^*)}{F(u_B^*)}}(g_2^{F(u_A^*)}g^{J(u_B^*)})^{r_u}\cdot C^{L(M_\gamma)}\\&=g^{-a\cdot\frac{J(u_A^*)}{F(u_B^*)}}(g_2^{F(u_A^*)}g^{J(u_B^*)})^{r_u}\cdot C^{L(M_\gamma)}\\&=g_2^a(g_2^{F(u_A^*)}g^{J(u_B^*)})^{r_u-\frac{a}{F(u_A^*)}}\cdot\left(m'\prod_{i\in\mathcal{M}_\gamma}m_i\right)^c.\end{aligned}$$

第二阶段敌手可以进行和第一阶段相同的多项式次数询问，注意敌手不能发起对身份信息 u_B^* 的私钥提取询问和对挑战密文的解签密询问.

猜测. 在模拟的末尾,敌手输出对 γ 的猜测值 $\gamma' \in \{0,1\}$,如果 $\gamma'=\gamma$,$\mathcal{D}$ 返回 1 表示 $Z=e(g,g)^{abc}$;否则$\mathcal{D}$返回 0,作为 DBDH 问题的解.

成功的概率. 现在来计算$\mathcal{D}$成功的概率,为保证模拟顺利进行,在模拟过程中必须保证如下条件:

(1)对身份信息 u 的私钥提取询问,必须满足 u 是域 $PKG_x(x\neq i^*)$的用户或者 u 是域 PKG_{i^*} 的用户且 $F(u)\neq 0 \bmod l_u$;

(2)对消息 m 的发起签密询问,签密者的身份信息 u_A,必须满足 u_A是域 $PKG_x(x\neq i^*)$的用户或者 u_A是域 PKG_{i^*} 的用户且 $F(u_A)\neq 0 \bmod l_u$;

(3)对密文 σ 的解签密询问,解签密者的身份信息为 u_B,必须满足 u_B是域 $PKG_x(x\neq i^*)$的用户或者 u_B是域 PKG_{i^*} 的用户且 $F(u_B)\neq 0 \bmod l_u$;

(4)在挑战阶段,必须满足 u_A^* 是域 PKG_{i^*} 的用户且满足$F(u_A^*)\neq 0 \bmod p$,另外$K(M_\gamma)=0 \bmod p$,其中 $M_\gamma=H_m(m_\gamma \| Z)$.

令 $u_1,\cdots,u_{q_I}$ 为所有出现私钥提取询问中的身份信息,易得 $q_I\leq q_E+q_S+q_U$. 定义事件如下:

A_i 为 $F(u_i)\neq 0 \bmod l_u$;

A' 为 $F(u_B^*)\neq 0 \bmod p$;

B^* 为 $K(M_\gamma)=0 \bmod p$;

C 为 u 是域 PKG_{i^*} 中的用户.

这样,$\mathcal{D}$不会放弃模拟的概率可以表示为

$$Pr[\overline{\text{abort}}]\geq Pr[\bigwedge_{i=1}^{q_I}((C\wedge A_i)\vee\bar{C})\wedge C\wedge A'\wedge B^*].$$

首先,根据概率事件的分配率有

$$(C\wedge A_i)\vee\bar{C}=(C\vee\bar{C})\wedge(A_i\vee\bar{C})=(A_i\vee\bar{C}),$$

因此,

$$\begin{aligned}&Pr[\bigwedge_{i=1}^{q_I}((C\wedge A_i)\vee\bar{C})\wedge C\wedge A'\wedge B^*]\\=&Pr[\bigwedge_{i=1}^{q_I}(A_i\vee\bar{C})\wedge C\wedge A'\wedge B^*]\\=&Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A'\wedge B^*]\\=&Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A'\wedge B^*\wedge C].\end{aligned}$$

因为 i^* 是独立选择的,因此,事件 $\bigwedge_{i=1}^{q_I}A_i\wedge A'\wedge B^*$ 和 C 是相互独立的,因此,我们有

$$Pr[C]=\frac{1}{l}.$$

因为函数 F 和 K 是独立选择的,因此,事件 $\bigwedge_{i=1}^{q_I}A_i\wedge A'$ 和 B^* 是相互独立的,因为 k_u、x' 和 X 的随机性,有

$$\begin{aligned}Pr[A']=&Pr[F(u^*)=0 \bmod p]\\=&Pr[F(u^*)=0 \bmod l_u]\cdot\\&Pr[F(u^*)=0 \bmod p\,|\,F(u^*)=0 \bmod l_u]\\=&\frac{1}{l_u}\cdot\frac{1}{n_u+1};\end{aligned}$$

同理,$Pr[B^*]=\frac{1}{l_m}\cdot\frac{1}{n_m+1}$.

另一方面,对任意 i,事件 A_i 和 A' 均为独立的,因此有

$$\begin{aligned}Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A']=&Pr[\bigwedge_{i=1}^{q_I}A_i]Pr[A']\\=&(1-Pr[\overline{\bigwedge_{i=1}^{q_I}A_i}])Pr[A']\\=&(1-Pr[\bigvee_{i=1}^{q_I}\overline{A_i}])Pr[A']\\=&\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}\\\geq&\left(1-\frac{q_E+q_S+q_U}{2(q_E+q_S+q_U)}\right)\cdot\\&\frac{1}{2(q_E+q_S+q_U)}\cdot\frac{1}{n_u+1}\\=&\frac{1}{4(q_E+q_S+q_U)(n_u+1)}.\end{aligned}$$

最后,可以得到挑战者不放弃模拟的概率为

$$\begin{aligned}Pr[\overline{\text{abort}}]\geq&Pr[\bigwedge_{i=1}^{q_I}((C\wedge A_i)\vee\bar{C})\wedge C\wedge A'\wedge B^*]\\=&Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A'\wedge B^*\wedge C]\\\geq&\frac{1}{4(q_E+q_S+q_U)(n_u+1)}\cdot\frac{1}{l_m}\cdot\frac{1}{n_m+1}\cdot\frac{1}{l}\\=&\frac{1}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}.\end{aligned}$$

这样,如果模拟没有被放弃,敌手可以以 ε 的概率赢得定义 3 中的游戏,那么挑战者可以解决 DBDH 问题实例的概率就至少为

$$\frac{\varepsilon}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}.$$

因此,提出的多 PKG 环境下基于身份签密方案在自适应选择密文攻击下满足密文不可区分性. 定理 1 得证. 证毕.

定理 2. 在 CDH 困难问题假设下,提出的多 PKG 基于身份签密方案在自适应选择消息攻击下具有密文的存在性不可伪造性. 假设存在定义 2 中的敌手,在经过至多 q_E 次私钥提取询问,q_S 次签密询问以及 q_U 次解签密询问,可以以概率 ε 伪造密文,则存在一个挑战者,可以以

$$\frac{2q_S(n_m+1)+2(q_E+q_S+q_U)(n_u+1)-1}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}\varepsilon$$

的优势解决计算性 Diffie-Hellman 问题.

证明.　假设存在成功的 EUF-MPIDSC-CMA 敌手,则可以构造挑战者$\mathcal{C}$,将敌手作为子程序解决 CDH 困难问题的实例. 给定一个 CDH 困难问题实例:群 G,生成元 g,元素 g^a 和 g^b,$\mathcal{C}$的目标是输出 g^{ab}. $\mathcal{C}$首先如定理 1 中所示设定全局系统参数及域主密钥和域公钥,其中 $g_2=g^b$,PKG_{i^*} 的域公钥为 g^a. 在$\mathcal{C}$定义函数 $F(u)$,$J(u)$,$K(m)$和 $L(m)$后有

$$u'\prod_{i\in\mathcal{U}}u_i=g_2^{F(u)}g^{J(u)},\quad m'\prod_{j\in\mathcal{M}}m_j=g_2^{K(u)}g^{L(u)}.$$

敌手可以发起多项式次数的询问,包括私钥提取询问、签密询问和解签密询问,挑战者$\mathcal{C}$如定理 1 中方法回答询问. 如果$\mathcal{C}$没有放弃模拟,敌手返回一个对消息 m^* 的签密密文 σ^*,其中敌手对元组(m^*,u_A^*,u_B^*)没有询问过. $\mathcal{C}$可以解签密 σ^* 得到消息(m^*,R^*),计算 $M^*=H_m(m^*\|R^*)$,如果不同时满足下面的条件,$\mathcal{C}$放弃模拟:

(1) u_A^* 是域 PKG_{i^*} 中的用户;

(2) $F(u_A^*)=0 \bmod p$ 或者 $K(M^*)=0 \bmod p$.

否则$\mathcal{C}$计算并返回

$$\frac{\sigma_4^*}{(\sigma_5^*)^{J(u_A^*)}\cdot(\sigma_2^*)^{L(M^*)}}=\frac{P_{i^*}\left(u'\prod_{j\in\mathcal{U}_j}u_j\right)^{r_A}\cdot\left(m'\prod_{j\in\mathcal{M}^*}m_j\right)^{r_m}}{g^{r_A\cdot J(u_A^*)}\cdot g^{r_m\cdot L(M^*)}}=P_{i^*}=g^{ab}$$

作为 CDH 问题的解.

成功的概率. 现在来计算$\mathcal{D}$成功的概率,为保证模拟顺利进行,在模拟过程中必须保证如下条件:

(1) 对身份信息 u 的私钥提取询问,必须满足 u 是域 $PKG_x(x\neq i^*)$的用户或者 u 是域 PKG_{i^*} 的用户且 $F(u)\neq 0 \bmod l_u$;

(2) 对消息 m 的发起签密询问,签密者的身份信息 u,必须满足 u 是域 $PKG_x(x\neq i^*)$的用户或者 u 是域 PKG_{i^*} 的用户且 $F(u)\neq 0 \bmod l_u$;

(3) 对密文 σ 的解签密询问,解签密者的身份信息为 u_B,必须满足 u_B是域 $PKG_x(x\neq i^*)$的用户或者 u_B是域 PKG_{i^*} 的用户且 $F(u_B)\neq 0 \bmod l_u$;

(4) 在伪造阶段,必须满足 u_A^* 是域 PKG_{i^*} 的用户,$F(u_A^*)=0 \bmod p$ 或者 $K(M^*)=0 \bmod p$,其中 $M^*=H_m(m^*\|R^*)$.

令 $u_1,\cdots,u_{q_I}$ 为所有出现私钥提取询问中的身份信息,易得 $q_I\leq q_E+q_S+q_U$. 定义与定理 1 中相同的事件 A_i, A', B^* 及 C,这样,$\mathcal{D}$不会放弃模拟的概率可以表示为

$$\begin{aligned}
Pr[\overline{\text{abort}}]&\geq Pr[\bigwedge_{i=1}^{q_I}((C\wedge A_i)\vee\bar{C})\wedge C\wedge(A'\vee B^*)]\\
&=Pr[\bigwedge_{i=1}^{q_I}(A_i\vee\bar{C})\wedge C\wedge(A'\vee B^*)]\\
&=Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge(A'\vee B^*)]\\
&=Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A']+Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge B^*]-\\
&\quad Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A'\wedge B^*].
\end{aligned}$$

根据定理 1 中的分析,我们有

$$Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A']=\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}\cdot\frac{1}{l};$$

$$Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge B^*]=\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_m}\cdot\frac{1}{n_m+1}\cdot\frac{1}{l};$$

$$Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A'\wedge B^*]=\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}\cdot\frac{1}{l}\cdot\frac{1}{l_m}\cdot\frac{1}{n_m+1};$$

从而,

$$\begin{aligned}
Pr[\overline{\text{abort}}]&\geq Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A']+Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge B^*]-Pr[\bigwedge_{i=1}^{q_I}A_i\wedge C\wedge A'\wedge B^*]\\
&=\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}\cdot\frac{1}{l}+\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_m}\cdot\frac{1}{n_m+1}\cdot\frac{1}{l}-\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}\cdot\frac{1}{l}\cdot\frac{1}{l_m}\cdot\frac{1}{n_m+1}\\
&=\left(1-\frac{q_I}{l_u}\right)\cdot\frac{1}{l}\cdot\frac{l_m(n_m+1)+l_u(n_u+1)-1}{l_u(n_u+1)l_m(n_m+1)}\\
&\geq\left(1-\frac{q_E+q_S+q_U}{2(q_E+q_S+q_U)}\right)\cdot\frac{1}{l}\cdot\frac{2q_S(n_m+1)+2(q_E+q_S+q_U)(n_u+1)-1}{4q_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}\\
&=\frac{2q_S(n_m+1)+2(q_E+q_S+q_U)(n_u+1)-1}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}.
\end{aligned}$$

这样,如果模拟没有被放弃,敌手可以以 ε 的概率赢得定义 3 中的游戏,那么挑战者可以解决 CDH 问题实例的概率就至少为

$$\frac{2q_S(n_m+1)+2(q_E+q_S+q_U)(n_u+1)-1}{8lq_S(q_E+q_S+q_U)(n_u+1)(n_m+1)}\varepsilon.$$

因此,提出的多 PKG 环境下基于身份签密方案在自适应选择消息攻击下具有密文的存在性不可伪造性,定理 2 得证.　　证毕.

4.4 性能比较

本节我们将新方案与已有的签密方案进行性能比较,注意:我们仅比较需要在线计算的运算个数,可以预先计算的运算不予统计.首先,我们将新构造的多 PKG 环境下签密方案与已有的 RO 模型下的方案[12-13,15]进行性能比较,见表 1.从表 1 中可以看到,我们的方案在增加计算代价的基础上,实现了标准模型下的可证明安全.因此,新方案在安全性方面具有一定的优势.

表 1 多 PKG 环境下基于身份签密方案的性能比较

文献	计算代价			安全性	
	对运算	指数运算	点乘运算	CCA 安全	安全模型
Li 方案[12]	3	2	3	No	RO 模型
Li 方案[13]	3	1	4	No	RO 模型
闻方案[15]	3	2	3	Yes	RO 模型
本文方案	5	4	$2n_m+4$	Yes	标准模型

表 2 中我们对方案退化为单个 PKG 环境时与其他标准模型下基于身份的签密方案进行了比较,从中我们可以看到新方案实现了 CCA 安全和存在不可伪造性,在计算效率方面稍有优势.

表 2 单个 PKG 环境下基于身份签密方案的性能比较

文献	计算代价			安全性	
	对运算	指数运算	点乘运算	CCA 安全	不可伪造性
Yu 方案[8]	5	4	$2n_m+6$	No	No
Jin 方案[9]	5	4	$2n_m+6$	No	No
张方案[10]	5	8	$2n_m+8$	No	Yes
Li 方案[12]	5	7	$2n_m+9$	Yes	Yes
本文方案	5	4	$2n_m+4$	Yes	Yes

5 结束语

本文提出了一个有效的多 PKG 环境下基于身份签密方案,并在标准模型下对方案的 CCA2 安全和存在性不可伪造性进行了证明.特别的,当环境退化为单个 PKG 时,我们的方案也是安全有效的.下一步的工作是对各个 PKG 拥有不同系统参数签密方案进行深入研究.

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption)// Burton S, Kaliski Jr. Proceedings of the CRYPTO 1997. LCNS 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Malone-Lee J. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, July 2002. http://eprint.iacr.org/2002/098

[3] Boyen X. Multipurpose identity based signcryption: A Swiss army knife for identity based cryptography//Boneh D. Proceedings of the CRYPTO 2003. LCNS 2729. Berlin: Springer-Verlag, 2003: 383-399

[4] Chen L, Malone-Lee J. Improved identity-based signcryption//Vaudenay S. Proceedings of the PKC 2005. LCNS 3386, Berlin: Springer-Verlag, 2005: 362-379

[5] Barreto P, Libert B, McCullagh N et al. Efficient and provably-secure identity based signatures and signcryption from bilinear maps//Roy Bimal K. Proceedings of the ASIACRYPT 2005. LCNS 3788. Berlin: Springer-Verlag, 2005: 515-532

[6] Li Fa-Gen, Hu Yu-Pu, Li Gang. An efficient identity-based signcryption scheme. Chinese Journal of Computers, 2006, 29(9): 1641-1647(in Chinese)
(李发根, 胡予濮, 李刚. 一个高效的基于身份的签密方案. 计算机学报, 2006, 29(9): 1641-1647)

[7] Yu Y, Yang B, Sun Y et al. Identity based signcryption scheme without random oracles. Computer Standards & Interfaces, 2009, 31(1): 56-62

[8] Zhang B. Cryptanalysis of an identity based signcryption scheme without random oracles. Journal of Computational Information Systems, 2010, 6(6): 1923-1931

[9] Jin Z, Wen Q, Du H. An improved semantically-secure identity-based signcryption scheme in the standard model. Computers & Electrical Engineering, 2010, 36(3): 545-552

[10] Li Fa-Gen, Muhaya F, Zhang M et al. Efficient identity-based signcryption in the standard model//Boyen X, Chen X. Proceedings of the ProvSec 2011. LNCS 6980. Berlin: Springer-Verlag, 2011: 120-137

[11] Zhang Bo, Xu Qiu-Liang. Identity-based multi-signcryption scheme without random oracles. Chinese Journal of Computers, 2011, 33(1): 103-110(in Chinese)
(张波, 徐秋亮. 无随机预言机的基于身份多签密方案. 计算机学报, 2010, 33(1): 103-110)

[12] Li F, Hu Y, Zhang C. An identity-based signcryption scheme for multi-domain ad hoc networks//Katz J, Yung M. Proceedings of the ACNS 2007. Berlin: Springer-Verlag, 2007: 373-384

[13] Li F, Shirase M, Takagi T. Efficient multi-PKG ID-based signcryption for Ad hoc networks//Yung M, Liu P, Lin D. Proceedings of the INSCRYPT 2008. LNCS 5487. Berlin: Springer-Verlag, 2008: 289-304

[14] Zhang J, Zou J. On the security of some Multi-PKG/Multi-Recipient signcryption schemes//Proceedings of the 3rd 2009 International Conference on Anti-Counterfeiting, Security, and Identification in Communication (ASID 2009). Hong Kong, China, 2009: 497-500

[15] Wen Ying-You, Luo Ming, Zhao Hong. Research and implementation of a signcryption-base security mechanism in VoIP network. Journal of Communications. 2010, 31(4): 8-15(in Chinese)
(闻英友, 罗铭, 赵宏. VoIP 网络基于签密的安全机制的研究与实现. 通信学报, 2010, 31(4): 8-15)

[16] Waters R. Efficient identity based encryption without random oracles//Cramer R. Proceedings of the EUROCRYPT 2005. LNCS 3494. Berlin: Springer-Verlag, 2005: 114-127

ZHAO Xiu-Feng, born in 1977, Ph. D. candidate, lecturer. Her current research interests focus on provably secure public key cryptology algorithm, the analysis and design of authenticated and key agreement protocols.

XU Qiu-Liang, born in 1960, Ph. D., professor, Ph. D. supervisor. His main research interests include secure multi-party computation, digital signature and identity-based cryptosystem.

Background

The concept of identity-based cryptography was first proposed by Shamir in 1984. Since Boneh and Franklin gave a practical IBE scheme from Weil pairing in 2001, a lot of researches have been done in this area. Signcryption, first proposed by Zheng in 1997, is a cryptographic primitive that combines the functionality of a public key encryption scheme with that of a digital signature scheme. The first ID-Based signcryption (IBSC) scheme was proposed by Malone-Lee. Subsequently, a number of secure and efficient IBSC schemes were proposed.

As the development of cloud computation and grid computation, the authentication and confident communication cross-domain has become an important research issue. ID-based signcryption with multiple private key generators is very suitable to provide security solution for such ad hoc networks. Several identity-based signcryption with multiaple PKGs schemes are proved security in random oracle model, the security of the schemes was proven secure in the random oracle. However, it has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure. Therefore, it is necessary to construct a secure ID-base signcrytion with multi-PKG scheme without random oracles.

In this paper, we proposed a new identity-based signcryption scheme with multiple PKG, which achieve provable semantic security and existential unforgeability without using random oracles. This research is supported by the National Natural Science Foundation of China under Grant No. 61173139, the Natural Science Foundation Key Project of Shandong Province under Grant No. ZR2011FZ005, and the Doctoral Fund of Ministry of Education under Grant No. 20110131110027. These projects focus on the study of foundational problems in multi-party secure computation, UC security and cross-domain authentication technology based on the public key cryptology. Our research team produces a lot of good work in this area, such as, multiparty computation protocol for modulo reduction problem, identity-based multi-signcryption scheme without random oracles, provably secure anonymous HIBE scheme, extractable concurrent ZK protocol, and so on.