对一个基于身份的多重签密方案的分析和改进

张秋璞,叶顶锋
(中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: Waters 提出了一个标准模型下的基于身份的加密和签名方案,Paterson 和 Schuldt 在此基础上提出了一个基于身份的签名方案.Zhang 和 Xu 在上述两个方案的基础上,提出了一个基于身份的多重签密方案.本文指出 Zhang-Xu 的方案会受到私钥随机化攻击,并在标准模型下提出了一个改进的基于身份的多重签密方案,其中将解密私钥和签名私钥分开,用于签名的私钥无法随机化,同时该方案还可以抵抗内部泄漏攻击.

关键词: 基于身份密码; 多重签密; 私钥随机化; 双线性对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 12-2713-08

Cryptanalysis and Improvement of an Identity-Based Multi-Signcryption Scheme

ZHANG Qiu-pu, YE Ding-feng
(*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Waters proposed an identity-based encryption and signature scheme in standard model. Then Paterson and Schuldt proposed an identity-based signature scheme based on Waters' IBE. Zhang and Xu proposed an identity-based multi-signcryption scheme that using the above schemes. However, we show that Zhang-Xu's scheme is insecure under randomizing private key attack. Furthermore, we propose an improved identity-based multi-signcryption scheme in standard model. In our scheme, we divide the private keys into two parts, one is for decryption, the other is for signature, and the private key used for signature cannot be randomized. Moreover, our scheme can resist insider leak attack.

Key words: identity-based cryptography; multi-signcryption; randomize private key; bilinear pairings

1 引言

基于身份的加密(Identity-Based Encryption, IBE)由 Shamir 在文献[1]中提出,但是直到 2001 年,才由 Boneh 和 Franklin 提出了基于双线性对(Bilinear Pairings)的有效的 IBE 方案[2].之后,大量的基于身份的加密,签名以及签密方案[3~5]被提出.Waters 在文献[6]中提出了标准模型下的 IBE 和 IBS(Identity-Based Signature)方案,Paterson 和 Schuldt 在此基础上提出了一个标准模型下的 IBS 方案[7],这两个方案被广泛地应用[8~10].但是在这两个方案中,用户的私钥可以被随机化.尽管这两个方案本身是安全的,但是在使用它们构造新的方案时,需要注意可能由私钥随机化引发的不安全性.

签密的概念由 Zheng 在文献[11]中首次提出,可以在合理的步骤内同时完成签名和加密.签密的形式化定义由 Baek 等在文献[12]提出.第一个基于身份的签密方案由 Malone-Lee 在文献[13]中给出,但是 Libert 等在文献[14]中指出该方案是不安全的.Duan 和 Cao 在文献[15]中提出了基于身份的多接受者签密,将签密扩展到了多用户的环境.

多重签密是指多个发送者对同一消息进行签密,并使多重签密数据长度大致与单独的签密数据长度相等,从而在完成对多个发送者认证的同时,可大大降低数据的传输量.基于身份的密码体系不需要公钥,因此基于身份的多重签密方案能进一步降低数据的传输量.在文献[16]中,Zhang 和 Mao 在随机预言模型下提出了第一个基于身份的多重签密方案.Selvi 等指出文献[16]是不安全的,并提出了改进方案[17].基于身份的多重签密的形式化定义在文献[16,18]中给出.

在文献[18]中,Zhang-Xu 在 Waters 的 IBE 方案[6]和 Paterson-Schuldt 的 IBS 方案[7]的基础上,提出了一个标准模型下的基于身份的多重签密方案.本文指出,该方

收稿日期:2011-04-14;修回日期:2011-07-07

案忽略了私钥随机化问题,因此无法抵抗针对多重签名的内部伪造攻击和外部攻击.Yap 在文献[19]中指出,由于文献[7]中的 IBS 方案有私钥随机化问题,验证者无法确认用户私钥中使用的随机数是 Private Key Generator (PKG)颁发的,因此不适合直接用于构造多重签名方案,但是文献[19]并没有给出改进的方案.

对于基于身份的密码体系,在解密时,私钥随机化不会带来问题,事实上,解密私钥无需随机化.但是在签名时,如果部分私钥以某种形式公开,则可能会带来安全性上的风险,因为公开的部分私钥可能会被随机化.本文在文献[6,7]的基础上,对文献[18]做了改进,提出了一个标准模型下的基于身份的多重签密方案,将解密私钥和签名私钥分开,其中签名私钥无法随机化,因此可以抵抗针对多重签名的私钥随机化攻击.同时,我们的方案还可以抵抗内部泄漏攻击,对聚合者之外的签名者,即使他泄露了使用的明文和随机数,也无法使第三者可以通过解签密验证.

我们的方案的安全性基于标准的判定性双线性 Diffie-Hellman (the Decisional Bilinear Diffie-Hellman, DBDH)假设和计算性 Diffie-Hellman(the Computational Diffie-Hellman, CDH)假设.

2 Zhang-Xu 的多重签密方案简介及分析

2.1 Zhang-Xu 的方案简介

Zhang-Xu 在文献[18]中介绍了一个标准模型下的基于身份的多重签密方案.

Setup 设 p 是一个大素数, G 和 G_T 是两个阶为 p 的乘法循环群, $e: G\times G\rightarrow G_T$ 为双线性映射.随机选择 G 的生成元 g,以及 $\alpha\in_R Z_p^*$,令 $g_1=g^\alpha$,并随机选择 $g_2\in G$.此外,随机选择 $u', m'\in G$,以及长度分别为 n_u 与 n_m 的向量 $\boldsymbol{U}=\{u_i\}$ 与 $\boldsymbol{M}=\{m_i\}$,其中 $u_i, m_i\in_R G$.再定义两个 Hash 函数 $H_1: G_T\rightarrow\{0,1\}^{l_t}$, $H_2: \{0,1\}^{l_t}\times G_T\rightarrow\{0,1\}^{n_m}$,其中 l_t 为明文的长度.则公共参数为 $PK=(g, g_1, g_2, e, u', \boldsymbol{U}, m', \boldsymbol{M}, H_1, H_2)$,主密钥 MK 为 α.

KeyGen 该算法的输入为身份 u,主密钥 MK 和公共参数 PK,返回 u 的私钥.设 u 是一个用于表示身份的长为 n_u 的比特字符串,令 $u[i]$表示身份 u 的 i 个比特,定义 $U'\subset\{1,\cdots,n_u\}$为满足 $u[i]=1$ 的序号 i 的集合.定义 $W(u)=u'\prod_{i\in U'}u_i$.随机选择 $r_u\in Z_p$,计算私钥 $D_u=(D_{u,1}, D_{u,2})=(g^{r_u}, g_2^\alpha\cdot W(u)^{r_u})$.

MultiSigncrypt 一组发送者 $A_j(j=1,\cdots,n)$对消息 m 做多重签密,接收者为 B.

每个发送者 A_j 随机选择 $r_j\in Z_p$,计算:

(1) $w_j=(e(g_1,g_2)\cdot e(D_{B,1}, W(B)))^{r_j}$,将 w_j 广播给其它发送者.

(2)发送者 A_j 计算 $\sigma_{j,1}=g^{r_j}, \sigma_{j,2}=D_{A_j,1}, w=\prod_{j=1}^{n}w_j$, $M=H_2(m\parallel w)$.

(3)设 M 的长度为 n_m, $M[i]$表示 M 的第 i 个比特,定义 $M'\subset\{1,\cdots,n_m\}$为满足 $M[i]=1$ 的序号 i 的集合.定义 $V(M)=m'\prod_{i\in M'}m_i$.发送者 A_j 计算 $\sigma_{j,3}=D_{A_j,2}\cdot V(M)^{r_j}$.发送者 A_j 将 $(\sigma_{j,1},\sigma_{j,2},\sigma_{j,3})$发送给聚合者($A_j$ 之一).

(4)聚合者计算 $c=m\oplus H_1(w)$, $\sigma_1=\prod_{j=1}^{n}\sigma_{j,1}$, $\sigma_2=\{\sigma_{j,2}\mid j=1,\cdots,n\}$, $\sigma_3=\prod_{j=1}^{n}\sigma_{j,3}$.

最终输出多重签密数据 $\sigma=(c,\sigma_1,\sigma_2,\sigma_3)$.

Unsigncrypt 接收者 B 计算 $w=e(\sigma_1, D_{B,2})$, $m=c\oplus H_1(w)$, $M=H_2(m\parallel w)$,并验证下面的等式是否成立,若成立则接受多重签密数据,否则拒绝多重签密数据.

$$\frac{e(\sigma_3,g)}{\left(\prod_{j=1}^{n}e(W(A_j),\sigma_{j,2})\right)\cdot e(V(M),\sigma_1)}=e(g_1,g_2)^n \tag{1}$$

2.2 Zhang-Xu 的方案分析

Zhang-Xu 的方案[18]并不满足多重签名的特性,我们采用文献[19]中的方法来攻击该方案.当发送者知道接收者的 $D_{B,1}$(接收者的 $D_{B,1}$无需保密)时,有如下的内部伪造攻击和外部攻击.

2.2.1 内部伪造攻击

任何一个不诚实的发送者可以在未授权的情况下伪造包含他人的多重签密数据.设敌手为 A_1,其私钥为 D_{A_1}.在不知道发送者 A_2 的私钥的情况下, A_1 可以伪造包含 A_2 的多重签密数据:

(1) A_1 随机选择 $r_{A_2}, r_1\in Z_p^*$,计算 $w_1=(e(g_1,g_2)\cdot e(D_{B,1}, W(B)))^{r_1}$,令 $w^*=w_1$,计算 $c=m\oplus H_1(w^*)$, $M=H_2(m\parallel w^*)$.

(2) A_1 计算 $D'_{A_1,1}=(D_{A_1,1})^2=g^{2r_{A_1}}$, $D'_{A_1,2}=(D_{A_1,2})^2=g_2^{2\alpha}\cdot W(A_1)^{2r_{A_1}}$.

(3) A_1 计算 $c^*=c, \sigma_1^*=g^{r_1}, \sigma_{1,2}^*=D'_{A_1,1}=g^{2r_{A_1}}, \sigma_{2,2}^*=g^{r_{A_2}}, \sigma_3^*=D'_{A_1,2}\cdot W(A_2)^{r_{A_2}}\cdot V(M)^{r_1}=g_2^{2\alpha}\cdot W(A_1)^{2r_{A_1}}\cdot W(A_2)^{r_{A_2}}\cdot V(M)^{r_1}$.

则 $\sigma^*=(c^*,\sigma_1^*,\sigma_2^*,\sigma_3^*)$是一个包含 A_2 的成功的伪造.在解签密时,接收者 B 计算:

$$\begin{aligned}w&=e(\sigma_1^*, D_{B,2})=e(g^{r_1}, g_2^\alpha\cdot W(B)^{r_B})\\&=(e(g_1,g_2)\cdot e(g^{r_B}, W(B)))^{r_1}=w_1=w^*\end{aligned}$$

因此 B 可计算出 $m=c^*\oplus H_1(w^*)$, $M=H_2(m\parallel$

w^*),并通过如下验证:

$$\frac{e(\sigma_3^*, g)}{\left(\prod_{j=1,2} e(W(A_j), \sigma_{j,2}^*)\right) \cdot e(V(M), \sigma_1^*)}$$
$$= \frac{e(g_2^{2\alpha} \cdot W(A_1)^{2r_{A_1}} \cdot W(A_2)^{r_{A_2}} \cdot V(M)^{r_1}, g)}{e(W(A_1), g^{2r_{A_1}}) \cdot e(W(A_2), g^{r_{A_2}}) \cdot e(V(M), g^{r_1})}$$
$$= e(g_1, g_2)^2$$

2.2.2 外部攻击

对于聚合者,只要有一个用户的合法签密数据,就可以在未授权的情况下伪造包含任意用户的多重签密数据.假设聚合者知道发送者 A_1 的合法签密数据,在不知道发送者 A_2 的私钥的情况下,聚合者可以伪造包含 A_2 的多重签密数据.攻击方案如下:

(1)A_1 正常计算 w_1,随机选择 $r_1 \in Z_p^*$,计算 $w_1 = (e(g_1, g_2) \cdot e(D_{B,1}, W(B)))^{r_1}$.

(2)聚合者在收到 w_1 后,将 w_1 作为 w_2 发回给 A_1,则 A_1 正常计算 $w^* = w_1 w_2 = w_1^2$,$\sigma_{1,1} = g^{r_1}$,$\sigma_{1,2} = D_{A_1,1} = g^{r_{A_1}}$,$\sigma_{1,3} = D_{A_1,2} \cdot V(M)^{r_1} = g_2^{\alpha} \cdot W(A_1)^{r_{A_1}} \cdot V(M)^{r_1}$.

(3)聚合者收到 A_1 发送过来的$(\sigma_{1,1}, \sigma_{1,2}, \sigma_{1,3})$,计算 $c = m \oplus H_1(w^*)$,$M = H_2(m \| w^*)$.

(4)聚合者随机选取 $r_{A_2} \in Z_p^*$,计算

$c^* = c$,$\sigma_1^* = (\sigma_{1,1})^2 = g^{2r_1}$,$\sigma_{1,2}^* = \sigma_{1,2}^2 = g^{2r_{A_1}}$,$\sigma_{2,2}^* = g^{r_{A_2}}$,

$\sigma_3^* = (\sigma_{1,3})^2 \cdot W(A_2)^{r_{A_2}} = g_2^{2\alpha} \cdot W(A_1)^{2r_{A_1}} \cdot V(M)^{2r_1} \cdot W(A_2)^{r_{A_2}}$.

则 $\sigma^* = (c^*, \sigma_1^*, \sigma_2^*, \sigma_3^*)$是一个包含 A_2 的成功的伪造.在解签密时,接收者 B 计算:

$$w = e(\sigma_1^*, D_{B,2}) = e(g^{2r_1}, g_2^{\alpha} \cdot W(B)^{r_B})$$
$$= (e(g_1, g_2) \cdot e(g^{r_B}, W(B)))^{2r_1} = w_1^2 = w^*$$

因此 B 可计算出 $m = c^* \oplus H_1(w^*)$,$M = H_2(m \| w^*)$,并通过验证:

$$\frac{e(\sigma_3^*, g)}{\left(\prod_{j=1,2} e(W(A_j), \sigma_{j,2}^*)\right) \cdot e(V(M), \sigma_1^*)}$$
$$= \frac{e(g_2^{2\alpha} \cdot W(A_1)^{2r_{A_1}} \cdot V(M)^{2r_1} \cdot W(A_2)^{r_{A_2}}, g)}{e(W(A_1), g^{2r_{A_1}}) \cdot e(W(A_2), g^{r_{A_2}}) \cdot e(V(M), g^{2r_1})}$$
$$= e(g_1, g_2)^2$$

2.2.3 内部泄露攻击

Zhang-Xu 的方案[18]无法抵抗内部泄露攻击.任何一个发送者都知道(w, m),如果某一个发送者将(w, m)泄露给第三者,则第三者可通过等式(1)的验证,第三者将知道某一组发送者对消息 m 做了多重签密.引起该攻击的原因是因为该方案的所有发送者的地位是平等的.解决的思路是区分开聚合者和普通发送者.除了所有发送者都有的信息外,聚合者将使用两个随机数,一个用于随机化多重签名,另外一个用于和原有的随机数一起加密明文.文献[16,17]中的方案也无法抵抗内部泄露攻击,本文用于抵抗内部泄露攻击的方法也适用于文献[16,17]中方案.对文献[16,17]中方案的描述和改进不再单独给出.

Zhang-Xu 的方案[18]采用了 Waters 的 IBE 方案[6]与 Paterson-Schuldt 的 IBS 方案[7],但是这两个方案中的私钥是可以随机化的,Zhang-Xu 的方案忽略了私钥随机化可能带来的影响.我们注意到前两个攻击的实质都是由私钥随机化引起的.

另外,由于私钥是可以随机化的,如果解密者每次使用私钥时都随机化自己的私钥,则发送者使用的可能是接收者用过的某一个部分私钥,对于接收者而言,除非存储所有用过的私钥,否则难以解密.

实际上,该方案并不是基于身份的方案,发送者在加密时需要计算 w_j,其中使用到了 $D_{B,1}$,即发送者需要提前知道接收者 B 的某些信息,在这里 $D_{B,1}$起到了公钥的作用.

3 一个改进的基于身份的多重签密方案

本节在文献[6,7]的基础上提出了一个基于身份的多重签密方案.文献[2]指出,IBE 的私钥生成过程可以看作是一个签名算法.Paterson-Schuldt 的 IBS 方案[7]的私钥生成过程可以看作是用 Waters 的 IBS 方案[6]对身份 u 的签名.而在我们的方案中,签名私钥的生成过程可以看作是用 Waters 的 IBS 方案对身份 u 及可公开的部分私钥的签名.因此在我们的方案中,用户无法随机化签名私钥,从而可以避免敌手的私钥随机化攻击.带来的开销是与文献[6,7]相比,私钥多了一个分量.

3.1 方案构造

Setup　设 p 是一个大素数,G 和 G_T 是两个阶为 p 的乘法循环群,$e: G \times G \to G_T$ 为双线性映射.随机选择 G 的生成元 g,以及 $\alpha \in_R Z_p^*$,令 $g_1 = g^{\alpha}$,并随机选择 $g_2 \in G$.此外,随机选择 u',m',$h' \in G$,以及长度分别为 n_u,n_m 与 n_h 的向量 $\boldsymbol{U} = \{u_i\}$,$\boldsymbol{M} = \{m_i\}$ 与 $\boldsymbol{H} = \{h_i\}$,其中 $u_i, m_i, h_i \in_R G$,并要求明文 $m \in G_T$.则主密钥 MK 为 α,公共参数为 PK $= (g, g_1, g_2, e, u', \boldsymbol{U}, m', \boldsymbol{M}, h', \boldsymbol{H})$.

KeyGen　该算法的输入为身份 u,主密钥 MK 和公共参数 PK,返回 u 的私钥.PKG 随机选择 $r_u \in Z_p$,计算 $D_{u,1} = g^{r_u}$,$D_{u,2} = g_2^{\alpha} \cdot W(u)^{r_u}$.定义 $U' \subset \{1, \cdots, n_u\}$ 为满足 $u[i] = 1$ 的序号 i 的集合.定义 $W(u) = u' \prod_{i \in U'} u_i$.

设 $D_{u,1}$的比特长度为 n_h,令 $h[i]$表示 $D_{u,1}$的第 i 个比特,定义 $H' \subset \{1, \cdots, n_h\}$ 为满足 $h[i] = 1$ 的序号 i 的集合.记 $\lambda(D_{u,1}) = (u' \prod_{i \in U'} u_i) \cdot (h' \prod_{i \in H'} h_i)$,任何人在收到 $D_{u,1}$后,都可计算出 $\lambda(D_{u,1})$.PKG 计算 $D_{u,3} = g_2^{\alpha} \cdot \lambda(D_{u,1})^{r_u} = g_2^{\alpha} \cdot ((u' \prod_{i \in U'} u_i) \cdot (h' \prod_{i \in H'} h_i))^{r_u}$.用户的私钥

可表示为:

$$D_u=(D_{u,1},D_{u,2},D_{u,3})=(g^{r_u},g_2^{\alpha}\cdot W(u)^{r_u},g_2^{\alpha}\cdot\lambda(D_{u,1})^{r_u})$$

用户在收到 D_u 后,验证下式成立:

$$\frac{e(D_{u,2},g)}{e(W(u),D_{u,1})}=\frac{e(g_2^{\alpha}\cdot W(u)^{r_u},g)}{e(W(u),g^{r_u})}=e(g_1,g_2),$$

$$\frac{e(D_{u,3},g)}{e(\lambda(D_{u,1}),D_{u,1})}=\frac{e(g_2^{\alpha}\cdot\lambda(D_{u,1})^{r_u},g)}{e(\lambda(D_{u,1}),g^{r_u})}=e(g_1,g_2) \tag{2}$$

其中$(D_{u,1},D_{u,2})$为解密私钥,$(D_{u,1},D_{u,3})$为签名私钥,$(D_{u,1},D_{u,3})$可以看作是 Waters 的 IBS 方案[6]对 $u\|D_{u,1}$ 的签名,解密私钥和签名私钥共用 $D_{u,1}$.

MultiSigncrypt 设 $N=\{1,\cdots,n\}$,该函数的输入为消息 m,和 n 个发送者的集合 $U_N=\{A_1,\cdots,A_n\}$,接收者为 B,该函数返回多重签密数据 σ.每个发送者 A_j 执行下列步骤:

(1)随机选择 $r_j\in Z_p$,计算 $\theta_{j,1}=e(g_1,g_2)^{r_j}$,将 $\theta_{j,1}$ 通过一个安全信道广播给其它发送者.

(2)在收到其它发送者发送过来的 $\theta_{j,1}$后,A_j 计算 $\xi=\prod_{j\in N}\theta_{j,1}$,$\theta_{j,2}=W(B)^{r_j}$,$\theta_{j,3}=g^{r_j}$,$\theta_{j,4}=D_{A_j,1}$.

(3)记 $M=m\|\xi$,设 M 的长度为 n_m,令 $M[i]$表示 M 的第 i 个比特,定义 $M'\subset\{1,\cdots,n_m\}$为满足 $M[i]=1$ 的序号 i 的集合.定义 $V(M)=m'\prod_{i\in M'}m_i$. A_j 计算 $\theta_{j,5}=D_{A_j,3}\cdot V(M)^{r_j}$,将$(\theta_{j,2},\theta_{j,3},\theta_{j,4},\theta_{j,5})$发送给聚合者($A_j$ 之一).

在收到其它所有发送者发送过来的数据后,聚合者执行下列操作:

(1)验证$(m,\xi,\theta_{j,3},\theta_{j,4},\theta_{j,5})$满足

$$\frac{e(\theta_{j,5},g)}{e(\lambda(D_{A_j,1}),\theta_{j,4})\cdot e(V(M),\theta_{j,3})}=e(g_1,g_2).$$

(2)随机选择 $r\in Z_p$,计算 $\xi_1=e(g_1,g_2)^r$,$\sigma_{0,1}=W(B)^r$,$\sigma_{0,2}=g^r$,令 $\sigma_0=(\sigma_{0,1},\sigma_{0,2})$.

(3)随机选择 $\theta_0\in G_T$,计算 $\sigma_1=(m\|\theta_0)\cdot(\xi\cdot\xi_1)$,$\sigma_2=\prod_{j\in N}\theta_{j,2}$,$\sigma_3=\prod_{j\in N}\theta_{j,3}$,$\sigma_4=\{\sigma_{4,j}\}_{j\in N}=\{\theta_{j,4}\}_{j\in N}=\{D_{A_j,1}\}_{j\in N}$,$\sigma_5=\theta_0\cdot\prod_{j\in N}\theta_{j,5}$.

最后输出多重签密数据 $\sigma=(U_N,\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$.

Unsigncrypt 该函数的输入为 σ,返回是否接受多重签密数据.接收者 B 首先解析σ,执行下列操作:

(1)接收者可计算出

$$\xi_1=\frac{e(D_{B,2},\sigma_{0,2})}{e(D_{B,1},\sigma_{0,1})}=\frac{e(g_2^{\alpha}\cdot W(B)^{r_B},g^r)}{e(g^{r_B},W(B)^r)}=e(g_1,g_2)^r,$$

$$\xi=\frac{e(D_{B,2},\sigma_3)}{e(D_{B,1},\sigma_2)}=\frac{e(D_{B,2},\prod_{j\in N}\theta_{j,3})}{e(D_{B,1},\prod_{j\in N}\theta_{j,2})}$$

$$=\prod_{j\in N}\frac{e(D_{B,2},g^{r_j})}{e(D_{B,1},W(B)^{r_j})}=\prod_{j\in N}\frac{e(g_2^{\alpha}\cdot W(B)^{r_B},g^{r_j})}{e(g^{r_B},W(B)^{r_j})}$$

$$=\prod_{j\in N}e(g_2^{\alpha},g)^{r_j}=\prod_{j\in N}e(g_1,g_2)^{r_j}$$

接收者计算 $m\|\theta_0=\sigma_1\cdot(\xi\cdot\xi_1)^{-1}$,则可以得到发送者签名的明文 $M=m\|\xi$ 和θ_0.

(2)接收者验证下述等式是否成立,若成立则接受多重签密数据,否则拒绝多重签密数据.

$$\frac{e(\sigma_5/\theta_0,g)}{(\prod_{j\in N}e(\lambda(D_{A_j,1}),\sigma_{4,j}))\cdot e(V(M),\sigma_3)}=e(g_1,g_2)^n \tag{3}$$

在本方案中,聚合者与普通发送者是有区别的.

为了提高性能,可以使用 Hash 函数 $H_1:\{0,1\}^*\to G_1$,$H_2:G_1\to G_1$,$H_3:G_2\times G_2\to G_2$ 分别替换

$$W(u)=u'\prod_{i\in U'}u_i,\ h'\prod_{i\in H'}h_i,\ V(M)=m'\prod_{i\in M'}m_i$$

即可.

3.2 正确性

接收者 B 可计算出:

$$\begin{aligned}\sigma_1\cdot(\xi\cdot\xi_1)^{-1}&=((m\|\theta_0)\cdot e(g_1,g_2)^r\cdot\prod_{j\in N}e(g_1,g_2)^{r_j})\\&\quad\cdot(e(g_1,g_2)^r\cdot\prod_{j\in N}e(g_1,g_2)^{r_j})^{-1}\\&=m\|\theta_0\end{aligned}$$

则等式(3)的正确性可按如下流程验证:

$$\frac{e(\sigma_5/\theta_0,g)}{\left(\prod_{j\in N}e(\lambda(D_{A_j,1}),\sigma_{4,j})\right)\cdot e(V(M),\sigma_3)}$$

$$=\frac{e(\prod_{j\in N}\theta_{j,5},g)}{\left(\prod_{j\in N}e(\lambda(D_{A_j,1}),D_{A_j,1})\right)\cdot e\left(V(M),\prod_{j\in N}g^{r_j}\right)}$$

$$=\frac{\prod_{j\in N}e(D_{A_j,3}\cdot V(M)^{r_j},g)}{\left(\prod_{j\in N}e(\lambda(D_{A_j,1}),g^{r_{A_j}})\right)\cdot\prod_{j\in N}e(V(M),g^{r_j})}$$

$$=\prod_{j\in N}\frac{e(g_2^{\alpha}\cdot\lambda(D_{A_j,1})^{r_{A_j}},g)}{e(\lambda(D_{A_j,1}),g^{r_{A_j}})}$$

$$=\prod_{j\in N}e(g_2^{\alpha},g)=e(g_1,g_2)^n$$

4 安全性分析

4.1 签名私钥的不可伪造性

在本方案中,$(D_{u,1},D_{u,2})$为解密私钥,$(D_{u,1},D_{u,3})$为签名私钥.$(D_{u,1},D_{u,3})$可以看作是 Waters 的 IBS 方案[6]对 $u\|D_{u,1}$ 的签名,因此无法被随机化.在解密时,$(D_{u,1},D_{u,2})$是否随机化对安全没有影响,也无需随机化.在选择消息攻击模型下,本方案的签名私钥是强不可伪造的,即使敌手已经有了一对合法的签名私钥,也

无法构造出新的签名私钥.

定理 1　对于本方案,在选择消息攻击模型下,签名私钥是强不可伪造的.且对用户 A,已知自己的签名私钥$(D_{A,1}, D_{A,3})$,在不知道用户 B 的签名私钥时,无法伪造$(D^*_{A,1}\cdot D^*_{B,1}, D^*_{A,3}\cdot D^*_{B,3})$.

证明　敌手已知签名私钥$(D_{u,1}, D_{u,3})$,假设敌手可以伪造签名私钥$(D^*_{u,1}, D^*_{u,3})$.

定义 $s' = u'\cdot h'$,构造长度为 $n_u + n_h$ 的向量 $\boldsymbol{S} = \{s_j\}$,其中当 $1\leqslant j\leqslant n_u$ 时,令 $s_j = u_j$,否则当 $n_u < j\leqslant n_u + n_h$ 时,令 $s_j = h_{j-n_u}$.此时 $u \parallel D_{u,1}$为长为 $n_u + n_h$ 的比特字符串,令 $s[j]$表示 $u \parallel D_{u,1}$的第 j 个比特,定义 $S_u \subset \{1,\cdots, n_u + n_h\}$为满足 $s[j] = 1$ 的序号 j 的集合.则有 $(u'\prod_{i\in U'} u_i)\cdot(h'\prod_{i\in H'} h_i) = s'\prod_{j\in S_u} s_j$.即 PKG 颁发的签名私钥相当于

$$(D_{u,1}, D_{u,3}) = (g^{r_u}, g_2^{\alpha}\cdot(s'\prod_{j\in S_u} s_j)^{r_u})$$

显然,$(D_{u,1}, D_{u,3})$是 Waters 的 IBS 方案[6]对 $u \parallel D_{u,1}$的签名.

当 $D^*_{u,1}\neq D_{u,1}$时,伪造$(D^*_{u,1}, D^*_{u,3})$相当于敌手对新的消息 $u \parallel D^*_{u,1}$伪造签名.由 Waters 的 IBS 方案是存在不可伪造的,因此 $D^*_{u,1}\neq D_{u,1}$不可能发生.

当 $D^*_{u,1} = D_{u,1} = g^{r_u}$时,对于$(D^*_{u,1}, D^*_{u,3})$,由于 $h'\prod_{i\in H'} h_i$ 的值是由 $D_{u,1}$决定的,因此 $e(\lambda(D_{u,1}), \sigma_{4,j}) = e((u'\prod_{i\in U'} u_i)\cdot(h'\prod_{i\in H'} h_i), g^{r_u})$保持不变.由等式(2),可知 $e(D^*_{u,3}, g) = e(D_{u,3}, g)$,即 $D^*_{u,3} = D_{u,3}$.综上所述,本方案的签名私钥是强不可伪造的.

对于用户 A,已知自己的签名私钥为$(D_{A,1}, D_{A,3})$,且不知道用户 B 的签名私钥,假设用户 A 可以伪造出$(D^*_{A,1}\cdot D^*_{B,1}, D^*_{A,3}\cdot D^*_{B,3})$.由签名私钥是强不可伪造的,有$(D^*_{A,1}, D^*_{A,3}) = (D_{A,1}, D_{A,3})$.因此用户 A 伪造出$(D^*_{A,1}\cdot D^*_{B,1}, D^*_{A,3}\cdot D^*_{B,3})$等价于 A 伪造出$(D^*_{B,1}, D^*_{B,3})$,由签名私钥的强不可伪造性,用户 A 伪造出$(D^*_{B,1}, D^*_{B,3})$是不可能的.即用户 A 无法伪造$(D^*_{A,1}\cdot D^*_{B,1}, D^*_{A,3}\cdot D^*_{B,3})$.

4.2　机密性

在 IND-CCA2 的攻击模型下,在不知道接收者私钥的情况下,给定两个等长的消息 m_1 和 m_2,敌手无法区分这两个消息的密文.

定理 2　在 IND-CCA2 攻击模型下,如果敌手可以攻破本方案,则可以构造一个多项式有界的模拟器,以不可忽略的优势解决 DBDH 问题.

证明　假设敌手可以攻破本方案,则我们利用敌手来构造模拟器,可以解决 DBDH 问题.我们的证明基于文献[6,7]中的思想.

挑战者随机选择 $\mu\in\{0,1\}$,并随机选择 $a, b, c, z\in Z_p$,对于(g^a, g^b, g^c, Z),如果 $\mu = 0$,则挑战者令 $Z = e(g,g)^{abc}$,否则令 $Z = e(g,g)^z$.挑战者将(g^a, g^b, g^c, Z)发送给模拟器.

Setup　模拟器收到(g^a, g^b, g^c, Z),模拟器的目标是判断 Z 是否等于 $e(g,g)^{abc}$.

假设敌手最多询问 q_K 次 KeyGen, q_S 次 MultiSigncrypt 和 q_U 次 Unsigncrypt 运算.令 $l_m = 2q_S$, $l_u = 2(q_K + q_S + q_U)$,设 $l_u(n_u + 1) < p$, $l_m(n_m + 1) < p$(l_u, l_m 的定义参考文献[7]),模拟器随机选择:

(1)两个整数 k_u 和 k_m,其中 $0\leqslant k_u\leqslant n_u$, $0\leqslant k_m\leqslant n_m$.

(2)整数 $x'\in Z_{l_u}$和一个 n_u 维向量 $\boldsymbol{X} = (x_i)(x_i\in Z_{l_u})$.

(3)整数 $z'\in Z_{l_m}$和一个 n_m 维向量 $\boldsymbol{Z} = (z_i)(z_i\in Z_{l_m})$.

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

(5)整数 $t'\in Z_p$,一个 n_h 维向量 $\boldsymbol{T} = (t_i)(t_i\in Z_p)$.

关于身份 u,消息 $M = m \parallel \xi$ 和 $D_{u,1}$的函数定义如下:

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

$$J(u) = y' + \sum_{i\in U'} y_i,$$

$$K(M) = -l_m k_m + z' + \sum_{i\in M'} z_i,$$

$$L(M) = w' + \sum_{i\in M'} w_i,$$

$$T(D_{u,1}) = t' + \sum_{i\in H'} h_i$$

模拟器设置下列公共参数,令 $g_1 = g^a$, $g_2 = g^b$, $u' = g_2^{-l_u k_u + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}(1\leqslant i\leqslant n_u)$, $m' = g_2^{-l_m k_m + z'} g^{w'}$, $m_i = g_2^{z_i} g^{w_i}(1\leqslant i\leqslant n_m)$, $h' = g^{t'}$, $h_i = g^{t_i}(1\leqslant i\leqslant n_h)$.则对于任意的身份 u,消息 $M = m \parallel \xi$ 和 $D_{u,1}$,有:

$$W(u) = u'\prod_{i\in U'} u_i = g_2^{F(u)} g^{J(u)},$$

$$V(M) = m'\prod_{i\in M'} m_i = g_2^{K(M)} g^{L(M)},$$

$$h'\prod_{i\in H'} h_i = g^{T(D_{u,1})}$$

模拟器将公共参数发送给敌手.

第一阶段　在第一阶段,可以做 KeyGen 询问,MultiSigncrypt 询问和 Unsigncrypt 询问.

KeyGen 询问　当敌手询问用户 u 的私钥时,在不知道主密钥的情况下,模拟器按如下方式模拟 D_u.

当 $F(u)\neq 0 \bmod p$ 时,模拟器随机选择 $r'_u\in Z_p$,计算

$$D_{u,1} = g_1^{-1/F(u)}\cdot g^{r'_u},$$

$$D_{u,2} = g_1^{-J(u)/F(u)}\cdot(g_2^{F(u)} g^{J(u)})^{r'_u},$$

$$D_{u,3} = g_1^{-J(u)/F(u)}\cdot(g_2^{F(u)} g^{J(u)})^{r'_u}\cdot g_1^{-T(D_{u,1})/F(u)}\cdot(g^{T(D_{u,1})})^{r'_u},$$

令 $r_u = r'_u - a/F(u)$,则有:

$$D_{u,1} = g_1^{-1/F(u)} \cdot g^{r'_u} = g^{r'_u - a/F(u)} = g^{r_u},$$

$$\begin{aligned} D_{u,2} &= g_1^{-J(u)/F(u)} \cdot (g_2^{F(u)} g^{J(u)})^{r'_u} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)})^{-a/F(u)} \cdot (g_2^{F(u)} g^{J(u)})^{r'_u} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)})^{r'_u - a/F(u)} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)})^{r_u} \\ &= g_2^a \cdot W(u)^{r_u} \end{aligned}$$

$$\begin{aligned} D_{u,3} &= g_1^{-J(u)/F(u)} \cdot (g_2^{F(u)} g^{J(u)})^{r'_u} \cdot g_1^{-T(D_{u,1})/F(u)} \\ &\quad \cdot (g^{T(D_{u,1})})^{r'_u} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)})^{-a/F(u)} \cdot (g_2^{F(u)} g^{J(u)})^{r'_u} \\ &\quad \cdot (g^{T(D_{u,1})})^{-a/F(u)} \cdot (g^{T(D_{u,1})})^{r'_u} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)})^{r'_u - a/F(u)} \cdot (g^{T(D_{u,1})})^{r'_u - a/F(u)} \\ &= g_2^a \cdot (g_2^{F(u)} g^{J(u)} \cdot g^{T(D_{u,1})})^{r_u} \\ &= g_2^a \cdot \lambda(D_{u,1})^{r_u} \end{aligned}$$

对于敌手而言,模拟器计算的 D_u 与真正的 D_u 是不可区分的.

当 $F(u) = 0 \bmod p$ 时,上述操作无法执行,模拟器放弃.为了描述简单,当 $F(u) = 0 \bmod l_u$ 时,我们令模拟器放弃.同文献[7]分析,由 $l_u(n_u + 1) < p$,则有 $0 \leqslant l_u n_u < p$,可以得到 $-p < F(u) = -l_u k_u + x' + \sum_{i \in U'} x_i < p$,因此有 $F(u) = 0 \bmod p \Rightarrow F(u) = 0 \bmod l_u$,且有 $F(u) \neq 0 \bmod l_u \Rightarrow F(u) \neq 0 \bmod p$.上述条件可以使询问 KeyGen 不放弃.

MultiSigncrypt 询问 在任何时候,敌手可以对消息 m,发送者集合 U_N,接收者 B 做 MultiSigncrypt 询问.如果对于所有发送者 $A_j \in U_N$,都有 $F(A_j) \neq 0 \bmod l_u$,模拟器可以询问 KeyGen 得到 D_{A_j},并按原始方案执行 MultiSigncrypt,将结果返回给敌手.如果存在发送者 $A_j \in U_N$,使得 $F(A_j) = 0 \bmod l_u$,则模拟器放弃.

Unsigncrypt 询问 任何时候,敌手可以对发送者集合 U_N,接收者 B 的多重签密数据 σ 做 Unsigncrypt 询问.如果 $F(B) \neq 0 \bmod l_u$,模拟器可以询问 KeyGen 得到 D_B,并按原始方案执行 Unsigncrypt,将结果返回给敌手.否则模拟器放弃.

Challenge 在经过多项式界次数的询问后,敌手选择发送者集合 $U_N^* = \{A_1^*, \cdots, A_n^*\}$,接收者 B^*.如果在第一阶段,询问过 B^* 的私钥,则模拟器失败.敌手提交两个等长的消息 m_0 和 m_1,发送者集合 U_N^*,接收者 B^* 给模拟器.其中对于所有的 $A_j^* \in U_N^*$,要求 $F(A_j^*) \neq 0 \bmod l_u$,否则模拟器放弃.模拟器随机选择 $\nu \in \{0,1\}$,如果 $K(M_\nu) \neq 0 \bmod p$,则模拟器放弃,其中 $M_\nu = m_\nu \| \xi$.如果 $F(B^*) \neq 0 \bmod p$,模拟器放弃.否则,模拟器构造多重签密数据 $\sigma^* = (U_N^*, \sigma_0^*, \sigma_1^* = (m_\nu \| \theta_0^*) \cdot Z, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$.

当 $\mu = 0$ 时,此时 $Z = e(g,g)^{abc}$.由于对于所有的 $A_j^* \in U_N^*$,有 $F(A_j^*) \neq 0 \bmod l_u$,模拟器询问所有发送者的私钥,然后按原始方案执行即可,其中令 $\sigma_{0,2}^* = g^c / \sigma_3^*$,即 $g^c = \sigma_{0,2}^* \cdot \sigma_3^* = g^r \cdot \prod_{j \in N} g^{r_j} = g^{r + \sum_{j \in N} r_j}$,此时 σ^* 是合法的多重签密数据.

当 $\mu = 1$ 时,此时 $Z = e(g,g)^z$,其中 $z \in {}_R Z_p$,则 $\sigma_1^* = (m_\nu \| \theta_0^*) \cdot e(g_1, g_2)^z$ 为 G_2 中的随机元素.

第二阶段 第二阶段的操作同第一阶段,除了不可以询问接收者 B^* 的私钥,以及 B^* 挑战的多重签密数据 σ^*.

Guess 敌手输出对 ν 的猜测 ν'.如果 $\nu' = \nu$,则模拟器输出 $\mu' = 0$,即输入为 $(g^a, g^b, g^c, e(g,g)^{abc})$.否则模拟器输出 $\mu' = 1$,即输入为 $(g^a, g^b, g^c, e(g,g)^z)$.

模拟器成功的概率分析 假设敌手能够以 ε 的概率攻破本方案.设模拟器不放弃的概率为 $\Pr[\overline{\text{abort}}]$.模拟器不放弃的概率与文献[18]的分析相同,为 $\Pr[\overline{\text{abort}}] \geqslant \dfrac{1}{8 q_S (q_K + q_S + q_U)(n_u + 1)(n_m + 1)}$.

当 $\mu = 1$ 时,敌手无法得到 ν 的任何信息,则无论模拟器是否放弃,都有 $\Pr[\nu \neq \nu'] = \dfrac{1}{2}$.而当 $\nu' \neq \nu$ 时,模拟器输出 $\mu' = 1$.因此有 $\Pr[\mu = \mu' \mid \mu = 1] = \dfrac{1}{2}$.

当 $\mu = 0$ 时,敌手得到 m_ν 的密文.设 $\eta = \Pr[\overline{\text{abort}}]$.Waters 在文献[6]中指出,此时模拟器猜测成功的概率 $\Pr[\mu = \mu' \mid \mu = 0] \geqslant \dfrac{1}{2} + \dfrac{3}{4}\eta\varepsilon$.

模拟器解决 DBDH 问题的优势为:

$$\frac{1}{2}\Pr[\mu = \mu' \mid \mu = 0] + \frac{1}{2}\Pr[\mu = \mu' \mid \mu = 1] - \frac{1}{2} \geqslant \frac{1}{2}\left(\frac{1}{2} + \frac{3}{4}\eta\varepsilon\right) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} = \frac{3}{8}\eta\varepsilon$$

因此,模拟器解决 DBDH 问题的优势至少为

$$\frac{3\varepsilon}{64 q_S (q_K + q_S + q_U)(n_u + 1)(n_m + 1)}$$

4.3 不可伪造性

在选择消息攻击模型下,基于身份的多重签名的存在不可伪造性是指:如果至少有一个发送者的私钥不知道,且没有询问过该发送者对 m 做的签名,则敌手不能伪造消息签名对 (m, σ).

定理 3 在选择消息攻击模型下,如果敌手可以在存在不可伪造安全模型下攻破本方案,则可以构造一个多项式有界的模拟器,以不可忽略的优势解决 CDH 问题.

证明 假设敌手可以攻破本方案,则我们利用敌手来构造模拟器,可以解决 CDH 问题.挑战者生成随机

的(g, g^a, g^b)发送给模拟器.

Setup 模拟器收到(g, g^a, g^b),令 $g_1 = g^a, g_2 = g^b$,目标是计算出 g^{ab}.模拟器设置公共参数的方法同定理2.

敌手可以询问多项式界次数的 KeyGen, MultiSigncrypt 和 Unsigncrypt.模拟器回答询问的方法同定理2.

最后,如果模拟器不放弃,敌手输出关于消息 m^*,发送者集合 U_N^* 与接收者 B^* 的伪造的多重签密数据 $\sigma^* = (U_N^*, \sigma_0^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$,其中没有用 m^* 询问过关于发送者集合 U_N^* 与接收者 B^* 的 MultiSigncrypt 运算.同时模拟器可以解签密 σ^* 得到 m^*, θ_0^*, ξ^* 与 ξ_1^*,则模拟器得到 $M^* = m^* \| \xi^*$.

如果对所有的 A_j^*,都有 $F(A_j^*) \neq 0 \bmod p$,或 $K(M^*) \neq 0 \bmod p$,则模拟器放弃.否则,如果存在 A_j^* 使得 $F(A_j^*) = 0 \bmod p$,且 $K(M^*) = 0 \bmod p$,此时模拟器的操作如下:

设 $N_1 = \{j \mid j \in N, F(A_j^*) \neq 0\}$,则对所有的 $j \in N_1$,模拟器知道 A_j^* 的签名私钥$(D_{A_j^*,1}, D_{A_j^*,3})$.且由定理1,签名私钥是强不可伪造的,因此对所有的 $j \in N_1$,有 $\sigma_{4,j}^* = D_{A_j^*,1} = g^{r_{A_j^*}}$.设 $N_2 = N - N_1$,即 $N_2 = \{j \mid j \in N, F(A_j^*) = 0\}$.设 $|N_1| = d_1, |N_2| = d_2$,显然 $d_1 + d_2 = n$.由安全模型定义,有 $d_2 \geqslant 1$.此时,模拟器可计算出:

$$\prod_{j \in N_1} \frac{e(D_{A_j^*,3}, g)}{e(\lambda(D_{A_j^*,1}), \sigma_{4,j}^*)} = \prod_{j \in N_1} \frac{e(g_2^a \cdot \lambda(D_{A_j^*,1})^{r_{A_j^*}}, g)}{e(\lambda(D_{A_j^*,1}), g^{r_{A_j^*}})} = e(g_1, g_2)^{d_1}$$

设 $\sigma'_5 = \theta_0^* \cdot \prod_{j \in N_1} D_{A_j^*,3}$,模拟器可计算出 $\sigma''_5 = \frac{\sigma_5^*}{\sigma'_5} = \frac{\sigma_5^*}{\theta_0^* \cdot \prod_{j \in N_1} D_{A_j^*,3}}$.由等式(3)成立,可知:

$$\frac{e(\sigma''_5, g)}{(\prod_{j \in N_2} e(\lambda(D_{A_j^*,1}), \sigma_{4,j}^*)) \cdot e(V(M), \sigma_3^*)}$$

$$= \frac{e(\sigma''_5, g)}{(\prod_{j \in N_2} e(W(A_j^*) \cdot (h' \prod_{i \in H'} h_i), \sigma_{4,j}^*)) \cdot e(V(M), \sigma_3^*)}$$

$$= \frac{e(\sigma''_5, g)}{(\prod_{j \in N_2} e(g^{J(A_j^*)+T(D_{A_j^*,1})}, \sigma_{4,j}^*)) \cdot e(g^{L(M)}, \sigma_3^*)}$$

$$= \frac{e(\sigma''_5, g)}{(\prod_{j \in N_2} e(g, (\sigma_{4,j}^*)^{J(A_j^*)+T(D_{A_j^*,1})})) \cdot e(g, (\sigma_3^*)^{L(M)})}$$

$$= e\left(\frac{\sigma''_5}{(\prod_{j \in N_2} (\sigma_{4,j}^*)^{J(A_j^*)+T(D_{A_j^*,1})}) \cdot (\sigma_3^*)^{L(M)}}, g\right)$$

$$= e(g_1, g_2)^{d_2} = e(g^{ab}, g)^{d_2}$$

因此可计算出 $\left(\frac{\sigma''_5}{(\prod_{j \in N_2} (\sigma_{4,j}^*)^{J(A_j^*)+T(D_{A_j^*,1})}) \cdot (\sigma_3^*)^{L(M)}}\right)^{1/d_2} = g^{ab}$. 成功解决 CDH 问题,矛盾.

假设敌手能够以 ε 的概率攻破本方案.模拟器不放弃的概率分析与文献[18]的机密性安全证明中的模拟器不放弃的概率分析类似,则模拟器成功解决 CDH 问题的概率至少为 $\frac{\varepsilon}{8 q_S (q_K + q_S + q_U)(n_u + 1)(n_m + 1)}$.

4.4 对内部泄漏攻击的抵抗

对除了聚合者之外的发送者,即使他泄露了使用的随机数和 $M = m \| \xi$,也无法使第三者能够通过解签密验证.因为在签密数据中,m 是用 $\xi \cdot \xi_1$ 加密的,同时,在 σ_5 中使用了随机数 θ_0,只有聚合者和接收者才知道 ξ_1 和 θ_0.因此即使第三者得到了某一个发送者泄漏的 $M = m \| \xi$,也无法通过等式(3)的签名验证.

5 结论

本文指出了在 Zhang-Xu 的基于身份的多重签密方案[18]中,由于忽略了 Waters 的 IBE 方案[6]与 Paterson-Schuldt 的 IBS 方案[7]中的私钥随机化问题,因此无法抵抗私钥随机化攻击.本文在文献[6,7]的基础上提出了一个标准模型下的基于身份的多重签密方案,其中签名私钥无法随机化,因此可以抵抗私钥随机化攻击.同时,我们的多重签密方案还可以抵抗内部泄漏攻击.

参考文献

[1] A Shamir. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology-CRYPTO 1984 [C]. Berlin: Springer, 1984. 47 – 53.

[2] D Boneh, M Franklin. Identity-based encryption from the Weil Pairing [A]. Advances in Cryptology-CRYPTO 2001 [C]. Berlin: Springer, 2001. 213 – 229.

[3] D Boneh, X Boyen. Efficient selective-ID secure identity-based encryption without random oracles [A]. Advances in Cryptology-EUROCRYPT 2004 [C]. Berlin: Springer, 2004. 223 – 238.

[4] F Hess. Efficient identity based signature schemes based on paring [A]. Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002 [C]. Berlin: Springer, 2003. 310 – 324.

[5] P S L M Barreto, B Libert, N McCullagh, J Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps [A]. Advances in Cryptology ASIACRYPT 2005 [C]. Berlin: Springer, 2005. 515 – 532.

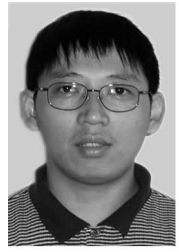
[6] B Waters. Efficient identity-based encryption without random oracles [A]. Advances in Cryptology-EUROCRYPT 2005 [C]. Berlin: Springer, 2005. 114 – 127.

[7] K G Paterson, J C N Schuldt. Efficient identity-based signatures

secure in the standard mode[A]. ACISP 2006[C]. Berlin: Springer, 2006. 207 – 222.
[8] M Bellare, T Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters' IBE scheme[A]. Advances in Cryptology-EUROCRYPT 2009 [C]. Berlin: Springer, 2009. 407 – 424.
[9] C Sato, T Okamoto, E Okamoto. Strongly unforgeable ID-based signatures without random oracles[A]. Proceedings of ISPEC 2009[C]. Berlin: Springer, 2009. 35 – 46.
[10] A Sahai, B Waters. Fuzzy identity based encryption[A]. Advances in Cryptology-EUROCRYPT 2005 [C]. Berlin: Springer, 2005. 457 – 473.
[11] Y Zheng. Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption)[A]. Advances in Cryptology-CRYPTO 1997[C]. Berlin: Springer, 1997. 165 – 179.
[12] J Baek, R Steinfeld, Y Zheng. Formal proofs for the security of signcryption[A]. PKC 2002[C]. Berlin: Springer, 2002. 80 – 98.
[13] J Malone-Lee. Identity-Based Signcryption[OL]. Cryptology ePrint Archive. Report 2002/098. Available at http://eprint.iacr.org/2002/098, 19 July, 2002.
[14] B Libert, and J Quisquator. A new identity based signcryption scheme from pairings[A]. Proceedings of the 2003 IEEE Information Theory Workshop[C]. USA: IEEE, 2003. 155 – 158.
[15] S Duan, Z Cao. Efficient and provably secure multi-receiver identity-based signcryption [A]. Proceedings of the ACISP 2006[C]. Berlin: Springer, 2006. 195 – 206.
[16] J Zhang, J Mao. A novel identity-based multi-signcryption scheme[J]. Computer Communications, 2009, 32(1), 14 – 18.
[17] S S D Selvi, S S Vivek, C P Rangan. Breaking and fixing of an identity based multi-signcryption scheme[A]. ProvSec 2009 [C]. Berlin: Springer, 2009. 61 – 75.
[18] ZHANG Bo, XU Qiu-Liang. Identity-based multi-signcryption scheme without random oracles[J]. Chinese Journal of Computers, 2010, 33(1): 103 – 110.
[19] W S Yap, S H Heng, and B M Goi. On the Security of an Identity-Based Aggregate Signature Scheme[A]. The 22nd International Conference on Advanced Information Networking and Applications-Workshops, AINAW 2008[C]. USA: IEEE, 2008. 1523 – 1528.

作者简介

张秋璞 男, 1976 年 4 月出生于河北新城. 现为中国科学院研究生院信息安全国家重点实验室博士研究生, 主要研究方向为密码学.
E-mail: qpzhang@is.ac.cn



叶顶锋 男, 1966 年 12 月出生于四川隆昌. 教授, 博士生导师. 现为中国科学院研究生院信息安全国家重点实验室博士生导师, 主要研究方向为密码分析和理论密码学.
E-mail: ydf@is.ac.cn