Journal of Computer Applications
计算机应用,2013,33(7):1846 - 1850
ISSN 1001-9081
CODEN JYIIDU
2013-07-01
http://www.joca.cn

文章编号:1001-9081(2013)07-1846-05
doi:10.11772/j.issn.1001-9081.2013.07.1846

标准模型下可证安全的有效无证书签密方案

孙　华[1*],孟　坤[2]
(1.安阳师范学院 计算机与信息工程学院,河南 安阳 455000;　2.清华大学 计算机科学与技术系,北京 100084)
(*通信作者电子邮箱 sh1227@163.com)

摘　要:目前大多数无证书签密方案都是在随机预言模型下提出的,针对随机预言模型下的方案往往无法在实际应用中构造相应实例这一问题,采用标准模型的方法来进行构造。在对几个已有标准模型下相应方案分析的基础上,指出它们都是不安全的。以 Au 等所提出的方案(AU M H, LIU J K, YUEN T H, *et al*. Practical hierarchical identity based encryption and signature schemes without random oracles. http://eprint.iacr.org/2006/368.pdf)为基础,利用椭圆曲线上的双线性对性质,提出了一个新的标准模型下可证安全的无证书签密方案。最后,利用决策双线性 Diffie-Hellman(DBDH)等困难问题,证明该方案满足适应性选择密文攻击下的不可区分性以及适应性选择消息和身份攻击下的存在不可伪造性,因而方案是安全可靠的。

关键词:标准模型;签密;可证明安全;无证书公钥密码体制
中图分类号:TP309.2　　**文献标志码**:A

Efficient provably secure certificateless signcryption scheme in standard model

SUN Hua[1*], MENG Kun[2]
(1. *School of Computer and Information Engineering, Anyang Normal University, Anyang Henan* 455000, *China*;
2. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: At present, most of the existing certificateless signcryption schemes proven secure are proposed in the random oracle. Concerning the problem that this kind of schemes usually can not construct the corresponding instance in the practical application, a certificateless signcryption scheme was designed in the standard model. By analyzing several certificateless signcryption schemes in the standard model, it was pointed out that they were all insecure. Based on Au's scheme (AU M H, LIU J K, YUEN T H, *et al*. Practical hierarchical identity based encryption and signature schemes without random oracles. http://eprint.iacr.org/2006/368.pdf), a new proven secure certificateless signcryption scheme was proposed in the standard model by using bilinear pairing technique of elliptic curves. In the end, it is proved that the scheme satisfies indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message and identity attack under the complexity assumptions, such as Decisional Bilinear Diffie-Hellman (DBDH) problem. Therefore, the scheme was secure and reliable.

Key words: standard model; signcryption; provable security; certificateless Public Key Cryptography (PKC)

0　引言

1984 年,Shamir[1]创造性地提出了基于身份的公钥密码学,它可以有效地解决传统公钥密码系统中的复杂证书管理问题,随后许多基于身份的密码方案被相继提出[2-3]。由于在基于身份密码体制中,用户私钥由密钥产生中心(Key Generation Center, KGC)产生,因而其存在密钥托管问题,故不能实现真正意义上的不可否认性。2003 年,Al-Riyami 等[4]提出了无证书公钥密码学,在该体制中存在两类攻击者:A_{I}(恶意用户)和 A_{II}(恶意的 KGC)。对于 A_{I} 而言,其可以替换任意用户的公钥;对于 A_{II} 而言,它知道系统主密钥,但不可以替换用户的公钥。由于该体制无需使用证书且密钥生成中心只产生用户的部分私钥,这就避免了密钥托管问题,因而具有传统公钥体制和基于身份公钥体制两者的优点。

1997 年,Zheng[5]首次提出了签密这一密码原语,同时提出了一个有效的签密方案,它结合了公钥加密和数字签名的功能,然而含有形式化安全证明的签密方案[6-7]直到若干年后才被提出来。2008 年,Barbosa 等[8]提出了无证书签密的概念,并给出了第一个无证书签密方案,然而该方案在实现过程中需要六个双线性对运算,不仅效率较低而且方案本身也是不安全的。随后,Aranha 等[9]也提出了一种无证书签密方案,可是该方案中没有给出形式化的安全性证明过程。同年,Wu 等[10]给出了一个有效的无证书签密方案,该方案在实现过程中需要四个双线性对运算,然而文献[11]指出 Wu 等所提出的方案既不满足机密性同时也不满足不可伪造性。2008 年,Selvi 等[12]还提出了第一个多接收者签密方案。2010 年,Xie 等[13]提出了一个仅需要两个双线性对运算的无证书签密方案,然而文献[14]指出该方案不满足第一类攻击下的存在不可伪造性。

以上这些方案都是在随机预言模型下提出的,然而将随机预言模型中的 Hash 函数看成是完全随机的,这是一个很强的要求,在实际应用中往往无法构造相应的实例,因而设计标

收稿日期:2013-01-30;**修回日期**:2013-03-15。　**基金项目**:国家自然科学基金资助项目(61170244,U1204402);河南省科技厅科技攻关计划项目(112102210370);河南省教育厅科学技术研究重点项目(12A520002)。

作者简介:孙华(1980 -),男,河南安阳人,副教授,博士,主要研究方向:密码学、信息安全;　孟坤(1980 -),男,河南项城人,博士,主要研究方向:无线网络安全、计算机网络性能评价。

准模型下的无证书签密更有实际意义。2010 年,Liu 等[15]提出了一种标准模型下的无证书签密方案,然而文献[16]指出 Liu 等所提出的签密方案是不安全的。随后,文献[17]和文献[18]也分别提出了标准模型下的无证书签密方案,在本文的第 2 章中将通过分析指出这两个方案也是不安全的。

本文以文献[3]为基础,在标准模型下提出了一种有效的无证书签密(certificateless signcrypiton,CLSC)方案,并通过困难问题假设证明了其安全性,同时对方案的效率进行了分析。

1　预备知识

1.1　双线性对

设 G 和 G_T 是阶为素数 p 的两个循环群,群 G 的生成元为 g,双线性对是满足如下性质的映射 $e:G\times G\to G_T$:

1)双线性性:对于所有的 $P,Q\in G$ 与 $a,b\in \mathbf{Z}_p^*$,都有 $e(P^a,Q^b)=e(P,Q)^{ab}$。

2)非退化性:$e(g,g)\neq 1$。

3)可计算性:存在一个有效的算法计算 $e(P,Q)$,其中 $P,Q\in G$。

1.2　有关困难问题

1)计算 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题:已知阶为素数 p 的循环群 G,g 是其生成元,对于任意 $a,b\in \mathbf{Z}_p^*$,给定 $g^a,g^b\in G$,计算 g^{ab}。

2)决策双线性 Diffie-Hellman(Decisional Bilinear Diffie-Hellman,DBDH)问题:已知阶为素数 p 的循环群 G,g 是其生成元,对于任意 $a,b,c\in \mathbf{Z}_p^*$,给定 $g^a,g^b,g^c\in G,h\in G_T$,判定 $h=e(g,g)^{abc}$ 是否成立。

3)截断的确定性 q-增强双线性 Diffie-Hellman 指数(truncated decisional q-Augmented Bilinear Diffie-Hellman Exponent,truncated decisional q-ABDHE)问题[2]:给定一个 G 中 $(q+3)$ 个元素组成的向量 $(g',g'^{a^{q+2}},g,g^a,g^{a^2},\cdots,g^{a^q})$ 以及 $Z\in G_T$,判定等式 $Z=e(g^{a^{q+1}},g')$ 是否成立。

4)q-强 Diffie-Hellman(q-Strong Diffie-Hellman,q-SDH)问题[19]:已知阶为素数 p 的循环群 G,g 是其生成元,对于任意 $x\in \mathbf{Z}_p^*$,给定 $(g,g^x,\cdots,g^{x^q})\in G^{q+1}$,计算 $(c,g^{1/(x+c)})$,$c\in_R \mathbf{Z}_p^*$。

2　几个无证书签密方案的密码学分析

2.1　对 Liu 等所提方案的安全性分析

文献[16]中指出 Liu 等[15]所提出的标准模型下无证书签密方案,在面对 A_I(恶意用户)的攻击时,方案不满足机密性这一安全特性,故这里不再重复该分析过程。

2.2　对向新银中所提方案的安全性分析

下面证明文献[17]方案不满足不可伪造性这一安全特性。

证明　给定一有效密文 $C=(C_1,C_2,C_3,C_4,\sigma)$,其中:$C_1=g_1^s g^{-s\cdot id}$,$C_2=m\cdot e(g,g_1)^{-s}$,$C_3=psk_3^s=g^{s\cdot r_{id}}$,$C_4=(hu^{id})^s$,$\sigma=psk_2\cdot g^s=(hu^{id})^{1/a-id}\cdot g^s$,攻击者任意选取 $x\in \mathbf{Z}_q^*$,可计算:

$$C_1^*=g_1^s g^{-s\cdot id}\cdot g_1^x g^{-x\cdot id}=g_1^{s+x}g^{-(s+x)\cdot id}$$

$$C_2^*=m\cdot e(g,g_1)^{-s}\cdot e(g,g_1)^{-x}=m\cdot e(g,g_1)^{-(s+x)}$$

$$C_3^*=g^{s\cdot r_{id}}\cdot g^{x\cdot r_{id}}=g^{(s+x)\cdot r_{id}}$$

$$C_4^*=(hu^{id})^s\cdot(hu^{id})^x=(hu^{id})^{s+x}$$

$$\sigma^*=(hu^{id})^{1/a-id}\cdot g^s\cdot g^x=(hu^{id})^{1/a-id}\cdot g^{s+x}$$

因此有 $C^*=(C_1^*,C_2^*,C_3^*,C_4^*,\sigma^*)$ 是一个有效的伪造无证书签密,故该方案不满足不可伪造性。

2.3　对王培东等所提方案的安全性分析

下面证明文献[18]方案不满足不可伪造性这一安全特性。

证明　给定一有效密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$,其中 $\sigma_1=e(g,g)^s$,$\sigma_2=m\cdot e(g,h)^{-s}$,$\sigma_3=sk_2^s=(hg^{-id})^{s/a-id}$,$\sigma_4=sk_3^{s-1}=(hg^{-id})^{1/s(a-id)}$,$\sigma_5=g_1^s g^{-s\cdot id}$,攻击者任意选取 $x\in \mathbf{Z}_q^*$,令 $m^*=m^x$,可计算:

$$\sigma_1^*=e(g,g)^{sx}$$

$$\sigma_2^*=m^*\cdot e(g,h)^{-sx}$$

$$\sigma_3^*=sk_2^{sx}=(hg^{-id})^{sx/a-id}$$

$$\sigma_4^*=(sk_3^{s-1})^{x-1}=(hg^{-id})^{1/sx(a-id)}$$

$$\sigma_5^*=g_1^{sx}g^{-sx\cdot id}$$

因此有 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*)$ 是一个有效的伪造无证书签密,故该方案不满足不可伪造性。

3　安全有效的无证书签密方案

本文提出的无证书签密方案描述如下。

令 G、G_T 是阶为素数 p 的循环群,$e:G\times G\to G_T$ 是一个双线性映射,无碰撞的哈希函数 $H:\{0,1\}^*\to\{0.1\}^{n_m}$ 将任意长度的消息 M 输出为长度 n_m 的位串。

1)系统参数设置。KGC 选取 G 的生成元 $g\in_R G$、h_1,h_2,$h_3\in_R G$ 以及 n_m 维向量 $\hat{\boldsymbol{M}}=(m_i)$,其中 $m_i\in_R \mathbf{Z}_p^*$。KGC 选取 $\alpha\in_R \mathbf{Z}_p$,计算 $g_1=g^\alpha$,$z_0=e(g,g)$,$z_1=e(g,h_1)$,则系统公开参数为 $params=(G,G_T,e,g,g_1,h_1,h_2,h_3,H,\hat{\boldsymbol{M}},z_0,z_1)$,系统私钥 $msk=\alpha$ 保密。

2)部分私钥提取。给定用户身份 $ID\in \mathbf{Z}_p$,KGC 随机选取 $r_{ID}\in \mathbf{Z}_p$,计算 $d_1=(h_1 g^{-r_{ID}})^{1/\alpha-ID}$,如果 $ID=\alpha$,那么 KGC 将无法计算。令 $d_2=r_{ID}$,则用户的部分私钥为 $D_{ID}=(d_1,d_2)$,并通过安全信道将其发送给用户。

3)设置秘密值。对于身份为 ID 的用户,其任意选取 $x_{ID}\in \mathbf{Z}_p^*$ 作为其秘密值。

4)用户公钥产生。计算 $PK_{ID}=g^{x_{ID}}$ 作为用户 ID 的公钥。

5)私钥产生。对于用户 ID,其私钥为 $SK_{ID}=(s_1,s_2,s_3)=(d_1,d_2,x_{ID})$。

6)签密。设签密产生者的身份为 ID_S,签密接收者的身份为 ID_R,待签密消息为 $M\in G_T$,可通过如下步骤来产生无证书签密:

①令 $W=H(M)$ 为消息 M 的长度为 n_m 的位串,$M\subseteq\{1,2,\cdots,n_m\}$ 为其位串中 $W[k]=1$ 的序号 k 的集合,计算 $T=\sum_{i\in M} m_i$。

②签密产生者利用其私钥 SK_{ID_S},随机选取 $s\in \mathbf{Z}_p$,计算:

$$C_1=g_1^s g^{-sID_S}$$

$$C_2=g_1^s g^{-sID_R}$$

$$C_3=e(g,g)^s=z_0^s$$

$$C_4=M\cdot e(h_1,g^{xID_R})^{-s}$$

$$C_5=s_{ID_S,1}\cdot(h_3 h_2^{ID_S})^{s\cdot T}$$

$$C_6=s_{ID_S,2}=r_{ID_S}$$

则生成的无证书签密为 $C=(C_1,C_2,C_3,C_4,C_5,C_6,T)$。

7)解签密。设签密产生者的身份为 ID_S，签密接收者 ID_R 的私钥为 SK_{ID_R}，其在收到无证书签密 $C=(C_1,C_2,C_3,C_4,C_5,C_6,T)$ 后，其进行如下计算：

①首先验证等式 $e(g_1g^{-ID_S},C_5)=z_1\cdot z_0^{-C_6}\cdot e(C_1,(h_3h_2^{ID_S})^T)$ 是否成立；

②若等式成立，可知是 $C=(C_1,C_2,C_3,C_4,C_5,C_6,T)$ 一个有效的无证书签密，然后签密接收者 ID_R 利用其私钥 SK_{ID_R} 计算出消息 $M=C_4\cdot[e(C_2,s_{ID_R,1})C_3^{sID_R,2}]^{sID_R,3}$。

4 安全性分析

4.1 方案的正确性

本文方案正确性可由下面的等式进行验证：

①$e(g_1g^{-ID_S},C_5)=$

$$e\left(g_1g^{-ID_S},(h_1g^{-rID_S})^{1/\alpha-ID_S}(h_3h_2^{ID_S})^{s\cdot\left(\sum_{i\in M}m_i\right)}\right)=$$

$$e(g,h_1)e(g,g^{-rID_S})e\left(g_1^sg^{-sID_S},(h_3h_2^{ID_S})^{\left(\sum_{i\in M}m_i\right)}\right)=$$

$$z_1\cdot z_0^{-C_6}\cdot e\left(C_1,(h_3h_2^{ID_S})^{\left(\sum_{i\in M}m_i\right)}\right)$$

②$C_4\cdot[e(C_2,s_{ID_R,1})C_3^{sID_R,2}]^{sID_R,3}=$

$M\cdot e(h_1,g^{xID_R})^{-s}\cdot[e(g_1^sg^{-sID_R},(h_1g^{-rID_R})^{1/\alpha-ID_R})z_0^{srID_R}]^{xID_R}=$

$M\cdot e(h_1,g^{xID_R})^{-s}\cdot[e(g^s,h_1)\cdot e(g^s,g^{-rID_R})e(g,g)^{srID_R}]^{xID_R}=$

$M\cdot e(h_1,g^{xID_R})^{-s}\cdot e(g^s,h_1)^{xID_R}=M$

因而方案是正确的。

4.2 不可区分性

在无证书签密方案中存在着两类攻击者，$\mathcal{A}_\mathrm{I}$（恶意用户），$\mathcal{A}_\mathrm{II}$（恶意的 KGC）。对于 $\mathcal{A}_\mathrm{I}$ 类攻击者而言，它不知道系统私钥 msk，但可以替换任意用户的公钥；对于 $\mathcal{A}_\mathrm{II}$ 类攻击者而言，它知道系统私钥 msk，但不能替换用户的公钥。下面通过模拟两类攻击者 $\mathcal{A}\in(\mathcal{A}_\mathrm{I},\mathcal{A}_\mathrm{II})$ 与挑战者 P 之间进行交互的攻击场景游戏，证明方案满足不可区分性。

定理 1 在 truncated decisional q-ABDHE 困难问题假设下，本文方案在第一类攻击者 $\mathcal{A}_\mathrm{I}$ 攻击下满足适应性选择密文攻击下的不可区分性。

证明 假设攻击者 $\mathcal{A}_\mathrm{I}$ 能以不可忽略的优势攻击本方案，那么就可以构造算法 B，B 可利用 $\mathcal{A}_\mathrm{I}$ 解决 truncated decisional q-ABDHE 问题。

给定算法 B 一个 truncated decisional q-ABDHE 问题的实例$(g',g'^{a^{q+2}},g,g^a,g^{a^2},\cdots,g^{a^q},Z)$，其目标是判定 $Z=e(g,g')^{a^{q+1}}$ 是否成立。为此算法 B 模仿 $\mathcal{A}_\mathrm{I}$ 的挑战者，具体过程如下。

初始化 算法 B 通过如下计算来构造系统公开参数 $params$。首先，算法 B 选取哈希函数 $H:\{0,1\}^*\rightarrow\{0.1\}^{n_m}$ 以及 n_m 维向量 $\hat{\boldsymbol{M}}=(m_i)$；其次，算法 B 随机选取一阶为 q 的多项式 $f_q(x)\in\mathbf{Z}_p[x]$ 和 $u\in\mathbf{Z}_p^*$，令 $g_1=g^a,h_1=g^{f(a)}$，$h_2=g^u,h_3=g_1^u,z_0=e(g,g),z_1=e(g,h_1)$，则系统公开参数为 $params=(G,G_T,e,g,g_1,h_1,h_2,h_3,H,\hat{\boldsymbol{M}},z_0,z_1)$，系统主密钥为 $msk=a$；最后，算法 B 将 $params$ 发送给敌手 $\mathcal{A}_\mathrm{I}$。

第一阶段 敌手 $\mathcal{A}_\mathrm{I}$ 可以适应性地向算法 B 发起如下一定数量的询问（这里假定 $\mathcal{A}_\mathrm{I}$ 在对用户私钥询问和签密询问之前已进行 H 询问和用户公钥询问），算法 B 维护列表 L_1、L_2、L_3、L_4，它在初始状态下是空表。当敌手 $\mathcal{A}_\mathrm{I}$ 发起询问时，算法 B 做如下响应。

①H 询问。询问 $H(M)$ 时，$1\leqslant i\leqslant q_H$，$q_H$ 为 H 询问的最大次数，算法 B 在向量 $\hat{\boldsymbol{M}}$ 中任意选取不多于 n_m 个元素，并计算其和 $T=\sum m_i$，然后将(M,T) 添加到列表 L_1 中。

②部分私钥询问。当询问身份为 ID_i 的部分私钥 D_{ID_i} 时，如果 $ID_i=a$，那么算法 B 可以利用 a 解决 truncated decisional q-ABDHE 问题；否则，令 $q-1$ 阶多项式为 $f_{q-1}(x)=f_q(x)-f(ID_i)/x-ID_i$，算法 B 计算 $d_1=g^{f_{q-1}(a)}$，$d_2=f_q(a)$，然后把 (ID_i,D_{ID_i}) 添加到列表 L_2 中，其中 $D_{ID_i}=(d_1,d_2)$，并将 D_{ID_i} 作为用户 ID_i 的部分私钥返回。

③用户公钥询问。当询问身份为 ID_i 的公钥 PK_{ID_i} 时，如果列表 L_3 中存在 $(ID_i,PK_{ID_i},x_{ID_i},c)$，则返回 PK_{ID_i}；否则，算法 B 随机选取 $x_{ID_i}\in\mathbf{Z}_p^*$ 并计算 $PK_{ID_i}=g^{xID_i}$，然后把 $(ID_i,PK_{ID_i},x_{ID_i},1)$ 添加到列表 L_3 中，并将 PK_{ID_i} 作为用户 ID_i 的公钥返回。

④用户私钥询问。当询问身份为 ID_i 的私钥 SK_{ID_i} 时，如果列表 L_4 中存在 (ID_i,SK_{ID_i})，则返回 SK_{ID_i}；否则，算法 B 分别从列表 L_2、L_3 中查询相应的值 (ID_i,D_{ID_i}) 和 $(ID_i,PK_{ID_i},x_{ID_i},c)$，令 $SK_{ID_i}=(D_{ID_i},x_{ID_i})$，然后把 (ID_i,SK_{ID_i}) 添加到列表 L_4 中，并将 SK_{ID_i} 作为用户 ID_i 的私钥返回。

⑤公钥替换询问。当敌手 $\mathcal{A}_\mathrm{I}$ 需将身份 ID_i 的公钥替换为 PK'_{ID_i} 时，算法 B 先在列表 L_3 中查询 $(ID_i,PK_{ID_i},x_{ID_i},1)$，若含有相应的值，则将公钥替换为 $PK_{ID_i}=PK'_{ID_i}$ 且 $c=0$；否则，算法 B 先对 ID_i 进行用户公钥询问，然后令 $PK_{ID_i}=PK'_{ID_i}$ 且 $c=0$，并将修改后的值添加到列表 L_3 中。

⑥签密询问。当敌手 $\mathcal{A}_\mathrm{I}$ 发起 (M,ID_S,ID_R) 的签密询问时，若 $ID_S=a$，那么算法 B 可以利用 a 解决 truncated decisional q-ABDHE 问题；否则，算法 B 能够构造 ID_S 的私钥，然后运行签密算法并返回相应的无证书签密 $C=(C_1,C_2,C_3,C_4,C_5,C_6,T)$。

⑦解签密询问。当敌手 $\mathcal{A}_\mathrm{I}$ 发起 C 的解签密询问时，若 $ID_R=a$，那么算法 B 可以利用 a 解决 truncated decisional q-ABDHE 问题；否则，算法 B 从列表 L_4 中查找其私钥 SK_{ID_R}，然后运行解签密算法计算出相应的消息 m 并将其返回。

挑战阶段 敌手 $\mathcal{A}_\mathrm{I}$ 选取两个长度相同的消息 M_0、M_1，签密产生者为 ID_S^*，签密接收者为 ID_R^*，如果 $ID_S^*=a$，那么算法 B 可以利用 a 解决 truncated decisional q-ABDHE 问题；否则，算法 B 随机选取 $b\in(0,1)$，计算 ID_S^* 和 ID_R^* 的私钥 $SK_{ID_S^*}$ 和 $SK_{ID_R^*}$。设 $W^*=H(M_b)$ 为消息 M_b 的长度为 n_m 的位串，$M^*\subseteq\{1,2,\cdots,n_m\}$ 为其位串中 $W^*[k]=1$ 的序号 k 的集合，计算 $T^*=\sum_{i\in M^*}m_i$。令 $f_{q+2}(x)=x^{q+2}$，$f_{q+1}(x)=f_{q+2}(x)-f(ID_S^*)/x-ID_S^*$，多项式 $f_{q+1}(x)$ 中 x^i 的系数为 $F_{q+1,i}$，其中 $0\leqslant i\leqslant q+1$。算法 B 进行如下构造：

$$C_1^*=g'^{f_{q+2}(x)-f_{q+2}(ID_S^*)}$$

$$C_2^*=g'^{f_{q+2}(x)-f_{q+2}(ID_R^*)}$$

$$C_3^*=Z\cdot e\left(g',\prod_{i=0}^{q}g^{F_{q+1,i}a^i}\right)$$

$$C_4^*=M_b/[e(C_2^*,s_{ID_R^*,1})C_3^{*sID_R^*,2}]^{sID_R^*,3}$$

$$C_5^*=s_{ID_S^*,1}(g_1^ug^{uID_S^*})^{s\cdot T^*}$$

$C_6^* = s_{ID_S^*,2} = f_q(ID_S^*) = r_{ID_S^*}$

令 $s = (\log_g g')f_{q+1}(a)$,如果 $Z = e(g^{a^{q+1}}, g')$,则有

$C_1^* = g_1^s g^{-sID_S^*}$

$C_2^* = g_1^s g^{-sID_R^*}$

$C_3^* = e(g,g)^s$

$C_4^* = M_b \cdot e(h_1, g^{xID_R^*})^{-s}$

$C_5^* = s_{ID_S^*,1}(g_1^u g^{uID_S^*})^{s \cdot T^*}$

$C_6^* = s_{ID_S^*,2} = f_q(ID_S^*) = r_{ID_S^*}$

可知 $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, T^*)$ 是一个有效的无证书签密,并将其返回给敌手 $\mathcal{A}_{\mathrm{I}}$。

第二阶段　敌手 $\mathcal{A}_{\mathrm{I}}$ 可以像第一阶段那样发起一定数量的询问,但是敌手 $\mathcal{A}_{\mathrm{I}}$ 不能询问 ID_R^* 的私钥以及不能对 C^* 进行解签密询问。

猜测阶段　敌手 $\mathcal{A}_{\mathrm{I}}$ 输出对 b 的猜测 b'。如果 $b = b'$,那么算法 B 输出 $Z = e(g^{a^{q+1}}, g')$ 作为 truncated decisional q-ABDHE 问题的解;否则,算法 B 认为 Z 是 G_T 中的一个随机元素。

因此,如果存在一个敌手 $\mathcal{A}_{\mathrm{I}}$ 能够以不可忽略的概率攻击本方案,那么就存在一个有效的算法能够以不可忽略的概率解决 truncated decisional q-ABDHE 问题,而这与 truncated decisional q-ABDHE 是一个困难问题相矛盾,故本文方案在第一类攻击者 $\mathcal{A}_{\mathrm{I}}$ 攻击下是安全的。

定理 2　在 DBDH 困难问题假设下,本文方案在第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 攻击下满足适应性选择密文攻击下的不可区分性。

证明　假设攻击者 $\mathcal{A}_{\mathrm{II}}$ 能以不可忽略的优势攻击本方案,那么就可以构造算法 B,B 可利用 $\mathcal{A}_{\mathrm{II}}$ 解决 DBDH 问题。

给定算法 B 一个 DBDH 问题的实例 (g^a, g^b, g^c, h),其目标是判定 $h = e(g,g)^{abc}$ 是否成立。为此算法 B 模仿 $\mathcal{A}_{\mathrm{II}}$ 的挑战者,具体过程如下。

初始化　算法 B 通过如下计算来构造系统公开参数 *params*。首先,算法 B 选取哈希函数 $H: \{0,1\}^* \rightarrow \{0,1\}^{n_m}$ 以及 n_m 维向量 $\hat{\boldsymbol{M}} = (m_i)$;其次,算法 B 随机选取 $\gamma, u, v \in \mathbf{Z}_p^*$,令 $g_1 = g^\gamma, h_1 = g^a, h_2 = g^u, h_3 = g^v, z_0 = e(g,g), z_1 = e(g,h_1)$,系统主密钥为 $msk = \gamma$,系统公开参数为 $params = (G, G_T, e, g, g_1, h_1, h_2, h_3, H, \hat{\boldsymbol{M}}, z_0, z_1)$;最后,算法 B 将 *params*、*msk* 发送给敌手 $\mathcal{A}_{\mathrm{II}}$。

第一阶段　敌手 $\mathcal{A}_{\mathrm{II}}$ 可以如同定理 1 中那样,发起一定数量的询问,由于 $\mathcal{A}_{\mathrm{II}}$ 知道系统主密钥,因而这里不需要进行部分私钥询问且不能进行用户公钥替换询问。

挑战阶段　敌手 $\mathcal{A}_{\mathrm{II}}$ 选取两个长度相同的消息 M_0、M_1,签密产生者为 ID_S^*,签密接收者为 ID_R^*。算法 B 随机选取 $b \in (0,1)$ 并计算 ID_S^* 的私钥 $SK_{ID_S^*}$。设 $W^* = H(M_b)$ 为消息 M_b 的长度为 n_m 的位串,$M^* \subseteq \{1,2,\cdots,n_m\}$ 为其位串中 $W^*[k] = 1$ 的序号 k 的集合,计算 $T^* = \sum_{i \in M^*} m_i$。算法 B 进行如下构造:

$C_1^* = (g^c)^{\gamma - ID_S^*} = g_1^c g^{-cID_S^*}$

$C_2^* = (g^c)^{\gamma - ID_R^*} = g_1^c g^{-cID_R^*}$

$C_3^* = e(g, g^c) = e(g,g)^c = z_0^c$

$C_4^* = M_b \cdot h^{-1}$

$C_5 = s_{ID_S^*,1}(g^c)^{(v+uID_S^*)T^*} = s_{ID_S^*,1}(h_3 h_2^{ID_S^*})^{c \cdot T^*}$

$C_6 = s_{ID_S^*,2} = r_{ID_S^*}$

令 ID_R^* 的公钥为 $PK_{ID_R^*} = g^b$,如果 $h = e(g,g)^{abc}$,则有:

$C_4^* = M_b \cdot e(g,g)^{-abc} = M_b \cdot e(h_1, g^b)^{-c}$

可知 $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, T^*)$ 是一个有效的无证书签密,并将其返回给敌手 $\mathcal{A}_{\mathrm{II}}$。

第二阶段　敌手 $\mathcal{A}_{\mathrm{II}}$ 可以如同定理 1 中那样,发起一定数量的询问。

猜测阶段　敌手 $\mathcal{A}_{\mathrm{I}}$ 输出对 b 的猜测 b'。如果 $b = b'$,那么算法 B 输出 $h = e(g,g)^{abc}$ 作为 DBDH 问题的解;否则,算法 B 认为 h 是 G_T 中的一个随机元素。

因此,如果存在一个敌手 $\mathcal{A}_{\mathrm{II}}$ 能够以不可忽略的概率攻击本方案,那么就存在一个有效的算法能够以不可忽略的概率解决 DBDH 问题,而这与 DBDH 是一个困难问题相矛盾,故本文方案在第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 攻击下是安全的。

4.3　不可伪造性

下面通过模拟两类攻击者 $A \in (\mathcal{A}_{\mathrm{I}}, \mathcal{A}_{\mathrm{II}})$ 与挑战者之间进行交互的攻击场景游戏,证明方案满足存在不可伪造性。

定理 3　在 q-SDH 困难问题假设下,本文方案在第一类攻击者 $\mathcal{A}_{\mathrm{I}}$ 攻击下满足适应性选择消息攻击下的存在不可伪造性。

证明　假设攻击者 $\mathcal{A}_{\mathrm{I}}$ 能以不可忽略的优势攻击本方案,则可以构造算法 B,B 可以利用 $\mathcal{A}_{\mathrm{I}}$ 解决 q-SDH 问题。

给定算法 B 一个 q-SDH 问题的实例 $(g, g^a, g^{a^2}, \cdots, g^{a^q})$,其目标是计算 $(c, g^{1/(a+c)})$,其中 $c \in \mathbf{Z}_p^*$。为此算法 B 模仿 $\mathcal{A}_{\mathrm{I}}$ 的挑战者,具体过程如下。

初始化　算法 B 可以如同定理 1 中那样构造系统公开参数 *params*,与定理 1 中的区别在于 $h_2 = g^{-u}$,其他参数的构造与定理 1 中相同,然后算法 B 将其发送给敌手 $\mathcal{A}_{\mathrm{I}}$。

询问阶段　当敌手 $\mathcal{A}_{\mathrm{I}}$ 发起询问时,算法 B 进行如下响应:

① H_1 询问。如同在定理 1 中第一阶段那样,算法 B 进行响应。

②部分私钥询问。当询问身份为 ID_i 的部分私钥 D_{ID_i} 时,如果 $ID_i = a$,那么算法 B 可以利用 a 解决 q-SDH 问题;否则,算法 B 如同定理 1 中那样进行响应。

③用户公钥询问。如同在定理 1 中第一阶段那样,算法 B 进行响应。

④用户私钥询问。如同在定理 1 中第一阶段那样,算法 B 进行响应。

⑤公钥替换询问。如同在定理 1 中第一阶段那样,算法 B 进行响应。

⑥签密询问。当敌手 $\mathcal{A}_{\mathrm{I}}$ 发起 (M, ID_S, ID_R) 的签密询问时,若 $ID_S = a$,那么算法 B 可以利用 a 解决 q-SDH 问题;否则,如同在定理 1 中第一阶段那样,算法 B 进行响应。

⑦解签密询问。当敌手 $\mathcal{A}_{\mathrm{I}}$ 发起 C 的解签密询问时,若 $ID_R = a$,那么算法 B 可以利用 a 解决 q-SDH 问题;否则,如同在定理 1 中第一阶段那样,算法 B 进行响应。

伪造阶段　敌手 $\mathcal{A}_{\mathrm{I}}$ 输出在消息 M^*、签密产生者 ID_S^*、签密接收者 ID_R^* 下的伪造无证书签密 $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, T^*)$,这里要求敌手 $\mathcal{A}_{\mathrm{I}}$ 没有询问过 ID_S^* 的私钥,且没有对 (M^*, ID_S^*, ID_R^*) 进行过签密询问。令 $q-1$ 阶多项式为 $f_{q-1}(x) = f_q(x) - C_6^*/x - ID_S^*$,故有 $f_{q-1}(a) = \sum_{k=0}^{q-1} A_k a^k + A_{-1}/(a - ID_S^*)$,如果 $A_{-1} = 0$,那么算法 B 将失败

退出;否则,可以得到:

$$C_1^* = g^{s(a-ID_S^*)}$$

$$C_5^* = (h_1 g^{-C^{*6}})^{1/a-ID_S^*} \cdot (h_3 h_2^{ID_S^*})^{s \cdot T^*} = g^{f(a)-C_6^*/a-ID_S^*} \cdot g^{u(a-ID_S^*)s \cdot T^*}$$

故可得 q-SDH 问题的解 $g^{1/a-ID_S^*} = \left[\frac{C_5^*}{C_1^{*uT^*} \cdot g^{k=0}}\right]^{1/A-1}$。

因此,如果存在一个攻击者 $\mathcal{A}_{\mathrm{I}}$ 能够以不可忽略的概率伪造一个有效的无证书签密,那么就存在一个有效的算法能以不可忽略的概率解决 q-SDH 问题,而这与 q-SDH 问题是一个困难问题相矛盾,故方案是不可伪造的。

定理 4 在 CDH 困难问题假设下,本文方案在第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 攻击下满足适应性选择消息攻击下的存在不可伪造性。

证明 对于第二类攻击者 $\mathcal{A}_{\mathrm{II}}$,由于其知道系统的主密钥,因而很容易证明,如果存在这样的攻击者能够以不可忽略的优势攻击本方案,那么就可以构造算法 B,B 可以利用 $\mathcal{A}_{\mathrm{II}}$ 解决 CDH 问题,这里省略该证明过程。

5 性能分析

表 1 从方案效率和方案安全性两个方面入手,将本文方案与现有的几个标准模型下无证书签密方案进行比较。

表 1 4 种标准模型下无证书签密方案的比较

方案	公钥长度	私钥长度	密文长度	对运算量	方案是否安全
文献[15]方案	1	2	5	5	否
文献[17]方案	2	3	5	4	否
文献[18]方案	2	3	5	2	否
本文方案	1	3	7	4	是

这里的公钥长度、私钥长度、密文长度分别为相应群 G 或 G_T 中元素的个数,由于双线性对运算所花费的计算成本远高于诸如群中元素的点乘和指数运算,故这里仅考虑双线性对的计算量。在本方案中,可以通过预计算 $z_0 = e(g,g)$ 和 $z_1 = e(g,h_1)$ 并将其在系统公开参数中公布从而提高计算效率。通过方案的对比可知,现有的几个标准模型下的无证书签密方案是不安全的,同时从计算量方面考虑,本文方案也具有较高的效率。

6 结语

因无证书公钥密码体制既避免了传统 PKI 中复杂的证书管理,同时又克服了身份密码体制中的密钥托管问题,故引起了广大学者的浓厚研究兴趣。本文中提出了一个标准模型下的无证书签密方案,在整个过程中仅需要四个双线性对计算,并且在困难问题下对方案的安全性进行了证明,故方案是安全可靠的。下一步将继续对标准模型下的无证书签密方案进行研究,使其具有更少的运算量,同时结合具体的应用场景对标准模型下的其他无证书密码方案展开研究。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. Berlin: Springer-Verlag, 1985: 47 - 53.

[2] GENTRY C. Practical identity-based encryption without random oracles [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2006: 445 - 464.

[3] AU M H, LIU J K, YUEN T H, *et al*. Practical hierarchical identity based encryption and signature schemes without random oracles [EB/OL]. [2012 - 12 - 15]. http://eprint.iacr.org/2006/368.pdf.

[4] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 2894. Berlin: Springer-Verlag, 2003: 452 - 473.

[5] ZHENG Y L. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [C]// Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, LNCS 1294. Berlin: Springer-Verlag, 1997: 165 - 179.

[6] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption [C]// Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology, LNCS 2332. Berlin: Springer-Verlag, 2002: 83 - 107.

[7] BAEK J, STEINFELD R, ZHENG Y L. Formal proofs for the security of signcryption [J]. Journal of Cryptology, 2007, 20(2): 203 - 235.

[8] BARBOSA M, FARSHIM P. Certificateless signcryption [C]// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 369 - 372.

[9] ARANHA D, CASTRO R, LOPEZ J, *et al*. Efficient certificateless signcryption [EB/OL]. [2012 - 12 - 20]. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf.

[10] WU C H, CHEN Z X. A new efficient certificateless signcryption scheme [C]// Proceedings of the 2008 International Symposium on Information Science and Engineering. Washington, DC: IEEE Computer Society, 2008: 661 - 664.

[11] SELVI S S D, VIVEK S S, RANGAN C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [EB/OL]. [2012 - 12 - 21]. http://eprint.iacr.org/2009/298.

[12] SELVI S S D, VIVEK S S, SHUKLA D, *et al*. Efficient and provably secure certificateless multi-receiver signcryption [C]// Proceedings of the 2nd International Conference on Provable Security, LNCS 5324. Berlin: Springer-Verlag, 2008: 52 - 67.

[13] XIE W J, ZHANG Z. Efficient and provably secure certificateless signcryption from bilinear maps [EB/OL]. [2012 - 12 - 21]. http://eprint.iacr.org/2009/578.pdf.

[14] SELVI S S D, VIVEK S S, RANGAN C P. Security weaknesses in two certificateless signcryption schemes [EB/OL]. [2012 - 12 - 21]. http://eprint.iacr.org/2010/092.

[15] LIU Z H, HU Y P, ZHANG X S, *et al*. Certificateless signcryption scheme in the standard model [J]. Information Sciences, 2010, 180(3): 452 - 464.

[16] WENG J, YAO G X, DENG R H, *et al*. Cryptanalysis of a certificateless signcryption scheme in the standard model [J]. Information Sciences, 2011, 181(3): 661 - 667.

[17] 向新银. 标准模型下的无证书签密方案[J]. 计算机应用, 2010, 30(8): 2151 - 2153.

[18] 王培东, 解英, 解凤强. 标准模型下可证安全的无证书签密方案[J]. 哈尔滨理工大学学报, 2012, 17(3): 83 - 86.

[19] TANAKA N, SAITO T. On the *q*-strong diffie-hellman problem [EB/OL]. [2012 - 12 - 21]. http://eprint.iacr.org/2010/215.pdf.