一种新的无双线性对的无证书安全签密方案

夏 昂, 张龙军
(武警工程大学 信息工程系, 西安 710086)

摘 要: 针对现有的无证书签密方案存在安全性不高、计算效率较低等诸多不足,在 Sharmila 签密方案的基础上,设计了一种新的无双线性对的无证书安全签密方案,并在随机预言模型下证明了方案具有机密性和不可伪造性。同时,该方案不需要双线性对和指数运算,并且在确保安全性的前提下,仅比现有的最高效签密方案多出两次点乘运算。

关键词: 无证书; 签密; 安全性; 随机预言模型
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2014)02-0532-04
doi:10.3969/j.issn.1001-3695.2014.02.050

New secure cetificateless signcryption scheme without pairing

XIA Ang, ZHANG Long-jun
(*Dept. of Information Engineering, Engineering University of CAPF, Xi'an* 710086, *China*)

Abstract: The known certificateless signcryption schemes have many problems, for example, lack of security, low computational cost and so on. This paper proposed a new secure certificateless signcryption scheme without pairings, which was based on Sharmila's. And it was provably secure in the random oracle model (ROM). The proposed scheme did no use of pairing and exponentation. And compared with the most efficient scheme, the proposed one just needs 2 more point multiplications under the secure circumstance.

Key words: certificateless; signcryption; security; random oracle model

签密的最大优势就是将加密和认证结合,在一个逻辑步骤里同时实现了信息的机密性和不可否认性,并且与传统的"先签名后加密"方式相比较具有更低的通信开销和更少的计算量。1997 年,Zheng[1] 首次提出了签密的思想,并给出了相关的安全概念和第一个签密的方案[2]。针对 CB-PKC(certificate-based public key cryptography)中证书管理繁琐以及 IB-PKC (identity-based public key cryptography)的秘钥托管问题,Al-Riyami 等人[3] 于 2003 年首次提出了无证书公钥密码体制(certificateless public key cryptography, CL-PKG)。此后,不少学者对无证书签密进行了相关研究。

2008 年,Barbosa 等人[4] 第一次提出了无证书签密方案和给出了第一个无证书签密安全模型,但该方案存在可扩展伪造的安全问题;Wu 等人[5] 提出了一个新的有效无证书签密方案,该方案有公开验证性和更高的效率,但被文献[6]指出不具有机密性和认证性;Aranha 等人[7] 提出了一个高效的无证书签密方案,但被文献[6]指出不具有机密性和不可抗伪造性。上述方案都是利用双线性对构造实现的,比起只使用指数运算和点乘运算的计算量过大。因此,Barreto 等人[8] 提出了一种签密和解签密均不需要双线性对的无证书签密方案,但在公钥生成时却利用了双线性对运算。Sharmila 等人[6] 首次提出了一种不需要双线性对的无证书签密方案,并在随机预言模型下证明了其安全性。但该方案在签密和解签密过程中运用到了 12 次指数运算,运算效率不高。2009 年,Li 等人[9] 利用 KEM(key encapsulation mechanism)构造了一种无证书混合签密方案,但该方案运算量非常大。2011 年,刘文浩等人[10] 提出了一个无双线性对的无证书签密方案,该方案计算复杂度较低,但该方案无法抵抗来自内部人员的攻击,存在用户长期密钥泄露的安全问题。从以上分析可以得出,现有的无证书签密方案存在诸多不足:方案保证了安全性却运用到了对运算和指数运算,造成运算效率不高;方案提高了运算效率却不能保证方案的安全性。本文在文献[6]签密方案的基础上,设计了一种无双线性对的无证书安全签密方案,并在基于 CDH 问题的随机预言模型下证明了方案具有机密性和不可伪造性,从性能分析得出方案效率较为理想。

1 无证书签密的安全定义

通常一个无证书签密方案可分为六个概率多项式时间算法,即是建立系统参数(setup)、部分密钥提取(extract-partial-key)、用户公钥提取 (extract-pulic-key)、用户私钥提取(extract-private-key)、签密(signcrypt)和解签密(unsigncrypt),方案算法的细节参照文献[4]。根据文献[6],任何一个无证书签密方案都面临 Type-I 和 Type-II 两种不同的攻击。Type-I 攻击是敌手 A_1 不能获得 KGC 的秘密值,即系统主密钥 master key,但被允许替换任意用户的公钥或查询用户的公钥;Type-II 攻击是敌手 A_2 不能替换任意用户的公钥或查询用户的公钥,但可以获得 KGC 系统主密钥 master key。

定义 1 机密性。在任意概率多项式时间内,敌手 A_1 和敌手 A_2 赢得游戏的概率是可忽略的,则称该无证书签密方案

收稿日期: 2013-02-17; **修回日期**: 2013-04-16

作者简介:夏昂(1989-),男,硕士研究生,主要研究方向为信息与网络安全(935592289@qq.com);张龙军(1964-),男,教授,博士(后),主要研究方向为信息与网络安全.

在适应性选择密文攻击下具有机密性。

1)游戏 IND-CLSC-CCA2-I

初始化:输入安全参数 k,挑战者 C 利用建立系统参数算法计算系统参数 params 和系统主密钥 master key,保留 master key 并将 params 发送给敌手 A_1。

敌手 A_1 进行询问和猜测两个游戏阶段。

询问阶段,A_1 执行以下操作:

a)Hash 函数询问。A_1 可以询问键入的任意 hash 函数值。

b)部分密钥提取询问。根据 A_1 选择的用户 ID,C 计算用户的部分密钥 d_{ID}并发送给 A_1。

c)公钥提取询问。根据 A_1 选择的用户 ID,C 计算用户的公钥 PK_{ID}并发送给 A_1。

d)私钥提取询问。根据 A_1 选择的用户 ID,C 计算用户的私钥 sk_{ID}并发送给 A_1。

e)替换公钥询问。对于所有的用户 ID,A_1 任意选择并在重新选取秘密值后计算相应公钥 PK'_{ID},最后将用户 ID 的原有公钥 PK_{ID}替换为新公钥 PK'_{ID}。

f)签密询问。根据 A_1 选择的发送者 ID_s、接收者 ID_r 以及明文 m,C 进行计算并将 $\sigma=\mathrm{Signcrpt}(sk_{\mathrm{ID}_s},PK_{\mathrm{ID}_r},m)$ 返回给 A_1。此时,C 返回的公钥 PK_{ID_s}是发送者 ID_s 的原有公钥,但是 A_1 已将发送者 ID_s 的公钥替换为新公钥 $PK_{\mathrm{ID}_a}{}'$。

g)解签密询问。根据 A_1 选择的发送者 ID_s、接收者 ID_r 以及密文 σ,C 进行 $\mathrm{Unsigncrypt}(sk_{\mathrm{ID}_r},PK_{\mathrm{ID}_s},\sigma)$ 计算并将结果值返回给 A_1。

h)挑战。A_1 根据想要挑战的两个用户的身份$\langle \mathrm{ID}_s^*,\mathrm{ID}_r^*\rangle$生成两个等长的明文$\langle m_0,m_1\rangle$,同时 A_1 没有对 ID_r^* 进行部分密钥 $d_{\mathrm{ID}_r}^*$和私钥 $s_{\mathrm{ID}_r}^*$的询问。挑战者 C 随机选取 $\alpha\in\{0,1\}$,计算 $\sigma^*=\mathrm{Signcrypt}(sk_{\mathrm{ID}_s}^*,PK_{\mathrm{ID}_r}^*,m_\alpha)$并发送给 A_1。

i)猜测阶段。在概率多项式时间内和不允许对 ID_r^* 进行过部分密钥 $d_{\mathrm{ID}_r}^*$和私钥 $s_{\mathrm{ID}_r}^*$询问的约束条件下,A_1 仍像询问阶段一样执行适应性询问。最后,A_1 对 α 进行结果为 α'的猜测,如果 $\alpha'=\alpha$,A_1 赢得游戏。A_1 赢得游戏的概率为

$$\mathrm{Adv}_{A_1}^{\mathrm{IND-CLSC-CCA2-I}}=|2Pr[\alpha'=\alpha]-1|$$

2)游戏 IND-CLSC-CCA2-Ⅱ

初始化。输入安全参数 k,挑战者 C 利用建立系统参数算法计算系统参数 params 和系统主密钥 master key,保留 master key 并将 params 发送给敌手 A_2。

敌手 A_2 进行询问和猜测两个游戏阶段:

a)询问阶段。敌手 A_2 进行像游戏 IND-CLSC-CCA2-Ⅰ一样的多项式有界询问,但是 A_2 不能对任意用户进行公钥替换询问。

b)猜测阶段。在概率多项式时间内和不允许对 ID_r^* 进行私钥 $s_{\mathrm{ID}_r}^*$及解签密询问的约束条件下,A_2 仍像询问阶段一样执行适应性询问。最后,A_2 对 α 进行结果为 α'的猜测,如果$\alpha'=\alpha$,A_2 赢得游戏。A_2 赢得游戏的概率为

$$\mathrm{Adv}_{A_2}^{\mathrm{IND-CLSC-CCA2-Ⅱ}}=|2Pr[\alpha'=\alpha]-1|$$

定义 2　不可伪造性。在任意概率多项式时间内,敌手 A_1 和 A_2 赢得游戏的概率是可忽略的,则称该无证书签密方案在适应性选择消息攻击下具有不可伪造性。

1)游戏 EUF-CLSC-CMA-I

与定义 1 中的询问阶段相同。

伪造阶段。A_1 自己输出(而不是签密预言机产生)一个新的三元组$\langle \mathrm{ID}_s^*,\mathrm{ID}_r^*,\sigma^*\rangle$,那么在不允许对用户进行部分密钥 d_{ID}和私钥 sk_{ID}询问的约束条件下,A_1 解签密的结果正确,则赢得游戏。

2)游戏 EUF-CLSC-CMA-Ⅱ:

初始化。输入安全参数 k,挑战者 C 利用建立系统参数算法计算系统参数 params 和系统主密钥 master key,保留 master key 并将 params 发送给敌手 A_2。

敌手 A_2 进行询问和伪造两个游戏阶段:

a)询问阶段。A_2 进行像游戏 IND-CLSC-CCA2-Ⅱ一样的多项式有界询问。

b)伪造阶段。A_2 自己输出(而不是签密预言机产生)一个新的三元组$\langle \mathrm{ID}_s^*,\mathrm{ID}_r^*,\sigma^*\rangle$,那么在不允许对用户进行部分密钥 d_{ID}和私钥 sk_{ID}询问的约束条件下,A_2 解签密的结果正确,则赢得游戏。

2　Sharmila 签密方案

Sharmila[6] 签密方案主要由七个算法组成,具体如下:

a)系统参数建立。输入安全参数 1^k,随机选择两个大素数 p、q,且 $q|p-1$。选择一个阶为 q 的数 $g\in_R Z_p^*$ 和主密钥 s,计算系统公钥 $g_{\mathrm{pub}}=g^s$,定义五个安全 hash 函数:$H_1:\{0,1\}^*\to Z_q^*$,$H_2:\{0,1\}^*\times Z_p^*\times Z_p^*\to Z_q^*$,$H_3:\{0,1\}^*\to Z_q^*$,$H_4:\{0,1\}^*\to|M|\times Z_q^*\times Z_q^*$,$H_5:\{0,1\}^*\to Z_q^*$,其中 M 为消息长度,公开系统参数$\langle p,q,P,g,H_1,H_2,H_3\rangle$。

b)生成部分私钥。给定用户 U_A 身份 ID_A,KGC 随机选取 $x_{A0},x_{A1}\in_R Z_q^*$,计算 $X_{A0}=g^{x_{A0}}$,$X_{A1}=g^{x_{A1}}$,$q_{A0}=H_1(\mathrm{ID}_A,X_{A0})$,$q_{A0}=H_1(\mathrm{ID}_A,X_{A0})$,$q_{A1}=H_2(\mathrm{ID}_A,X_{A0},X_{A1})$,$d_{A0}=x_{A0}+sq_{A0}$,$d_{A1}=x_{A1}+sq_{A1}$,并将 $d_{A1}=\langle d_{A0},d_{A1}\rangle$ 和 $X_{A1}=\langle X_{A0},X_{A1}\rangle$ 发送给用户 U_A。

c)选取秘密值。用户 U_A 随机选择并保存秘密值 $y_A\in_R Z_q^*$。

d)生成用户私钥。用户 U_A 生成私钥 $s_A=\langle y_A,d_{A0}\rangle$。

e)生成用户公钥。用户 U_A 计算 $Y_A=g^{y_A}$并将 $PK_A=\langle d_{A1},X_{A0},X_{A1},Y_A\rangle$作为公钥。

f)签密。用户 U_A 随机选择 $r_1,r_2\in_R Z_q^*$,计算 $c_1=g^{r1}$,$c_2=g^{r2}$,$k_1=(Y_B)^{r1}$,$k_2=(X_{B0}\cdot(g_{\mathrm{pub}})^{q_{B0}})^{r2}$,$d=H_3(m,c_2,\mathrm{ID}_A,\mathrm{ID}_B,PK_A)$,$e=H_5(m,c_2,\mathrm{ID}_A,\mathrm{ID}_B,PK_A)$,$v=(d\cdot d_{A0}+e\cdot y_A)+r_2$,$c_3=H_4(k_1,k_2,\mathrm{ID}_A,\mathrm{ID}_B)\oplus(m\|r_1\|v)$,并将签密信息 $c=\langle c_1,c_2,c_3\rangle$发送给用户 U_B。

g)解签密。用户 U_B 计算 $k_1'=(c_1)^{y_B}$,$k_2'=(c_1)^{d_{B0}}$,$(m'\|r_1'\|v')=c\oplus H_4(k_1',k_2',\mathrm{ID}_A,\mathrm{ID}_B)$。若 $g^{r'1}=c_1$,则计算$d'=H_3(m',c_2,\mathrm{ID}_A,\mathrm{ID}_B,PK_A)$,$e'=H_5(m',c_2,\mathrm{ID}_A,\mathrm{ID}_B,PK_A)$;若$g^{v'}=((g_{\mathrm{pub}})^{q_{A0}}\cdot X_{A0})^{d'}\cdot(Y_A)^{e'}\cdot c_2$ 成立,则解签密消息为 m',否则拒绝。

考虑到方案的计算复杂性,文献[6]签密方案计算过于复杂,在签密和解签密过程中运用到了 12 次指数运算,运算效率不高。因此,本文在文献[6]签密方案基础上提出一个计算开销较小的新的安全签密方案。

3　新方案描述

a)初始化:

(a)输入安全参数 k,生成两个大素数 p、q,且 $q|p-1$。设

P 为任意阶 q 为循环群 G 的生成元,定义安全 hash 函数:$H_1:\{0,1\}^* \rightarrow Z_q^*$,$H_2:\{0,1\}^* \rightarrow \{0,1\}^n$,$H_3:\{0,1\}^* \times G \rightarrow Z_q^*$,其中 n 为消息 m 的比特长度。KGC(key generation centre)随机选取系统主密钥 $s \in Z_q^*$ 并保存,计算系统公钥 $g = sP$,公开系统参数$\langle p,q,P,g,H_1,H_2,H_3\rangle$。

(b)生成用户部分密钥。给定用户 U_A 身份 ID_A,KGC 随机选取 $x_A \in Z_q^*$,计算 $X_A = x_A P$,$Q_A = H_1(ID_A, X_A)$,$d_A = x_A + s \cdot Q_A$,并将$\langle d_A, X_A\rangle$发送给用户 U_A,d_A 作为 U_A 的部分私钥,X_A 作为 U_A 的部分公钥。

(c)生成用户密钥。U_A 随机选取 $y_A, z_A \in Z_q^*$,计算 $Y_A = z_A P$。则 U_A 生成的私钥为$\langle d_A, y_A\rangle$,公钥为$\langle X_A, Y_A\rangle$。

用户 U_A 可通过判断等式 $X_A + gH_1(ID_A, X_A) = d_A P$ 来检验 KGC 生成的部分密钥。

b)签密。用户 U_A 将消息 m 进行签密发送给用户 U_B,具体过程如下:

(a)U_A 随机选取 $r \in Z_q^*$,计算 $R = r \cdot y_A \cdot Y_B$。

(b)计算 $W = Y_B \cdot (d_A + H_2(ID_A, ID_B))$。

(c)计算 $t = \frac{r}{x_A} \cdot y_A$,$\sigma = H_3(W, ID_A) \oplus (m \| R \| t)$,发送 σ 给用户 U_B。

c)解签密。用户 U_B 接收到 σ 后,具体过程如下:

(a)计算 $W' = z_B \cdot (X_A + gH_1(ID_A, X_A) + PH_2(ID_A, ID_B))$。

(b)计算 $m = H_3(W', ID_A) \oplus \sigma$,得到 t、R。

(c)计算 $t \cdot z_B \cdot X_A = R$。若等式成立,用户 U_B 接收消息 m,否则拒绝。

4 新方案证明

4.1 正确性证明

方案的正确性基于以下两个等式正确性的证明:

$$W' = z_B \cdot (x_A P + sH_1(ID_A, X_A)P + H_2(ID_A, ID_B)P) = z_B P(x_A + sQ_A + H_2(ID_A, ID_B)) = W \quad (1)$$

$$t \cdot z_B \cdot X_A = \frac{r}{x_A} \cdot z_B \cdot X_A = r \cdot z_B \cdot y_A \cdot P = r \cdot y_A \cdot Y_B \quad (2)$$

4.2 安全性证明

本文提出的方案是在 ROM 下,基于离散对数问题(discrete logarithm problem, DLP)和计算性 Diffie-Hellman(computational diffie-hellman, CDH)假设证明了方案具有机密性和不可伪造性。根据文献[6,11],任何一个无证书签密方案都面临 Type-Ⅰ和 Type-Ⅱ两种不同的攻击。Type-Ⅰ攻击是敌手 A_1 不能获得 KGC 的秘密值,即系统主密钥 master key,但被允许替换任意用户的公钥或查询用户的公钥;Type-Ⅱ攻击是敌手 A_2 不能替换任意用户的公钥或查询用户的公钥,但可以获得 KGC 系统主密钥 master key。具体证明过程如下:

1)机密性

定义 3 Type-Ⅰ攻击下的机密性。在 ROM 中,如果在概率多项式时间内存在一个敌手 A_1 以 ε 的优势赢得游戏 IND-CLSC-CCA2-Ⅰ,则存在一个区分者 C 在概率多项式时间内以优势 $Succ_{A_1}^{CDH} \geqslant (\varepsilon / q_1^2 q_2 q_3)(1 - q_s / 2^k)$ 解决 CDH 困难问题。

证明 区分者 C 接受一个随机 CDH 问题(P, aP, bP),目标是计算出 abP。令 $g = cP$。C 扮演游戏 IND-CLSC-CCA2-Ⅰ中的挑战者,A_1 作为 C 的子程序。游戏中,C 维护$\langle L_1, L_2, L_3, L_P, L_{PK}, L_{sk}, L_s, L_u\rangle$八张列表,设表开始均为空表,这些表分别用于记录 A_1 对预言机 H_1、H_2、H_3、部分密钥提取、公钥提取、私钥提取、签密和解签密的询问。在游戏初始化阶段,C 发送系统参数$\langle p,q,P,g,H_1,H_2,H_3\rangle$给 A_1,然后 A_1 开始询问:

a)H_1 询问。假设 A_1 不会作重复询问,C 从$\langle 1,2,\cdots,q_1\rangle$中随机选取一个数 c_j,A_1 对用户 ID_u 进行 H_1 询问,若 $u \neq j$,C 随机选取 $h_1 \in Z_q^*$,将$\langle ID_u, X_u, h_1\rangle$保存至表 L_1 中并返回 h_1 值;否则,令 $h_1 = v$,将 v 返回给 A_1。

b)H_2 询问。A_1 询问$\langle ID_u, h_2\rangle$,C 查找表 L_2 将存在的相应值返回给 A_1;否则,C 随机选取 $h_2 \in \{0,1\}^n$,将其保存至表 L_2 中并返回 h_2 值。

c)H_3 询问。A_1 询问$\langle ID_u, W, h_3\rangle$,$C$ 查找表 L_3 将存在的相应值返回给 A_1;否则,C 随机选取 $h_3 \in Z_q^*$,将其保存至表 L_3 中并返回 h_3 值。

d)部分密钥提取询问。A_1 询问$\langle ID_u, d_u, X_u\rangle$,若 $ID_u = ID_j$,则终止模拟;否则,C 查找表 L_P 将存在的相应值返回给 A_1;若不存在,则从表 L_1 中提取 h_1,计算 $X_u = d_u P - gh_1$,将$\langle ID_u, d_u, X_u\rangle$保存至表 L_P 中并返回$\langle d_u, X_u\rangle$给 A_1。

e)公钥提取询问。A_1 询问$\langle ID_u, X_u, Y_u\rangle$,$C$ 查找表 L_{PK}将存在的相应值返回给 A_1,若不存在,C 随机选取 $x_u, z_u \in Z_q^*$,计算 $X_u = x_u P$,$Y_u = z_u P$,将$\langle ID_u, X_u, Y_u, x_u, z_u\rangle$保存至表 L_{PK}中并返回$\langle X_u, Y_u\rangle$给 A_1。

f)私钥提取询问。A_1 询问$\langle ID_u, d_u, y_u\rangle$,若 $ID_u = ID_j$,则终止模拟;否则,C 查找表 L_{sk}将存在的相应值返回给 A_1,若不存在,则 C 查找表 L_P 提取 d_u,随机选取 $y_u \in Z_q^*$,将$\langle ID_u, d_u, y_u\rangle$保存至表 L_{sk}中并返回$\langle d_u, y_u\rangle$给 A_1;若表 L_P 中不存在,则先进行 H_1 询问。

g)公钥替换。A_1 随机选取一个新值 x'_u,并计算 X'_u,将原来的公钥 X_u 替换为新公钥 X'_u。

h)签密询问。A_1 对 ID_A 和 ID_B 以及消息 m 进行签密询问,若 $ID_A = ID_j$,则 C 可根据知道的用户 ID_A 的私钥 d_A 和 y_A 进行签密计算,否则终止模拟;若 $ID_A \neq ID_j$,C 查找表 L_{PK}中的$\langle ID_B, X_B, Y_B\rangle$和表 L_{sk}中的$\langle ID_A, d_A, y_A\rangle$,按照前面所提出的签密算法对 m 进行签密,并将 σ 返回给 A_1。

i)解签密询问。A_1 询问$\langle ID_A, ID_B, \sigma, m\rangle$,若 $ID_B \neq ID_j$,C 查找表L_{sk}中的$\langle ID_B, d_B, y_B\rangle$和表 L_1 中的$\langle ID_A, X_A, h_1\rangle$,计算$W' = z_B(X_A + gh_1 + PH_2(ID_A, ID_B))$,$m = H_3(W', ID_A) \oplus c$,若 $t \cdot z_B \cdot X_A = R$ 成立,则返回 m,否则终止模拟;若 $ID_B = ID_j$,则终止模拟。

询问阶段结束后,A_1 输出想要挑战的两个用户的身份$\langle ID_A^*, ID_B^*\rangle$和两个等长明文$\langle m_0, m_1\rangle$,若 $ID_B^* \neq ID_j$ 则终止模拟;否则 C 掷一枚硬币 $\alpha \in \{0,1\}$,随机选取 $r^*, h^* \in Z_q^*$,计算 $R^* = r^* \cdot y_A \cdot Y_B$,$W^* = Y_B(d_A + h^*)$,$t^* = \frac{r^*}{x_A} \cdot y_A$,$c^* = H_3(W^*, ID_A) \oplus (m_\alpha \| t^* \| R^*)$,将 σ^* 发送给 A_1,其中 C 知道公钥被替换的信息。

A_1 在猜测阶段仍像阶段一样进行多项式有界询问,若 A_1 进行了签密询问,则终止模拟。最后 A_1 对 α 进行结果为 α'的猜测,若 $\alpha = \alpha'$,则 C 输出 $z_B \cdot (X'_A + gQ_A + h^* - (X'_A + h^*)) \cdot (1/v) = z_B cP = abP$ 作为 CDH 问题的答案,否则没有解决 CDH 问题。

如果在 A_1 询问阶段对 ID_j 进行过部分密钥询问或私钥询问,对 H_2 进行过询问,对 W'进行过 H_3 询问,则 C 失败。而 A_1

没有分别进行 H_1、H_2、H_3 询问的概率为 $1/q_1^2$、$1/q_2$、$1/q_3$,在解签密询问中,C 拒绝一个有效的密文信息的概率为 $q_s/2^k$,因此,C 成功解决 CDH 问题的概率为 $\mathrm{Succ}_{A_1}^{\mathrm{CDH}} \geqslant (\varepsilon/q_1^2 q_2 q_3)(1-q_s/2^k)$。证毕。

定义 4　Type-Ⅱ攻击下的机密性。在 ROM 中,如果在概率多项式时间内存在一个敌手 A_2 以 ε 的优势赢得游戏 IND-CLSC-CCA2-Ⅱ,则存在一个区分者 C 在概率多项式时间内以优势 $\mathrm{Succ}_{A_2}^{\mathrm{DLP}} \geqslant \varepsilon/(q_1^2 q_2 q_3)$ 解决 DL 困难问题。

证明　区分者 ε 接受一个随机 DL 问题实例 (P, aP),目标是计算出 a。C 扮演游戏 IND-CLSC-CCA2-Ⅱ中的挑战者,A_2 作为 C 的子程序。游戏初始化阶段,发送主密钥 s 和系统参数 $\langle p, q, P, g, H_1, H_2, H_3\rangle$ 给 A_2,其他建立过程同定义 1。因此,A_2 知道系统主密钥 s,但不能进行公钥替换。

a)询问阶段。A_2 进行同定义 1 一样的询问,但是 A_2 不能替换用户 ID_u 的公钥。

b)解签密询问。A_2 对 $\langle \mathrm{ID}_A, \mathrm{ID}_B, \sigma, m\rangle$ 进行询问,若 $\mathrm{ID}_B \neq \mathrm{ID}_j$,$C$ 查找表 L_{sk} 中的 $\langle \mathrm{ID}_B, d_B, y_B\rangle$ 和表 L_1 中的 $\langle \mathrm{ID}_A, X_A, h_1\rangle$,计算 $W' = z_B(X_A + sh_1 P + PH_2(\mathrm{ID}_A, \mathrm{ID}_B))$,$m = H_3(W', \mathrm{ID}_A) \oplus c$,若 $t \cdot z_B \cdot X_A = R$ 成立,则返回 m,否则终止模拟;若 $\mathrm{ID}_B = \mathrm{ID}_j$,则终止模拟。

询问阶段结束后,A_2 输出想要挑战的两个用户的身份 $\langle \mathrm{ID}_A^*, \mathrm{ID}_B^*\rangle$ 和两个等长明文 $\langle m_0, m_1\rangle$,若 $\mathrm{ID}_B^* \neq \mathrm{ID}_j$ 则终止模拟;否则 C 掷一枚硬币 $\alpha \in \{0,1\}$,随机选取 $r^*, h^* \in Z_q^*$,计算 $R^* = r^* \cdot y_A \cdot Y_B$,$W^* = Y_B(d_A + h^*)$,$t^* = \dfrac{r^*}{x_A} \cdot y_A$,$c^* = H_3(W^*, \mathrm{ID}_A) \oplus (m_\alpha \| t^* \| R^*)$,将 σ^* 发送给 A_2,其中 C 知道系统主密钥 s。

A_2 在猜测阶段仍像阶段一样进行多项式有界询问。最后 A_2 对 α 进行结果为 α' 的猜测,若 $\alpha = \alpha'$,则 C 输出 $z_B = a = z_B \cdot (X_A' + sQ_A P + h^* - (X_A' + h^*)) \cdot (1/v \cdot g)$ 作为 DL 问题的答案,否则没有解决 DL 问题。

如果在 A_2 询问阶段对 ID_j 进行过部分密钥询问或私钥询问,对 H_2 进行过询问,对 W' 进行过 H_3 询问,则 C 失败。而 A_2 没有分别进行 H_1、H_2、H_3 询问的概率为 $1/q_1^2$、$1/q_2$、$1/q_3$,因此,C 成功解决 CDH 问题的概率为 $\mathrm{Succ}_{A_1}^{\mathrm{CDH}} \geqslant (\varepsilon/q_1^2 q_2 q_3)(1-q_s/2^k)$。证毕。

2)不可伪造性

如果一个敌手能够伪造本文提出的签密方案,那么它也能伪造文献[6]中的方案。但是文献[6]已证明了方案具有不可伪造性,因此,本文提出的方案具有在适应性选择密文攻击下的不可伪造性。

5　新方案性能分析

本文提出方案在初始化阶段有三次 hash 运算,分别为:$H_1: \{0,1\}^* \to Z_q^*$,$H_2: \{0,1\}^* \to \{0,1\}^n$,$H_3: \{0,1\}^* \times G \to Z_q^*$;有 14 次点乘运算,在初始化阶段的系统公钥计算 $g = sP$,私钥 $\langle d_A, y_A\rangle$ 和公钥 $\langle X_A, Y_A\rangle$ 的生成,$X_A = x_A P$,$Q_A = H_1(\mathrm{ID}_A, X_A)$,$d_A = x_A + s \cdot Q_A$,$Y_A = z_A P$,签密时的 $R = r \cdot y_A \cdot Y_B$,$W = Y_B \cdot (d_A + H_2(\mathrm{ID}_A, \mathrm{ID}_B))$ 和 $t = \dfrac{r}{x_A} \cdot y_A$,解签密时的 $W' = z_B \cdot (X_A + gH_1(\mathrm{ID}_A, X_A) + PH_2(\mathrm{ID}_A, \mathrm{ID}_B))$ 和 $t \cdot z_B \cdot X_A = R$。此外,本文的方案不需要 $\hat{e}$ 双线性对运算和指数运算 EXP。

表 1 为本文提出的方案同其他已有方案的性能比较。表中的 hash 代表方案的 hash 运算,$\hat{e}$ 代表双线性对运算,EXP 代表指数运算,MUL 代表点乘运算。通过比较可以发现,本文提出的方案不需要双线性对和指数的运算,同时在确保了方案安全性的前提下,仅比现有方案中最高效方案[10]需要多出两次的点乘运算,因此方案在运算效率方面较为理想。

表 1　性能分析

方　案	hash	$\hat{e}$	EXP	MUL	方　案	hash	$\hat{e}$	EXP	MUL
文献[4]	4	6	1	7	文献[6]	5	0	16	8
文献[5]	3	5	9	6	文献[10]	3	0	0	12
文献[7]	3	4	1	10	本　文	3	0	0	14
文献[8]	4	2	8	8					

6　结束语

本文基于 Sharmila[6] 签密方案,提出了一种新的签密方案。在安全性方面,通过随机预言机模型证明了该方案具有在适应性选择密文攻击下的机密性和不可伪造性;在计算复杂性方面,通过与其他现有签密方案的比较和分析,本文方案不需要双线性对和指数运算,并且在确保安全性的前提下,仅比现有的最高效签密方案[10]多出 2 次点乘运算。因此,本文在安全性和效率方面均较为理想,是一种高效安全的签密方案。

参考文献:

[1] ZHENG Yu-liang. Digital signcryption or how to achieve cost (signature&encryption) << cost (signature) + cost (encryption) [C]//LNCS, vol 1294. Berlin: Springer-Verlag, 1997: 165-179.

[2] ZHENG Yu-liang. Signcryption and its applications in efficient public key solutions[C]// LNCS, vol 1397. Berlin: Springer-Verlag, 1997: 291-312.

[3] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography [C]// LNCS, vol 2894. Berlin: Springer-Verlag, 2003: 452-473.

[4] BARBOSA M, FARSHIM P. Certificateless signcryption[C]//Proc of ASIACCS. New York: ACM Press, 2008: 369-372.

[5] WU Chen-huang, CHEN Zhi-xiong. A new efficient ceritificateless signcryption scheme[C]//Proc of ISISE. 2008: 661-664.

[6] SHARMILA S, SELVI D, VIVEK S S, *et al*. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairings [EB/OL]. (2009-03-05). http://eprint.iacr.org/2009/298.pdf.

[7] ARANHA D, CASTRO R, LOPEZ J, *et al*. Efficient signcryption [EB/OL]. (2008-09-05). http://sbseg2008.inf.ufrgs.br/anais/data/pdf/st03_01_resumo.pdf.

[8] BARRETO P S L M, DEUSAJUTE A M, CRUZ E S, *et al*. Toward efficient certificateless signcryption from (and without) bilinear pairings[EB/OL]. (2008-09-05). http://sbseg2008.inf.ufrgs.br/anais/data/pdf/st03_03_artigo.pdf.

[9] LI F G, MASAAKI S, TSUYOSHI T. Certificateless hybrid signcryption[C]// LNCS, vol 5451. Berlin: Springer-Verlag, 2009: 112-123.

[10] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报, 2011, 22(8): 1918-1926.

[11] DENT A W. A survey of certificateless encryption schemes and security models[J]. International Journal of Information Security, 2008, 7(5): 349-377.