一种标准模型下无证书签名方案的安全性分析与改进

杨小东,王美丁,裴喜祯,李雨潼,陈春霖,麻婷春
(西北师范大学计算机科学与工程学院,甘肃兰州 730070)

摘 要: 无证书签名具有基于身份密码体制和传统公钥密码体制的优点,可解决复杂的公钥证书管理和密钥托管问题. Wu 和 Jing 提出了一种强不可伪造的无证书签名方案,其安全性不依赖于理想的随机预言机. 针对该方案的安全性,提出了两类伪造攻击. 分析结果表明,该方案无法实现强不可伪造性,并在"malicious-but-passive"的密钥生成中心攻击下也是不安全的. 为了提升该方案的安全性,设计了一个改进的无证书签名方案. 在标准模型中证明了改进的方案对于适应性选择消息攻击是强不可伪造的,还能抵抗恶意的密钥生成中心攻击. 此外,改进的方案具有较低的计算开销和较短的私钥长度,可应用于区块链、车联网、无线体域网等领域.

关键词: 无证书签名; 伪造攻击; 公钥; 私钥; 数字签名; 密码学
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2019)09-1972-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.09.022

Security Analysis and Improvement of a Certificateless Signature Scheme in the Standard Model

YANG Xiao-dong, WANG Mei-ding, PEI Xi-zhen, LI Yu-tong, CHEN Chun-lin, MA Ting-chun
(*College of Computer Science and Engineering, Northwest Normal University, Lanzhou, Gansu* 730070, *China*)

Abstract: Certificateless signature combines the advantages of identity-based cryptosystem and traditional public-key cryptosystem to solve the problems of complex public key certificate management and key escrow. Wu and Jing proposed a strongly unforgeable certificateless signature scheme whose security does not depend on the ideal random oracle. In this paper, two types of forgery attacks are proposed for the security of this scheme. The analysis results show that this scheme cannot achieve strong unforgeability and is insecure under the "malicious-but-passive" key generation center attack. To enhance the security of this scheme, an improved certificateless signature scheme is presented. The improved scheme is proved to be strongly unforgeable against adaptive chosen-message attacks and can also resist malicious key generation center attacks. In addition, the improved scheme has lower computational overhead and shorter private key length, and can be applied to blockchain, Internet of vehicles, wireless body area network and other fields.

Key words: certificateless signature; forgery attack; public key; private key; digital signature; cryptography

1 引言

在传统的数字签名方案中,系统需要庞大的计算和通信开销来支持公钥证书的生成、分发、存储、更新和撤销等管理操作[1,2]. 基于身份的签名方案简化了密钥管理[3],但存在密钥托管问题. 为了解决这些安全问题,Al-Riyami 和 Paterson[4] 提出了无证书签名体制,一个半可信的密钥生成中心(Key Generation Center, KGC)产生用户的部分私钥,用户独立生成自己的秘密值和公钥. 因此,无证书签名方案避免了复杂的证书管理及密钥托管问题,被广泛应用于无线传感器网络[5]、物联网[6]、云计算[7]等领域.

收稿日期:2018-07-21;修回日期:2018-11-13;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61662069, No. 61562077);中国博士后科学基金(No. 2017M610817);兰州市科技计划项目(No. 2013-4-22);西北师范大学青年教师科研能力提升计划项目(No. WNU-LKQN-14-7)

2003 年,Al-Riyami 和 Paterson[4] 提出了第一个无证书签名方案. 随后,Yum[8] 等给出了无证书签名方案的通用构造,Yap[9] 等设计了一个基于中介的无证书签名方案,Wang[10] 等构造了一个不需要双线性的无证书签名方案. 然而,这些方案的安全性证明依赖于理想的随机预言机,无法确保方案的现实安全性[11]. Liu[12] 等提出了一个无随机预言机的无证书签名方案,Yuan[13] 等提出了一个在标准模型中可证明安全的无证书签名方案,Canard[14] 等设计了一个标准模型下高效的无证书签名方案. 遗憾的是,这些方案仅满足存在不可伪造性,即攻击者不能伪造一个新消息的合法签名. 强不可伪造性具有更高的安全性,能保证攻击者不能伪造未签名或已签名消息的签名[15]. 因此,研究标准模型下强不可伪造的无证书签名方案具有重要的现实意义.

2016 年,Hung 等人[16] 设计了一个标准模型下的无证书签名方案(简称 Hung 方案),并证明其在适应性选择消息攻击下是强不可伪造的. 然而,Wu 等人[17] 在 2018 年指出 Hung 方案[16] 存在安全缺陷,无法抵抗“malicious-but-passive”的 KGC 攻击. 随后,Wu 等人[17] 提出了一个改进的无证书签名方案(简称 Wu 方案),并声称该方案能抵抗恶意 KGC 的伪造攻击. 本文对 Wu 方案进行了安全性分析,发现其并不满足强不可伪造性,攻击者很容易利用消息的合法签名伪造一个该消息的新签名;进一步指出 Wu 方案在“malicious-but-passive”的 KGC 攻击下是不安全的,并给出了具体的攻击方法. 针对 Wu 方案存在的安全问题,提出了一个改进的无证书签名方案,并证明其在标准模型下是强不可伪造的. 分析结果表明,新方案具有较低的计算开销和较小的私钥长度,并能抵抗恶意的 KGC 攻击.

2　预备知识

2.1　困难问题假设

计算性 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题[16]:给定三元组 $(g,g^{a},g^{\beta})\in G_1^3$,其中 $\alpha\beta\in Z_p^*$ 是未知的,计算 $g^{\alpha\beta}\in G_1$.

平方 Diffie-Hellman(Square Diffie-Hellman, Square-CDH)问题[13]:给定二元组 $(g,g^{\alpha})\in G_1^2$,其中 $\alpha\in Z_p^*$ 是未知的,计算 $g^{\alpha^2}\in G_1$.

2.2　强不可伪造的无证书签名方案的安全性定义

一个强不可伪造的无证书签名方案包含以下 6 个算法:

(1)Setup:给定安全参数 $\lambda\in Z$,该算法输出 KGC 的主密钥 msk 和系统参数 sp.

(2)UserKeyGen:给定系统参数 sp,用户独立生成自己的秘密值 $\mathrm{usk}_{\mathrm{ID}}$ 和公钥 $\mathrm{pk}_{\mathrm{ID}}$.

(3)PartialKeyGen:对于用户的身份 ID 和公钥 $\mathrm{pk}_{\mathrm{ID}}$,KGC 利用 msk 生成 ID 对应的部分私钥 $\mathrm{psk}_{\mathrm{ID}}$.

(4)SetSecKey:给定身份 ID 的 $\mathrm{usk}_{\mathrm{ID}}$ 和 $\mathrm{psk}_{\mathrm{ID}}$,用户生成自己的私钥 $\mathrm{sk}_{\mathrm{ID}}$.

(5)Sign:给定一个消息 m,签名者利用自己的私钥 $\mathrm{sk}_{\mathrm{ID}}$ 生成 m 的签名 σ.

(6)Verify:对于身份 ID、公钥 $\mathrm{pk}_{\mathrm{ID}}$ 和消息 m 的签名 σ,如果签名 σ 是合法的,输出 1;否则,输出 0.

对于一个无证书签名方案的安全性,其安全模型主要考虑以下两类攻击者[16,17]:

(1)第一类攻击者 $\mathcal{A}_1$:攻击者不能获得 KGC 的主密钥和目标用户的部分私钥,但拥有每个用户的秘密值,并能替换任意用户的公钥.

(2)第二类攻击者 $\mathcal{A}_2$:这类攻击模拟一个恶意的 KGC,其中“honest-but-curious”的 KGC 攻击者拥有 KGC 的主密钥,但无法知道目标用户的秘密值,也不能替换用户的公钥. “malicious-but-passive”的 KGC 攻击者除了“honest-but-curious”的 KGC 攻击者能力外,还能在主密钥和系统参数中添加陷门信息.

3　Wu 方案的安全性分析

3.1　Wu 方案描述

针对 Hung 方案[16] 存在的安全缺陷,Wu 和 Jing[17] 在 2018 年提出了一个改进的无证书签名方案. 具体描述如下:

(1)Setup:给定安全参数 $\lambda\in Z$,KGC 首先选择两个阶为素数 p 的循环群 G_1 和 G_2,一个 G_1 的生成元 g 和一个双线性映射 $e:G_1\times G_1\to G_2$;然后随机选择 4 个长度分别为 n_u、n_t、n_t 和 n_m 的向量 $\boldsymbol{u}=(u_i)$,$\boldsymbol{s}=(s_j)$,$\boldsymbol{t}=(t_j)$ 和 $\boldsymbol{w}=(w_k)$,其中 $u_i,s_j,t_j,w_k\in G_1$. 选择 5 个哈希函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_u}$,$H_2:\{0,1\}^*\to\{0,1\}^{n_t}$,$H_3:\{0,1\}^*\to\{0,1\}^{n_t}$,$H_4:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_5:\{0,1\}^*\to Z_p^*$. 随机选择 $g_2\in G_1$ 和 $\alpha\in Z_p^*$,计算 $g_1=g^{\alpha}$ 和 $\mathrm{msk}=g_2^{\alpha}$. 最后,KGC 秘密保存主密钥 msk,公开系统参数 $\mathrm{sp}=\{G_1,G_2,e,p,g,g_1,g_2,\boldsymbol{u},\boldsymbol{s},\boldsymbol{t},\boldsymbol{w},H_1,H_2,H_3,H_4,H_5\}$.

(2)UserKeyGen:身份为 ID 的用户机选择 $\theta_1,\theta_2\in Z_p^*$,计算 $\mathrm{pk}_{\mathrm{ID},1}=g^{\theta_1}$ 和 $\mathrm{pk}_{\mathrm{ID},2}=g^{\theta_2}$,并设置秘密值 $\mathrm{usk}_{\mathrm{ID}}=(\theta_1,\theta_2)$ 和公钥 $\mathrm{pk}_{\mathrm{ID}}=(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},2})$.

(3)PartialKeyGen:给定用户的身份 ID 和公钥 $\mathrm{pk}_{\mathrm{ID}}$,KGC 首先计算 $\boldsymbol{u}=H_1(\mathrm{ID},\mathrm{pk}_{\mathrm{ID}})=(u_1,\cdots,u_{n_u})$ 和 $U=\prod_{i=1}^{n_u}u_i^{v_i}$;然后随机选择 $r_v\in Z_p^*$,计算 $\mathrm{psk}_{\mathrm{ID},1}=g_2^{\alpha}U^{r_v}$ 和 $\mathrm{psk}_{\mathrm{ID},2}=g^{r_v}$;最后,将部分私钥 $\mathrm{psk}_{\mathrm{ID}}=(\mathrm{psk}_{\mathrm{ID},1},\mathrm{psk}_{\mathrm{ID},2})$ 发送给用户.

(4)SetSecKey:收到 KGC 发送的 $\mathrm{psk}_{\mathrm{ID}}$ 后,如果等式 $e(\mathrm{psk}_{\mathrm{ID},1},g)=e(g_2,g_1)e(U,\mathrm{psk}_{\mathrm{ID},2})$ 成立,用户设置私钥 $\mathrm{sk}_{\mathrm{ID}}=(\mathrm{usk}_{\mathrm{ID}},\mathrm{psk}_{\mathrm{ID}})$;否则,拒绝接受 $\mathrm{psk}_{\mathrm{ID}}$.

(5)Sign:对于一个消息 m,身份为 ID 的用户随机选择 $r_m \in Z_p^*$,计算 $\boldsymbol{a}=H_4(\mathrm{ID})=(a_1,\cdots,a_{n_m})$,$W=\prod_{k=1}^{n_m} w_k^{a_k}$,$\boldsymbol{b}=H_2(m\|g^{r_m}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})=(b_1,\cdots,b_{n_t})$,$S=\prod_{j=1}^{n_t} s_j^{b_j}$,$\boldsymbol{c}=H_3(\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})=(c_1,\cdots,c_{n_t})$,$T=\prod_{j=1}^{n_t} t_j^{c_j}$ 和 $h=H_5(m\|g^{r_m}\|\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})$;然后输出 m 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$,其中 $\sigma_1=(\mathrm{psk}_{\mathrm{ID},1})^h S^{\theta_1 h} T^{\theta_2} W^{r_m}$,$\sigma_2=(\mathrm{psk}_{\mathrm{ID},2})^h$ 和 $\sigma_3=g^{r_m}$.

(6)Verify:给定身份 ID、公钥 $\mathrm{pk}_{\mathrm{ID}}=(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},2})$ 和消息 m 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$,验证者计算 $U=\prod_{i=1}^{n_u} u_i^{v_i}$,$S=\prod_{j=1}^{n_t} s_j^{b_j}$,$T=\prod_{j=1}^{n_t} t_j^{c_j}$,$W=\prod_{k=1}^{n_m} w_k^{a_k}$ 和 $h=H_5(m\|\sigma_3\|\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})$. 如果等式 $e(\sigma_1,g)=e(g_1,g_2)^h e(U,\sigma_2) e(\mathrm{pk}_{\mathrm{ID},1},S)^h e(\mathrm{pk}_{\mathrm{ID},2},T) e(W,\sigma_3)$ 成立,输出 1;否则,输出 0.

3.2 Wu 方案的安全性分析

(1)针对 Wu 方案的普通伪造攻击

给定一个消息/签名对(m,σ),攻击者 $\mathcal{A}$ 通过下面的算法 1 成功伪造一个关于消息 m 的新签名 σ^*.

算法 1 普通伪造攻击

输入:一个消息/签名对(m,σ)

输出:一个消息 m 的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$

①假设 $\mathcal{A}$ 截获了一个关于身份 ID 和公钥 $\mathrm{pk}_{\mathrm{ID}}=(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},2})$ 的消息/签名对$(m,\sigma=(\sigma_1,\sigma_2,\sigma_3))$,其中 $\sigma_1=(g_2^\alpha U^{r_t})^h S^{\theta_1 h} T^{\theta_2} W^{r_m}$,$\sigma_2=(g^{r_t})^h$,$\sigma_3=g^{r_m}$ 和 $h=H_5(m\|\sigma_3\|\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})$.

②$\mathcal{A}$ 随机选取 $r^*\in Z_p^*$,计算 $\sigma_1^*=\sigma_1\cdot U^{r^* h}$ 和 $\sigma_2^*=\sigma_2\cdot(g^{r^*})^h$,并设置 $\sigma_3^*=\sigma_3$.

③$\mathcal{A}$ 输出一个消息 m 的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$.

因为 ID 的部分私钥 $\mathrm{psk}_{\mathrm{ID}}$ 和秘密值 $\mathrm{usk}_{\mathrm{ID}}$ 对攻击者 $\mathcal{A}$ 是未知的,但 σ^* 是一个消息 m 的合法签名,所以 $\mathcal{A}$ 成功伪造了一个 Wu 方案的签名,即 Wu 方案[17]不满足强不可伪造性. 以上伪造攻击成功的主要原因是哈希函数值 h 没有包含对部分私钥 $\mathrm{psk}_{\mathrm{ID},2}$ 的限制,使得伪造签名 σ^* 和原始签名 σ 具有相同的哈希值 $h=H_5(m\|\sigma_3\|\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})$. 因此,攻击者通过对原始签名 σ 的随机化处理,很容易伪造出新的合法签名 σ^*.

(2)针对 Wu 方案的“malicious-but-passive”KGC 攻击

令 $\mathcal{A}_2$ 是一个“malicious-but-passive”的 KGC 攻击者,则 $\mathcal{A}_2$ 生成主密钥 $\mathrm{msk}=g_2^\alpha$ 和系统参数 $\mathrm{sp}=\{G_1,G_2,e,p,g,g_1,g_2,\boldsymbol{u},\boldsymbol{s},\boldsymbol{t},\boldsymbol{w},H_1,H_2,H_3,H_4,H_5\}$. $\mathcal{A}_2$ 通过下面的算法 2 能成功伪造任意消息的合法签名.

算法 2 “malicious-but-passive”的 KGC 攻击

输入:一个消息 m^* 和一个用户的身份 ID 及公钥 $\mathrm{pk}_{\mathrm{ID}}$

输出:一个消息 m^* 的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$

①$\mathcal{A}_2$ 随机选取 $u_0,u_1,\cdots,u_{n_u}\in G_1$,选择 $\alpha,x_1,\cdots,x_{n_t},y_1,\cdots,y_{n_t},z_1,\cdots,z_{n_m}\in Z_p^*$,计算 $\mathrm{msk}=g_2^\alpha$,$s_1=g^{x_1},\cdots,s_{n_t}=g^{x_{n_t}}$,$t_1=g^{y_1},\cdots,t_{n_t}=g^{y_{n_t}}$,$w_1=g^{z_1},\cdots,w_{n_m}=g^{z_{n_m}}$,然后设置 4 个长度分别为 n_u、n_t、n_t 和 n_m 的向量 $\boldsymbol{u}=(u_i)$,$\boldsymbol{s}=(s_j)$,$\boldsymbol{t}=(t_j)$ 和 $\boldsymbol{w}=(w_k)$,并生成其它系统参数.

②$\mathcal{A}_2$ 随机选择一个消息 m^*,并获得目标用户的身份 ID 和公钥 $\mathrm{pk}_{\mathrm{ID}}=(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},2})$.

③$\mathcal{A}_2$ 计算 ID 的部分私钥 $\mathrm{psk}_{\mathrm{ID}}=(\mathrm{psk}_{\mathrm{ID},1},\mathrm{psk}_{\mathrm{ID},2})=(g_2^\alpha U^{r_v},g^{r_v})$,其中 $r_v\in Z_p^*$,$\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{pk}_{\mathrm{ID}})=(v_1,\cdots,v_{n_u})$ 和 $U=\prod_{i=1}^{n_u} u_i^{v_i}$.

④$\mathcal{A}_2$ 随机选取 $r_m^*\in Z_p^*$,计算 $\sigma_3^*=g^{r_m^*}$,$h^*=H_5(m^*\|\sigma_3^*\|\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})$,$\boldsymbol{a}=H_4(\mathrm{ID})=(a_1,\cdots,a_{n_m})$,$\boldsymbol{b}=H_2(m^*\|\sigma_3^*\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})=(b_1,\cdots,b_{n_t})$,$\boldsymbol{c}=H_3(\mathrm{ID}\|\mathrm{pk}_{\mathrm{ID},1}\|\mathrm{pk}_{\mathrm{ID},2})=(c_1,\cdots,c_{n_t})$.

⑤$\mathcal{A}_2$ 计算 $\sigma_1^*=(\mathrm{psk}_{\mathrm{ID},1})^{h^*}(\mathrm{pk}_{\mathrm{ID},1})^{h^*\cdot\sum_{i=1}^{n_t} x_i b_i}(\mathrm{pk}_{\mathrm{ID},2})^{\sum_{j=1}^{n_t} y_j c_j}(\sigma_3^*)^{\sum_{k=1}^{n_m} z_k a_k}$ 和 $\sigma_2^*=(\mathrm{psk}_{\mathrm{ID},2})^{h^*}$.

⑥$\mathcal{A}_2$ 输出一个消息 m^* 的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$.

很容易验证 $\mathcal{A}_2$ 伪造的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$ 是一个关于消息 m^* 的合法签名. 攻击者 $\mathcal{A}_2$ 不知道目标用户的秘密值 $\mathrm{usk}_{\mathrm{ID}}$,但能代表目标用户生成任意消息的合法签名. 这表明 Wu 方案无法抵抗来自“malicious-but-passive”的 KGC 攻击,即 Wu 方案[17]在第二类攻击 $\mathcal{A}_2$ 下是不安全的.

4 改进的无证书签名方案

4.1 方案描述

(1)Setup:给定安全参数 $\lambda\in Z$,KGC 首先选择两个阶为素数 p 的循环群 G_1 和 G_2,一个 G_1 的生成元 g 和一个双线性映射 $e:G_1\times G_1\to G_2$;然后随机选择 $u_0,w_0\in G_1$ 和 2 个向量 $\boldsymbol{u}=(u_i)$,$\boldsymbol{w}=(w_j)$,其中 $u_i,w_j\in G_1$,$i=1,\cdots,n_u$ 和 $j=1,\cdots,n_m$;并选择 3 个抗碰撞的哈希函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_u}$,$H_2:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_3:\{0,1\}^*\to Z_p^*$. KGC 随机选择 $\alpha\in Z_p^*$,计算 $g_1=g^\alpha$ 和 $\mathrm{msk}=g^{\alpha^2}$. 最后,KGC 秘密保存主密钥 msk,公开系统参数 $\mathrm{sp}=\{G_1,G_2,e,p,g,g_1,u_0,w_0,\boldsymbol{u},\boldsymbol{w},H_1,H_2,H_3\}$.

(2)UserKeyGen:身份为 ID 的用户随机选择 $\theta_1,\theta_2\in Z_p^*$,计算 $\mathrm{pk}_{\mathrm{ID},1}=g^{\theta_1}$ 和 $\mathrm{pk}_{\mathrm{ID},2}=g^{\theta_2}$,并设置秘密值 $\mathrm{usk}_{\mathrm{ID}}=g^{\theta_1^2}$ 和公钥 $\mathrm{pk}_{\mathrm{ID}}=(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},2})$.

(3)PartialKeyGen:给定用户的身份 ID 和公钥 $\mathrm{pk}_{\mathrm{ID}}$,KGC 首先计算 $\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{pk}_{\mathrm{ID}})=(v_1,\cdots,v_{n_u})$ 和 $U=u_0\prod_{i=1}^{n_u} u_i^{v_i}$;然后随机选择 $s\in Z_p^*$,计算 $\mathrm{psk}_{\mathrm{ID},1}=g^{\alpha^2}(U)^s$ 和 $\mathrm{psk}_{\mathrm{ID},2}=g^s$;最后,通过一个安全信道将部分私钥 $\mathrm{psk}_{\mathrm{ID}}=(\mathrm{psk}_{\mathrm{ID},1},\mathrm{psk}_{\mathrm{ID},2})$ 发送给用户.

(4) SetSecKey:收到 KGC 发送的 $\mathrm{psk_{ID}}=(\mathrm{psk_{ID,1}},\mathrm{psk_{ID,2}})$ 后,若等式 $e(\mathrm{psk_{ID,1}},g)=e(g_1,g_1)e(U,\mathrm{psk_{ID,2}})$ 不成立,用户拒绝接受部分私钥 $\mathrm{psk_{ID}}$;否则,用户随机选择 $r\in Z_p^*$,计算 $\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{pk_{ID}})=(v_1,\cdots,v_{n_u})$ 和 $U=u_0\prod_{i=1}^{n_u}u_i^{v_i}$,并利用自己的秘密值 $\mathrm{usk_{ID}}=g^{\theta_1^2}$ 计算私钥

$$\begin{aligned}\mathrm{sk_{ID}}&=(\mathrm{sk_{ID,1}},\mathrm{sk_{ID,2}})=(\mathrm{psk_{ID,1}}\times\mathrm{usk_{ID}}\times U^r,\mathrm{psk_{ID,2}}\times g^r)\\&=(g^{\alpha^2}g^{\theta_1^2}U^{s+r},g^{s+r}).\end{aligned}$$

(5) Sign:对于一个消息 m,身份为 ID 的用户随机选择 $r_m\in Z_p^*$,计算 $\boldsymbol{M}=H_2(m)=(M_1,\cdots,M_{n_m})$,$W=w_0\prod_{j=1}^{n_m}w_j^{M_j}$ 和 $h=H_3(m,\mathrm{ID},\mathrm{pk_{ID}},\mathrm{sk_{ID,2}},g^{r_m},\mathrm{sp})$,输出消息 m 的签名

$$\begin{aligned}\boldsymbol{\sigma}&=(\sigma_1,\sigma_2,\sigma_3)\\&=(\mathrm{sk_{ID,1}}\times((\mathrm{pk_{ID,2}})^h\times W)^{r_m},\mathrm{sk_{ID,2}},g^{r_m}).\end{aligned}$$

(6) Verify:给定身份 ID、公钥 $\mathrm{pk_{ID}}=(\mathrm{pk_{ID,1}},\mathrm{pk_{ID,2}})$ 和一个消息 m 的签名 $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\sigma_3)$,验证者计算 $U=u_0\prod_{i=1}^{n_u}u_i^{v_i}$,$W=w_0\prod_{j=1}^{n_m}w_j^{M_j}$ 和 $h=H_3(m,\mathrm{ID},\mathrm{pk_{ID}},\sigma_2,\sigma_3,\mathrm{sp})$. 如果等式

$$e(\sigma_1,g)=e(g_1,g_1)e(\mathrm{pk_{ID,1}},\mathrm{pk_{ID,1}})e(U,\sigma_2)e((\mathrm{pk_{ID,2}})^hW,\sigma_3)$$

成立,输出 1;否则,输出 0.

4.2　安全性分析

定理 1　在标准模型中,本文提出的无证书签名方案在公钥替换攻击下满足强不可伪造性.

证明　假定第一类攻击者 $\mathcal{A}_1$ 在多项式时间内最多进行了 q_{pk} 次公钥询问、q_{psk} 次部分私钥询问、q_{rep} 次公钥替换询问、q_{sk} 次私钥询问和 q_s 次签名询问. 给定一个 Squ-CDH 问题实例 (g,g^α),挑战者 C 为了计算 g^{α^2} 与 $\mathcal{A}_1$ 进行如下的交互游戏.

(1) 初始化:C 设置 $l_u=2(q_{\mathrm{psk}}+q_{\mathrm{sk}}+q_s)$ 和 $l_m=2q_s$,满足 $l_u(n_u+1)<p$ 和 $l_m(n_m+1)<p$,然后执行如下操作:

①随机选取两个整数 $k_u\in\{1,\cdots,n_u\}$ 和 $k_m\in\{1,\cdots,n_m\}$.

②随机选取 $x_0,x_1,\cdots,x_{n_u}\in Z_{l_u}$;$c_0,c_1,\cdots,c_{n_m}\in Z_{l_m}$;$y_0,y_1,\cdots,y_{n_u},d_0,d_1,\cdots,d_{n_m}\in Z_p^*$.

③选择 3 个哈希函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_u}$,$H_2:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_3:\{0,1\}^*\to Z_p^*$. 这些哈希函数在以下的证明中不被看作是理想的随机预言机,仅要求满足抗碰撞性.

④随机选取 $\theta_1^*,\theta_2^*\in Z_p^*$,计算 $\mathrm{pk}_1^*=g^{\theta_1^*}$ 和 $\mathrm{pk}_2^*=g^{\theta_2^*}$,设置目标用户的秘密值 $\mathrm{usk}^*=g^{(\theta_1^*)^2}$ 和公钥 $\mathrm{pk}^*=(\mathrm{pk}_1^*,\mathrm{pk}_2^*)$.

⑤设置参数 $g_1=g^\alpha$,$u_0=g_2^{-l_uk_u+x_0}g^{y_0}$,$u_i=g_2^{x_i}g^{y_i}(1\le i\le n_u)$,$w_0=g_2^{-l_mk_m+c_0}g^{d_0}$,$w_j=g_2^{c_j}g^{d_j}(1\le j\le n_m)$,$\boldsymbol{u}=(u_1,\cdots,u_{n_u})$ 和 $\boldsymbol{w}=(w_1,\cdots,w_{n_m})$.

⑥将参数 $\mathrm{sp}=\{G_1,G_2,e,p,g,g_1,u_0,w_0,\boldsymbol{u},\boldsymbol{w},H_1,H_2,H_3\}$ 和目标用户的秘密值/公钥对 $(\mathrm{usk}^*,\mathrm{pk}^*)$ 发送给 $\mathcal{A}_1$.

为了描述方便,对于 $\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{pk_{ID}})=(v_1,\cdots,v_{n_u})$,定义两个函数 $F(\mathrm{ID})=-l_uk_u+x_0+\sum_{i=1}^{n_u}x_iv_i$ 和 $J(\mathrm{ID})=y_0+\sum_{i=1}^{n_u}y_iv_i$. 对于 $\boldsymbol{M}=H_2(m)=(M_1,\cdots,M_{n_m})$,定义函数 $K(m)=-l_mk_m+c_0+\sum_{j=1}^{n_m}c_jM_j$ 和 $L(m)=d_0+\sum_{j=1}^{n_m}d_jM_j$,于是有等式 $U=u_0\prod_{i=1}^{n_u}u_i^{v_i}=g_1^{F(\mathrm{ID})}g^{J(\mathrm{ID})}$ 和 $W=w_0\prod_{j=1}^{n_m}w_j^{M_j}=g_1^{K(m)}g^{L(m)}$.

(2) 询问:为了响应攻击者 $\mathcal{A}_1$ 的询问,挑战者 C 维护一个初始化为空的列表 $L=\{(\mathrm{ID}_i,\theta_{i,1},\theta_{i,2},\mathrm{usk}_i,\mathrm{pk}_i,\mathrm{psk}_i,\mathrm{sk}_i)\}$.

①公钥询问:对于 $\mathcal{A}_1$ 发起的关于身份 ID_i 的公钥询问,若表 L 中包含 ID_i 的记录且 $\mathrm{pk}_i\ne\perp$,C 将相应的 pk_i 返回给 $\mathcal{A}_1$;否则,C 随机选择 $\theta_{i,1},\theta_{i,2}\in Z_p^*$,计算秘密值 $\mathrm{usk}_i=g^{(\theta_{i,1})^2}$ 和公钥 $\mathrm{pk}_i=(\mathrm{pk}_{i,1},\mathrm{pk}_{i,2})=(g^{\theta_{i,1}},g^{\theta_{i,2}})$;然后发送 pk_i 给 $\mathcal{A}_1$,并将 $(\mathrm{ID}_i,\theta_{i,1},\theta_{i,2},\mathrm{usk}_i,\mathrm{pk}_i,\perp,\perp)$ 添加到表 L 中.

②公钥替换询问:$\mathcal{A}_1$ 输入一个身份 ID_i 和新公钥 pk'_i,如果表 L 中包含 ID_i 的记录且 $\mathrm{pk}_i\ne\perp$,C 将 ID_i 对应的公钥 pk_i 替换为 pk'_i;否则,C 设置 pk'_i 为 ID_i 的公钥,在表 L 中添加 $(\mathrm{ID}_i,\perp,\perp,\perp,\mathrm{pk}'_i,\perp,\perp)$.

③部分私钥询问:当 $\mathcal{A}_1$ 请求关于 $(\mathrm{ID}_i,\mathrm{pk}_i)$ 的部分私钥时,如果表 L 中包含 ID_i 的记录且 $\mathrm{psk}_i\ne\perp$,则 C 将相应的 psk_i 返回给 $\mathcal{A}_1$. 否则,C 将考虑以下两种情况:

(a) 若 $F(\mathrm{ID}_i)=0\bmod l_u$,$C$ 退出游戏.

(b) 若 $F(\mathrm{ID}_i)\ne0\bmod l_u$,$C$ 选取 $s_i\in Z_p^*$,计算 $\boldsymbol{v}=H_1(\mathrm{ID}_i,\mathrm{pk}_i)=(v_1,\cdots,v_{n_u})$,$U_i=u_0\prod_{k=1}^{n_u}u_k^{v_k}$ 和 $\mathrm{psk}_i=(\mathrm{psk}_{i,1},\mathrm{psk}_{i,2})=(g_1^{\frac{-J(\mathrm{ID}_i)}{F(\mathrm{ID}_i)}}(U_i)^{s_i},g_1^{\frac{-1}{F(\mathrm{ID}_i)}}g^{s_i})$,发送 psk_i 给 $\mathcal{A}_1$,在表 L 中添加 ID_i 的部分私钥 psk_i.

④私钥询问:当 $\mathcal{A}_1$ 请求关于 ID_i 的私钥时,如果表 L 中包含 ID_i 的记录且 $\mathrm{sk}_i\ne\perp$,则 C 将相应的 sk_i 返回给 $\mathcal{A}_1$;否则,C 计算 $F(\mathrm{ID}_i)$. 如果 $F(\mathrm{ID}_i)=0\bmod l_u$,$C$ 退出游戏;否则,C 首先发起关于 ID_i 的公钥询问获得秘密值 usk_i 和公钥 pk_i,然后发起关于 $(\mathrm{ID}_i,\mathrm{pk}_i)$ 的私钥询问获得部分私钥 psk_i,最后运行 SetSecKey 算法将生成的私钥 sk_i 发送给 $\mathcal{A}_1$,并在表 L 中添加 ID_i 的私钥 sk_i.

⑤签名询问:当 $\mathcal{A}_1$ 请求关于身份 ID_i 和消息 m_i 的签名询问时,C 首先发起关于 ID_i 的公钥询问获得元组 $(\theta_{i,1},\theta_{i,2})$ 和公钥 $\mathrm{pk}_i=(\mathrm{pk}_{i,1},\mathrm{pk}_{i,2})$. 如果 $F(\mathrm{ID}_i)\neq 0 \bmod l_u$,$C$ 首先发起私钥询问获得 ID_i 的私钥,然后运行 Sign 算法将生成的签名发送给 $\mathcal{A}_1$. 如果 $F(\mathrm{ID}_i)=0 \bmod l_u$,$C$ 继续考虑以下两种情况:

(a)如果 $K(m_i)=0 \bmod l_m$,C 退出游戏;

(b)如果 $K(m_i)\neq 0 \bmod l_m$,C 随机选取 $r_i,s_i,r_m\in Z_p^*$,计算 $\boldsymbol{v}=H_1(\mathrm{ID}_i,\mathrm{pk}_i)$,$U_i=u_0\prod_{k=1}^{n_u}u_k^{v_k}$,$\boldsymbol{M}=H_2(m_i)$,$W_i=w_0\prod_{j=1}^{n_m}w_j^{M_j}$,$\sigma_{i,2}=g^{s_i+r_i}$,$\sigma_{i,3}=(g_1)^{\frac{-1}{K(m_i)}}g^{r_m}$,$h_i=H_3(m_i,\mathrm{ID}_i,\mathrm{pk}_i,\sigma_{i,2},\sigma_{i,3},\mathrm{sp})$ 和 $\sigma_{i,1}=(U_i)^{s_i+r_i}(g_1)^{\frac{-L(m_i)-h_i\theta_{i,2}}{K(m_i)}}((\mathrm{pk}_{i,2})^{h_i}W_i)^{r_m}g^{(\theta_{i,1})^2}$;然后将签名 $\sigma_i=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})$ 发送给 $\mathcal{A}_1$.

(3)伪造:$\mathcal{A}_1$ 最后输出一个关于身份 ID^* 和目标公钥 pk^* 的消息/签名对 $(m^*,\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*))$. 如果 $F(\mathrm{ID}^*)\neq 0 \bmod p$ 或 $K(m^*)\neq 0 \bmod p$,C 退出游戏;否则,C 计算 $h^*=H_3(m^*,\mathrm{ID}^*,\mathrm{pk}^*,\sigma_2^*,\sigma_3^*,\mathrm{sp})$,然后使用 (θ_1^*,θ_2^*) 计算 Squ-CDH 问题实例的值 $g^{\alpha^2}=\dfrac{\sigma_1^*}{g^{(\theta_1^*)^2}(\sigma_2^*)^{J(\mathrm{ID}^*)}(\sigma_3^*)^{L(m^*)}(\sigma_3^*)^{h^*\theta_2^*}}$.

定理 2 在标准模型中,本文提出的无证书签名方案对于 malicious-but-passive 的 KGC 攻击是强不可伪造的.

证明:假定第二类攻击者 $\mathcal{A}_2$ 在多项式时间内最多进行了 q_{pk} 次公钥询问、q_{sk} 次私钥询问和 q_s 次签名询问. 给定一个 Squ-CDH 问题实例 $(g,B=g^{\beta})$,C 为了计算 g^{β^2} 与 $\mathcal{A}_2$ 进行如下的交互游戏.

(1) 初始化:令 $l_u=2(q_{\mathrm{sk}}+q_s)$ 和 $l_m=2q_s$,满足 $l_u(n_u+1)<p$ 和 $l_m(n_m+1)<p$. C 随机选取 $\theta^*\in Z_p^*$,计算 $\mathrm{pk}_2^*=g^{\theta^*}$,设置目标实体的公钥 $\mathrm{pk}^*=(\mathrm{pk}_1^*,\mathrm{pk}_2^*)=(B=g^{\beta},g^{\theta^*})$. 收到 C 发送的 pk^* 后,$\mathcal{A}_2$ 随机选取整数 $k_u\in\{1,\cdots,n_u\}$,$k_m\in\{1,\cdots,n_m\}$,$x_0,x_1,\cdots,x_{n_u}\in Z_{l_u}$,$c_0,c_1,\cdots,c_{n_m}\in Z_{l_m}$ 和 $y_0,y_1,\cdots,y_{n_u},d_0,d_1,\cdots,d_{n_m}\in Z_p^*$. $\mathcal{A}_2$ 选择 3 个抗碰撞的哈希函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_u}$,$H_2:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_3:\{0,1\}^*\to Z_p^*$;然后随机选取 $\alpha\in Z_p^*$,计算 $g_1=g^{\alpha}$ 和 $\mathrm{msk}=g^{\alpha^2}$. $\mathcal{A}_2$ 设置 $u_0=B^{-l_uk_u+x_0}g^{y_0}$,$u_i=B^{x_i}g^{y_i}(1\leq i\leq n_u)$,$w_0=B^{-l_mk_m+c}g^{d_0}$,$w_j=B^{c_j}g^{d_j}(1\leq j\leq n_m)$,$\boldsymbol{u}=(u_1,\cdots,u_{n_u})$ 和 $\boldsymbol{w}=(w_1,\cdots,w_{n_m})$,将系统参数 $\{g_1,u_0,v_0,\boldsymbol{u},\boldsymbol{w},H_1,H_2,H_3\}$ 和主密钥 msk 发送给 C.

为了描述方便,类似定理 1 定义 4 个函数 $F(\mathrm{ID})$、$J(\mathrm{ID})$、$K(m)$ 和 $L(m)$,可得到下面两个等式

$$U=u_0\prod_{i=1}^{n_u}u_i^{v_i}=B^{F(\mathrm{ID})}g^{J(\mathrm{ID})},\ W=v_0\prod_{j=1}^{n_m}v_j^{M_j}=B^{K(m)}g^{L(m)}.$$

(2) 询问:为了响应 $\mathcal{A}_2$ 的询问,C 维护一个初始化为空的列表 $L=\{(\mathrm{ID}_i,\theta_{i,1},\theta_{i,2},\mathrm{pk}_i,\mathrm{sk}_i)\}$.

①公钥询问:对于 $\mathcal{A}_2$ 发起的关于身份 ID_i 的公钥询问,如果表 L 中包含 ID_i 的记录且 $\mathrm{pk}_i\neq\perp$,则 C 将相应的 pk_i 返回给 $\mathcal{A}_2$. 否则,C 随机选择 $\theta_{i,1},\theta_{i,2},\in Z_p^*$,计算公钥 $\mathrm{pk}_i=(\mathrm{pk}_{i,1},\mathrm{pk}_{i,2})=(B^{\theta_{i,1}},g^{\theta_{i,2}})$;然后发送 pk_i 给 $\mathcal{A}_2$,并将 $(\mathrm{ID}_i,\theta_{i,1},\theta_{i,2},\mathrm{pk}_i,\perp)$ 添加到表 L 中.

②私钥询问:当 $\mathcal{A}_2$ 请求关于 ID_i 的私钥时,如果表 L 中包含 ID_i 的记录且 $\mathrm{sk}_i\neq\perp$,C 将相应的 sk_i 返回给 $\mathcal{A}_2$;否则,C 发起关于 ID_i 的公钥询问获得元组 $(\theta_{i,1},\theta_{i,2})$ 和公钥 pk_i,并执行如下操作:

(a)如果 $F(\mathrm{ID}_i)=0 \bmod l_u$,$C$ 退出游戏.

(b)如果 $F(\mathrm{ID}_i)\neq 0 \bmod l_u$,$C$ 选取 $s_i\in Z_p^*$,计算 $\boldsymbol{v}=H_1(\mathrm{ID}_i,\mathrm{pk}_i)=(v_1,\cdots,v_{n_u})$ 和 $U_i=u_0\prod_{k=1}^{n_u}u_k^{v_k}$,并利用主密钥 $\mathrm{msk}=g^{\alpha^2}$ 计算 $\mathrm{sk}_i=(\mathrm{sk}_{i,1},\mathrm{sk}_{i,2})=(g^{\alpha^2}B^{\frac{-J(\mathrm{ID}_i)(\theta_{i,1})^2}{F(\mathrm{ID}_i)}}(U_i)^{s_i},B^{\frac{-(\theta_{i,1})^2}{F(\mathrm{ID}_i)}}g^{s_i})$;最后发送 sk_i 给 $\mathcal{A}_2$,并将 ID_i 的私钥 sk_i 添加到表 L 中.

③签名询问:当 $\mathcal{A}_2$ 请求关于身份 ID_i 和消息 m_i 的签名询问时,C 首先发起关于 ID_i 的公钥询问获得元组 $(\theta_{i,1},\theta_{i,2})$ 和公钥 $\mathrm{pk}_i=(\mathrm{pk}_{i,1},\mathrm{pk}_{i,2})$. 如果 $F(\mathrm{ID}_i)\neq 0 \bmod l_u$,$C$ 首先发起私钥询问获得 ID_i 的私钥,然后运行 Sign 算法,并将生成的签名发送给 $\mathcal{A}_2$. 如果 $F(\mathrm{ID}_i)=0 \bmod l_u$,$C$ 继续考虑以下两种情况:

(a)如果 $K(m_i)=0 \bmod l_m$,C 退出游戏;

(b)如果 $K(m_i)\neq 0 \bmod l_m$,C 随机选取 $r_i,s_i,r_m\in Z_p^*$,计算 $\boldsymbol{v}=H_1(\mathrm{ID}_i,\mathrm{pk}_i)$,$U_i=u_0\prod_{k=1}^{n_u}u_k^{v_k}$,$\boldsymbol{M}=H_2(m_i)$,$W_i=w_0\prod_{j=1}^{n_m}w_j^{M_j}$,$\sigma_{i,2}=g^{s_i+r_i}$,$\sigma_{i,3}=B^{\frac{-(\theta_{i,1})^2}{K(m_i)}}g^{r_m}$,$h_i=H_3(m_i,\mathrm{ID}_i,\mathrm{pk}_i,\sigma_{i,2},\sigma_{i,3},\mathrm{sp})$ 和 $\sigma_{i,1}=g^{\alpha^2}(U_i)^{s_i+r_i}B^{\frac{(-L(m_i)-h_i\theta_{i,2})(\theta_{i,1})^2}{K(m_i)}}((\mathrm{pk}_{i,2})^{h_i}W_i)^{r_m}$;然后将 $\sigma_i=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})$ 发送给 $\mathcal{A}_2$.

(3)伪造:$\mathcal{A}_2$ 最后输出一个关于身份 ID^* 和目标公钥 pk^* 的消息/签名对 $(m^*,\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*))$. 如果 $F(\mathrm{ID}^*)\neq 0 \bmod p$ 或 $K(m^*)\neq 0 \bmod p$,C 退出游戏;否则,C 计算 $h^*=H_3(m^*,\mathrm{ID}^*,\mathrm{pk}^*,\sigma_2^*,\sigma_3^*,\mathrm{sp})$,然后使用 θ^* 和主密钥 $\mathrm{msk}=g^{\alpha^2}$ 计算 Squ-CDH 问题实例的值 $g^{\beta^2}=\dfrac{\sigma_1^*}{g^{\alpha^2}(\sigma_2^*)^{J(\mathrm{ID}^*)}(\sigma_3^*)^{L(m^*)}(\sigma_3^*)^{h^*\theta^*}}$.

4.3 性能分析

下面将改进的无证书签名方案与 Hung 方案[16]、Wu 方案[17]进行私钥大小、签名长度、计算开销和安全属性方面的比较,结果如表 1 所示. E 和 P 分别表示一次幂指数运算和一次双线性对操作,$|p|$ 和 $|G_1|$ 分别表

示 Z_p 和 G_1 中一个元素的长度.

表 1　计算开销与安全性能的比较

方案	私钥大小	签名长度	签名生成	签名验证	强不可伪造性
Hung 方案[16]	$3\|G_1\|$	$3\|G_1\|$	$5E$	$3E+4P$	否
Wu 方案[17]	$2\|p\|+2\|G_1\|$	$3\|G_1\|$	$6E$	$2E+4P$	否
本文新方案	$2\|G_1\|$	$3\|G_1\|$	$3E$	$E+5P$	是

由于在改进方案的签名验证等式 $e(\sigma_1,g)=e(g_1,g_1)e(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},1})e(U,\sigma_2)e((\mathrm{pk}_{\mathrm{ID},2})^h W,\sigma_3)$ 中,$e(g_1,g_1)$,$e(\mathrm{pk}_{\mathrm{ID},1},\mathrm{pk}_{\mathrm{ID},1})$ 和 $e(U,\sigma_2)$ 可以预计算处理,因此签名验证的计算开销可以降低为一次幂指数运算和两次双线性对操作. 从表 1 可知,本文提出的新方案具有更短的私钥长度和更低的签名生成开销. 更重要的是,Hung 方案[16] 和 Wu 方案[17] 均存在安全缺陷,但改进方案在标准模型下满足强不可伪造性. 因此,本文的新方案具有更高的安全性.

5　结论

本文分析了 Wu 和 Jing[17] 在 2018 年提出的无证书签名方案,指出该方案不满足强不可伪造性,并且无法抵抗 malicious-but-passive 的 KGC 攻击. 针对 Wu 方案[17] 存在的安全问题,提出了一个改进的无证书签名方案,并在标准模型中证明新方案对于自适应性选择消息攻击是强不可伪造的. 分析结果表明,新方案具有较高的计算性能和较高的安全性. 然而,新方案无法抵抗量子计算攻击,下一步的任务是设计格上安全高效的无证书签名方案.

参考文献

[1] Shen L, Ma J, Liu X, et al. A secure and efficientid-based aggregate signature scheme for wireless sensor networks [J]. IEEE Internet of Things Journal, 2017, 4(2): 546-554.

[2] Kang J, Yu R, Huang X, et al. Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 99: 1-11.

[3] Shamir A. Identity-based cryptosystems and signature schemes[A]. Proceedings of Workshop on the Theory and Application of Cryptographic Techniques[C]. Berlin, Heidelberg, Germany: Springer, 1981. 47-53.

[4] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. Proceedings of International Conference on the Theory and Application of Cryptology and Information Security[C]. Berlin, Heidelberg, Germany: Springer, 2003. 452-473.

[5] Shim K A. Anew certificateless signature scheme provably secure in the standard model[J]. IEEE Systems Journal, 2018, 99: 1-10.

[6] Jia X, He D, Liu Q, et al. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment[J]. Ad Hoc Networks, 2018, 71: 78-87.

[7] Li F, Xie D, Gao W, et al. A certificateless signature scheme and a certificateless public auditing scheme with authority trust level 3 +[J]. Journal of Ambient Intelligence and Humanized Computing, 2017, 8(1): 1-10.

[8] Yum D H, Lee P J. Generic construction of certificateless signature[A]. Proceedings of Australasian Conference on Information Security and Privacy[C]. Berlin, Heidelberg, Germany: Springer, 2004. 200-211.

[9] Yap W S, Chow S S M, Heng S H, et al. Security mediated certificateless signatures[A]. Proceedings of Applied Cryptography and Network Security[C]. Berlin, Heidelberg, Germany: Springer, 2007. 459-477.

[10] Wang L, Chen K, Long Y, et al. An efficient pairing-free certificateless signature scheme for resource-limited systems[J]. Science China Information Sciences, 2017, 60(11): 119-102.

[11] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM (JACM), 2004, 51(4): 557-594.

[12] Liu J K, Au M H, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model[A]. Proceedings of the 2nd Symposium on Information, Computer and Communications Security[C]. Berlin, Heidelberg, Germany: Springer, 2007. 273-283.

[13] Yuan Y, Wang C. Certificateless signature scheme with security enhanced in the standard model[J]. Information Processing Letters, 2014, 114(9): 492-499.

[14] Canard S, Trinh V C. An efficient certificateless signature scheme in the standard model[A]. Proceedings of International Conference on Information Systems Security[C]. Berlin, Heidelberg, Germany: Springer, 2016. 175-192.

[15] Boneh D, Shen E, Waters B. Strongly unforgeable signatures based on computational Diffie-Hellman[A]. Proceedings of International Workshop on Public Key Cryptography[C]. Berlin, Heidelberg, Germany: Springer,

2006. 229 – 240.
[16] Hung Y H, Huang S S, Tseng Y M, et al. Certificateless signature with strong unforgeability in the standard model [J]. Informatica, 2015, 26(4): 663 – 684.
[17] 吴涛,景晓军. 一种强不可伪造无证书签名方案的密码学分析与改进[J]. 电子学报,2018,46(3):602 – 606.
Wu Tao, Jing Xiao-jun. Cryptanalysis and improvement of a certificateless signature scheme with strong unforgeability[J]. Acta Electronica Sinica, 2018, 46(3): 602 – 606. (in Chinese)

作者简介

杨小东 男,1981 年出生于甘肃甘谷. 现为西北师范大学副教授、硕士生导师. 主要研究方向为现代密码学和云计算安全.
Email: y200888@163.com

王美丁 女,1995 年生于辽宁阜新. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为代理重签名.
E-mail: 775631303@qq.com

裴喜祯 女,1995 年生于山西大同. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为应用密码学.
E-mail: 15635293587@163.com

李雨潼 男,1994 年生于甘肃兰州. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为区块链.
E-mail: lytnwnu@163.com

陈春霖 女,1995 年生于甘肃陇南. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为大数据安全.
E-mail: chenchunlin731@163.com

麻婷春 女,1995 年生于甘肃古浪. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为云存储安全.
E-mail: nwnumtch@163.com