JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 873-889 (2017)
DOI: 10.6688/JISE.2017.33.4.1

Strongly Secure Certificateless Signature Scheme in the Standard Model With Resisting Malicious-But-Passive KGC Attack Ability

FENG WANG[1,2] AND LI XU[1,*]
[1]*Fujian Provincial Key Laboratory of Network Security and Cryptology*
School of Mathematics and Computer Science
Fujian Normal University
Fuzhou, Fujian, 350117 P.R. China
[2]*College of Mathematics and Physics*
Fujian Provincial Key Laboratory of Big Data Mining and Applications
Fujian University of Technology
Fuzhou, Fujian, 350118 P.R. China
E-mail: w.h.feng@163.com; xuli@fjnu.edu.cn[*]

Digital signature is an important cryptographic tool in the security and privacy of smart city. Certificateless signature has not only simplified certificate management of traditional public-key signature, but also solved the private key escrow problem of ID-based signature. Recently, Pang *et al.*'s proposed a certificateless signature scheme in the standard model. We find that their scheme is vulnerable to the attack of malicious-but-passive KGC adversary. From the analysis of Pang *et al.*'s secure proof, we give a suggestion for the proof of certificateless signature, *i.e.*, we cannot remain some possible trapdoor information for KGC. Then we propose a strongly secure certificateless signature scheme, and give the secure proof in standard model. Compared with Pang *et al.*'s and other certificateless signature scheme in standard model, our proposed scheme can resist attack of malicious-but-passive KGC adversary.

Keywords: certificateless signature, smart city, malicious-but-passive KGC attack, public key replacement attack, standard model

1. INTRODUCTION

Smart city [1, 2] will be the next generation of urbanization by using information and communication technologies (ICT) to make cities "smarter", such as government services, smart grids, transport and traffic managements, water controlling, waste treatment and recycling, *etc.* While the smart city provides a novel way to improve the people's quality of life, it will also introduce new security issues in the smart city. Ijaz *etc.* [3] categorized the security of smart city into governance, socioeconomic, and technological factors, and RFID (Radio Frequency Identification System), WSN (wireless sensor networks), M2M (machine to machine) communication, smart grids, smartphones, biometrics are the important component of technological factor security in smart city. Digital signature is usually used in WSN [3], smart grids [4, 5], smartphones [6] *etc.* to ensure the security of smart city. Furthermore, as an IoT tested for a smart city in Santander, Spain, SmartSantander project [7] used digital signature to ensure the security of power grid. So, digital signature is an important cryptographic tool in the security and privacy

Received May 16, 2016; revised July 21, 2016; accepted August 30, 2016.
Communicated by Zhe Liu.
[*] Corresponding author.

of smart city.

The notion of certificateless public-key cryptography was first proposed by Al-Riyami and Paterson [8] in 2003. In certificateless public-key cryptography, the user's private key is composed by the user's secret key and partial secret key. The user's secret key is selected by the user behind closed doors, and the partial secret key is generated by key generation center (KGC) from the user's identity. The user generates and publishes his/her public key without certificate.

Certificateless public-key cryptography has not only simplified certificate management of traditional public-key cryptography, but also solved the private key escrow problem [9] of ID-based public-key cryptography [10]. So, many application scenarios such as searchable encryption [11, 12] were solved by certificateless public-key cryptography [13] instead of traditional public-key cryptography [14, 15] or ID-based public-key cryptography [16], Therefore, a lot of certificateless schemes were proposed following Al-Riyami and Paterson's work, including many certificateless signature schemes.

Al-Riyami and Paterson [8] proposed the first certificateless signature scheme, and introduced two adversaries: public key replacement adversary A_{I}^{*} and honest-but-curious KGC adversary A_{II}^{*}. Unfortunately, Huang *et al.* [17] pointed out that Al-Riyami and Paterson's scheme cannot resist the attack of the public key replacement adversary A_{I}^{*}. Latter, Zhang *et al.* [18] and Gorantla and Saxena [19] proposed certificateless signatures scheme based on bilinear pairings respectively; Harn *et al.* [20] proposed certificateless signature scheme based on discrete logarithm problem. He *et al.* [21] constructed a high-efficiency certificateless signature scheme without bilinear pairings. However, Tian *et al.* [22], pointed out that He *et al.*'s scheme cannot resist the attack of honest-but-curious KGC adversary A_{II}^{*}. In 2014, Tsai *et al.* [23] and Gong and Li [24] proposed improved schemes respectively. In 2007, Au *et al.* [25] introduced malicious-but-passive KGC adversary A_{I}^{+}, and pointed out that the schemes [8, 17] cannot resist this attack. Based on the hard lattice problems, Kim and Jeong [26] proposed a new certificateless signature scheme against the attack of malicious-but-passive KGC adversary A_{II}^{+}.

However, all the certificateless signature schemes mentioned above are provable security in the random oracle. In fact, Canetti *etc.* [27] pointed out that random oracle model is not secure in actual applications. So, it is more practical to design cryptography schemes which are secure in the standard model [28]. Based upon Waters' signature [29], Liu *et al.* [30] proposed the first certificateless signature scheme in the standard model. However Xiong *et al.* [31] pointed out that Liu *et al.*'s scheme cannot resist the attack of malicious-but-passive KGC adversary A_{II}^{+}, and proposed a modified scheme. Huang *et al.* [32] proposed a generic certificateless signature scheme for resisting malicious-but-passive KGC adversary. Yuan *et al.* [33] also proposed a certificateless signature scheme in the standard model. Unfortunately, Xia *et al.* [34] pointed out that [31, 33] cannot resist the attack of Xia's public key replacement adversary A_{I}^{+}, *i.e.*, when adversary A_{I}^{+} obtains a signature on a message of a signer, he/she can forge valid signatures on the same message under the replaced public key. In 2012, Yu *et al.* [35] constructed a new certificateless signature scheme without random oracle model to avoid the attack of Xia's public key replacement adversary A_{I}^{+}, however, Cheng *et al.* [36] pointed out that Yu *et al.*'s scheme was vulnerable to the attacks of malicious-but-passive KGC adversary A_{II}^{+} and public key replacement adversaries A_{I}^{+} and A_{I}^{+}, and, Yuan *et al.* [37] proposed an improved scheme. In 2015, Pang *et al.* [38] proposed a new certificateless signature scheme

without random oracle model, however, we found that Pang *et al.*'s scheme cannot resist the attacks of malicious-but-passive KGC adversary A_{II}^{+}. In other words, we have found that most of the existing schemes in the standard model are insecure. Therefore, to construct a secure certificateless signature scheme in the standard model is worthwhile.

Inspired by Waters' signature [29], Parampalli and Narayan's [39] identity based signature, and Pang *et al.*'s [38] certificateless signature scheme, we proposed a strongly secure certificateless signature scheme with resisting the attack of malicious-but-passive KGC adversary A_{II}^{+} in the standard model. In the following, we summarize our contributions.

- We point out that Pang *et al.*'s [38] certificateless signature scheme is vulnerable to the attack of malicious-but-passive KGC adversary A_{II}^{+}. The reason is partly because that the authors construct the hardness problem by using the value generated by KGC to complete their proof of resisting malicious-but-passive KGC attack.
- We proposed a strongly secure certificateless signature scheme with resisting the attack of malicious-but-passive KGC adversary A_{II}^{+} in the standard model.
- We gives a suggestion for proof the certificateless signature resisting malicious-but-passive KGC attack, *i.e.*, we cannot remain some possible trapdoor information for KGC, especially cannot construct the hardness problem by using the value generated by KGC.

The rest of the paper is organized as follows. Section 2 gives the preliminaries including bilinear pairing, hard problems, and definition and security model of certificateless signature scheme. Section 3 reviews Pang *et al.*'s [38] certificateless signature scheme, and analyzes the flaws in their scheme. We propose our scheme in Section 4, and give the formal security proof in Section 5. In Section 6, we compare our scheme with others, and give the conclusion.

2. PRELIMINARIES

In this section, we introduce the conception of bilinear pairings and certificateless signature, and talk about the security model of certificateless signature, and hard problems in our scheme.

2.1 Bilinear Pairings

Let G_1 and G_2 be two multiplicative cyclic groups with the same prime order p, while g is a generator of G_1. The map e: $G_1 \times G_1 \rightarrow G_2$ is called a bilinear map [38] if the following three properties are held:

(1) Bilinear: For all $a, b \in Z_p^*$, the equation $e(g^a, g^b) = e(g, g)^{ab}$ is held.
(2) Non-degenerate: $e(g, g) \neq 1$.
(3) Computable: For any $g_1, g_2 \in G_1$, there is an efficient algorithm to compute $e(g_1, g_2)$.

2.2 Certificateless Signature

Generally, a certificateless signature scheme [38] involves three entities: the key

generation center (KGC), the signer, and the verifier; and five algorithms: Setup, UserKeyGen, ExtractPartialKey, Sign, and Verify.

(1) **Setup:** The KGC runs this algorithm. Given the security parameter k, KGC generates the system public parameters pp, and master secret key msk.
(2) **UserKeyGen:** The signer runs this algorithm. Given the public parameters pp, the signer generates the public key pk and the secret value sk.
(3) **ExtractPartialKey:** The KGC runs this algorithm. Given the signer's identity ID and public key pk, KGC uses the system public parameters pp and the master secret key msk to generate the signer's partial secret key psk.
(4) **Sign:** The signer runs this algorithm. Given the message m, the signer use the system public parameters pp, his/her identity ID, public key pk, secret value sk, and partial secret key psk to generate the signature σ.
(5) **Verify:** The verifier runs this algorithm. Given the message m, the signature σ, the system public parameters pp, the signer's identity ID and public key pk, the verifier checks the validity of signature σ.

2.3 Security Models

According to [8, 25, 34], There are two types of adversaries in certificateless signature.

One is the public key replacement adversary A_{I}. Al-Riyami and Paterson [8] defined that the public key replacement adversary A_{I}^{*} cannot have access to master secret key, but can select identity and replace the public key. Xia *et al.* [34] expended the public key replacement adversary A_{I}^{*} to A_{I}^{+}, *i.e.*, obtained a signature on a message of a signer, A_{I}^{+} can forge valid signatures on the same message under the replaced public key. In our manuscript, we denote the public key replacement adversaries A_{I}^{*} and A_{I}^{+} as A_{I}.

The other is malicious-but-passive KGC adversary A_{II}. Al-Riyami and Paterson [8] defined that the honest-but-curious KGC adversary A_{II}^{*} can have access to master secret key, but cannot replace the public key. Au *et al.* [25] expended the honest-but-curious KGC adversary A_{II}^{*} to malicious-but-passive KGC adversary A_{II}^{+}, *i.e.*, A_{II}^{+} is malicious and tries to impersonate the user. Obviously, if a scheme can resist the attack of A_{II}^{+}, it can resist the attack of A_{II}^{*} too. In our manuscript, we denote malicious-but-passive KGC adversary A_{II}^{+} as A_{II}.

2.4 Complexity Assumptions

Computational Diffie-Hellman (CDH) problem [40]: Let G_1 be a multiplicative cyclic groups with the prime order p, while g is a generator of G_1, and g^{α}, g^{β} be two random elements of G_1 with α, β unknown. The CDH problem is to output g^{γ} such that $\gamma = \alpha \cdot \beta$.

We say that the CDH assumption holds in a group G_1 if no algorithm running in polynomial time can solve the CDH problem in G_1 with an advantage of at least ε.

Square computational Diffie-Hellman problem (SCDH) [40]: the SCDH problem is a variation of CDH problem except that is to output g^{γ} such that $\gamma = \beta^2$. The SCDH assumption and CDH assumption are equivalent [40].

3. OVERVIEW AND SECURITY ANALYSIS THE PANG *ET AL.*'S SCHEME

In 2015, Pang *et al.* [38] proposed a certificateless signature scheme in the standard model. In this section, we review and analyze their scheme.

3.1 Overview the Pang *et al.*'s Scheme

In Pang *et al.*'s scheme [38], there are five phases, *i.e.*, Setup, UserKeyGen, ExtractPartialKey, Sign, and Verify, which are described as below.

(A) Setup

Given a security parameter k, the KGC performs the following steps.

Step 1: Choose two multiplicative cyclic groups G_1 and G_2 with prime order p, the group G_1's generator g, and a bilinear pairing e: $G_1 \times G_1 \to G_2$.

Step 2: Select four collision resistant hash functions H_1: $G_1 \times G_1 \to G_1$, H_2: $\{0, 1\}^* \times G_1^2 \to Z_p^*$, H_3: $\{0, 1\}^* \times G_1^3 \to \{0, 1\}^n$, and H_4: $\{0, 1\}^* \times G_1^3 \to Z_p^*$.

Step 3: Choose a random number $x \in Z_p^*$, and compute $g_1 = g^x$, and $g_2 = H_0(g, g_1)$.

Step 4: Choose $n + 3$ random elements $t_0, t_1, v_0, v_1, \ldots, v_n \in G_1$, and denote $V = (v_0, v_1, \ldots, v_n)$.

Step 5: Define a function $f(z) = (z_x + z_y) \bmod 2$, where $z \in G_1$, and z_x, z_y denotes x-coordinate and y-coordinate of $z \in G_1$ respectively.

Step 6: The public parameters are $pp = \{G_1, G_2, e, p, g, g_1, g_2, V, f, H_1, H_2, H_3, H_4\}$, and the master secret key is $msk = g_2^x$.

(B) UserKeyGen

Given the public parameter pp, the user with identity ID selects three random numbers $s_1, s_2, s_3 \in Z_p^*$, and computes $pk_1 = g_1^{s_1}$, $pk_2 = g_1^{s_2}$, $pk_3 = s_2 + s_3 \cdot H_2(ID, pk_1, pk_2)$, and $pk_4 = g_1^{s_3}$, then he/she sets his/her secret value $sk = s_2$, publishes his/her public key $pk = (pk_1, pk_2, pk_3, pk_4)$, and sends his/her identity ID to KGC via a public channel.

(C) ExtractPartialKey

With the user's identity ID and public key pk, the KGC selects a random number $r \in Z_p^*$, computes $Q = v_0 \prod_{i=1}^{n} v_i^{(H_3(ID, pk))[i]}$ where $(H_3(ID, pk))[i]$ denotes the ith bit of $H_3(ID, pk)$, $psk_1 = g_2^x Q^r$, and $psk_2 = g^r$, then sends the partial secret key $pk = (pk_1, pk_2)$ to the user via a secret channel.

(D) Sign

With the identity ID, public key pk, secret value sk, and partial secret key psk, the signer performs the following steps to sign a given a message m.

Step 1: Choose two random numbers $k, k' \in Z_p$.

Step 2: Compute $\sigma_3 = g^k$, $h = H_2(m, ID, \sigma_3, pk_2)$, $h' = H_4(m, ID, \sigma_3, pk_2, g_2)$, $b = f(\sigma_3)$, $Q = v_0 \prod_{i=1}^{n} v_i^{(H_3(ID, pk))[i]}$, $\sigma_1 = psk_1^{h' \cdot sk} \cdot Q^{k'} \cdot t_b^k \cdot pk_1^{h \cdot k}$, $\sigma_2 = psk_2^{h' \cdot sk} \cdot g^{k'}$.

Step 3: Output the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on the message m.

(E) Verify

Given the public parameter pp, the user's identity ID and public key pk, the mes-

sage m, and the signature σ, the verifier performs the following steps.

Step 1: Check whether the equation $pk_1^{pk_3} = pk_2 \cdot pk_4^{H_3(ID, pk_1, pk_2)}$ is held, if so, go to Step 2, else, reject it.

Step 2: Compute $h = H_2(m, ID, \sigma_3, pk_2)$, $h' = H_4(m, ID, \sigma_3, pk_2, g_2)$, $b = f(\sigma_3)$, $Q = v_0 \cdot \prod_{i=1}^{n} v_i^{(H_3(ID, pk))[i]}$.

Step 3: Check whether the equation $e(\sigma_1, g) = e(g_2^{h'}, pk_2) \cdot e(Q, \sigma_2) e(t_b \cdot pk_1^h, \sigma_3)$ is held, if so, the signature σ is valid, otherwise, the signature σ is invalid.

3.2 Security Analysis

In Pang *et al.*'s scheme [38], the authors insisted that their scheme can resist the malicious-but-passive KGC attack, and give the security proof. However, we find that their scheme is vulnerable to the malicious-but-passive KGC attack.

In their security proof against the malicious-but-passive KGC attack, given a NGB-Many-DH problem instance $(g^{\alpha}, g^{\beta}, g^{\gamma}, g^{\alpha\beta}, g^{\alpha\gamma}, g^{\beta\gamma}) \in G_1^6$, the challenger C tries to output $(g^{\alpha\beta\gamma x}, g^{x}) \in G_1^2$ by interacting with adversary A_{II}. However, the adversary A_{II} is the malicious-but-passive KGC which generates the value of $g^{\alpha} = g_1$. Therefore, the security proof is not perfect and probably results that their scheme is vulnerable to the malicious-but-passive KGC attack. So, we suggest that we cannot remain some possible trapdoor information for KGC, especially cannot construct the hardness problem by using the value generated by KGC because that the KGC is the adversary A_{II} in the security proof against the malicious-but-passive KGC attack. We describe the details of attack process as follows.

Step 1: In Setup phase, A_{II} chooses $2n+4$ random elements τ_0, τ_1, α_0, α_1, …., α_n, β_0, β_1, …., $\beta_n \in Z_p^*$, computes $t'_0 = g^{\tau_0}$, $t'_1 = g^{\tau_1}$, and $v'_i = g_2^{\alpha_i} \cdot g^{\beta_i}$ for $i = 0, 1, \ldots, n$, and denotes $V' = (v'_0, v'_1, \ldots, v'_n)$, then replaces the t_0, t_1, V by t'_0, t'_1, V.

Step 2: In ExtractPartialKey phase, A_{II} computes $\lambda = H_3(ID, pk)$, $Q = F(\lambda) = v'_0 \prod_{i=1}^{n} v_i'^{\lambda[i]} = g_2^{\alpha_0} \cdot g^{\beta_0} \prod_{i=1}^{n} (g_2^{\alpha_i} \cdot g^{\beta_i})^{\lambda[i]} = g_2^{\alpha_0 + \sum_{i=1}^{n} \alpha_i \cdot \lambda[i]} \cdot g^{\beta_0 + \sum_{i=1}^{n} \beta_i \cdot \lambda[i]} = g_2^{\alpha} \cdot g^{\beta}$, sets $\alpha = \alpha_0 + \sum_{i=1}^{n} \alpha_i \cdot \lambda[i]$, $\beta = \beta_0 + \sum_{i=1}^{n} \beta_i \cdot \lambda[i]$, $r' = -x \cdot \alpha^{-1}$, computes $psk_1 = g_2^{x} \cdot Q^{r'} = g_2^{x} \cdot Q^{-x \cdot \alpha^{-1}} = g_2^{x} \cdot (g_2^{\alpha} \cdot g^{\beta})^{-x \cdot \alpha^{-1}} = g^{-x \cdot \alpha^{-1} \cdot \beta}$, and $psk_2 = g^{r'} = g^{-x \cdot \alpha^{-1}}$, then sends the partial secret key $psk = (psk_1, psk_2)$ to user via a secret channel.

Step 3: In Sign phase, A_{II} computes $psk_1^{sk} = (g^{-x \cdot \alpha^{-1} \cdot \beta})^{sk} = (g^{x \cdot sk})^{-\alpha^{-1} \cdot \beta} = (g^{x \cdot sk})^{-\alpha^{-1} \cdot \beta} = psk_2^{-\alpha^{-1} \cdot \beta}$, $psk_2^{sk} = (g^{-x \cdot \alpha^{-1}})^{sk} = (g^{x \cdot sk})^{-\alpha^{-1}} = (g^{x \cdot sk})^{-\alpha^{-1}} = psk_2^{-\alpha^{-1}}$. So, for every message m, A_{II} can compute the user's signature as follows. A_{II} chooses two random number k, $k' \in Z_p$, computes $\sigma_3 = g^k$, $h = H_2(m, ID, \sigma_3, pk_2)$, $h' = H_4(m, ID, \sigma_3, pk_2, g_2)$, $b = f(\sigma_3)$, $Q = F(H_3(ID, pk))$, $\sigma_1 = (psk_1^{sk})^{h'} \cdot Q^{k'} \cdot t_b^k \cdot psk_1^{h \cdot k}$, $\sigma_2 = (psk_2^{sk})^{h'} \cdot g^{k'}$, outputs the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on the message m.

4. OUR SCHEME

Inspired by Waters' signature [29], Parampalli and Narayan's [39] ID based signature, and Pang *et al.*'s [38] certificateless signature scheme, we proposed a strongly se-

cure certificateless signature scheme. Our scheme has five phases, *i.e.*, Setup, UserKeyGen, ExtractPartialKey, Sign, and Verify, which are described as follows.

4.1 Setup

Given a security parameter k, the KGC performs the following steps.

Step 1: Choose two multiplicative cyclic groups G_1 and G_2 with prime order p, the group G_1's generator g, and a bilinear pairing e: $G_1 \times G_1 \to G_2$.
Step 2: Choose $n_1 + 2$ random elements $g_2, u_0, u_1, \ldots, u_{n1} \in G_1$, and denote $U = (u_0, u_1, \ldots, u_{n1})$.
Step 3: Choose $n_2 + 2$ random numbers $x, x_0, x_1, \ldots, x_{n2} \in Z_p^*$, and denote $msk_2 = (x_0, x_1, \ldots, x_{n2})$.
Step 4: Compute $g_1 = g^x$, $msk_1 = g_2^x$, $v_0 = g^{x_0}$, $v_1 = g^{x_1}$, …, $v_{n_2} = g^{x_{n_2}}$, and denote $V = (v_0, v_1, \ldots, v_{n2})$.
Step 5: The public parameters are $pp = \{G_1, G_2, e, p, g, g_1, g_2, U, V\}$, and the master secret key is $msk = (msk_1, msk_2)$.

4.2 UserKeyGen

Given the public parameter pp, the user with identity ID selects $n_2 + 2$ numbers $y, y_0, y_1, \ldots, y_{n2} \in Z_p^*$, and computes $pk_1 = g^y, w_0 = g^{y_0}, w_1 = g^{y_1}, \ldots, w_{n_2} = g^{y_{n_2}} \in G_1$, chooses a random element $pk_2 \in G_1$, and denotes $pk_3 = (w_0, w_1, \ldots, w_{n2})$, $sk_2 = (y_0, y_1, \ldots, y_{n2})$, then he/she sets his/her secret value $sk = (sk_1, sk_2) = (pk_2^y, sk_2)$, publishes his/her public key $pk = (pk_1, pk_2, pk_3)$.

4.3 ExtractPartialKey

With the user's identity ID and public key pk, the KGC selects a random number $r_1 \in Z_p^*$, computes $psk_1 = g_2^x (u_0 \prod_{i=1}^{n_1} u_i^{(ID \| pk)[i]})^{r_1}$, and $psk_2 = g^{r_1}$, then sends the partial secret key $psk = (psk_1, psk_2)$ to user via a secret channel.

4.4 Sign

With the identity ID, public key pk, secret value sk, and partial secret key psk, the signer performs the following steps to sign a given message m.

Step 1: Choose a random number $r_2 \in Z_p$.
Step 2: Compute $d_0 = v_0^{y_0}$, $d_0 = v_1^{y_1}$, …., $d_{n_2} = v_{n_2}^{y_{n_2}}$, $\sigma_1 = psk_1 \cdot sk_1 \cdot (d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]})^{r_2}$, $\sigma_2 = g^{r_2}$, $\sigma_3 = psk_2$, $\sigma_4 = (d_0, d_1, \ldots, d_n)$.
Step 3: Output the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ on the message m.

4.5 Verify

Given the public parameter pp, the user's identity ID and public key pk, the message m, and the signature σ, the verifier performs the following steps.

Step 1: For $i = 0, 1, \ldots, n_2$, check whether the equations $e(d_i, g) = e(v_i, w_i)$ are held and $e(\sigma_1, g) = e(\sigma_2, (d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]}) \cdot e(\sigma_3, u_0 \cdot \prod_{i=1}^{n_1} u_i^{(ID\|pk)[i]}) \cdot e(g_1, g_2) \cdot e(pk_1, pk_2)$ is held, if so, the signature σ is valid, otherwise, the signature σ is invalid.

Correctness:

$$
\begin{aligned}
e(\sigma_1, g) &= e(psk_1 \cdot (sk_1 \cdot (d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]})^{r_2}, g) \\
&= e((g_2^x \cdot (u_0 \cdot \prod_{i=1}^{n_1} u_i^{(ID\|pk)[i]})^{r_1} \cdot (g_4^y \cdot (d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]})^{r_2}, g) \\
&= e((d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]})^{r_2}, g) \cdot e((u_0 \cdot \prod_{i=1}^{n_1} u_i^{(ID\|pk)[i]})^{r_1}, g) \cdot e(g_2^x, g) \cdot e(pk_2^{\cdot y}, g) \\
&= e(d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]}, g^{r_2}) \cdot e(u_0 \prod_{i=1}^{n_1} u_i^{(ID\|pk)[i]}, g^{r_1}) \cdot e(g_2, g^x) \cdot e(pk_2, g^y) \\
&= e(\sigma_2, (d_0 \cdot \prod_{i=1}^{n_2} d_i^{m[i]}) \cdot e(\sigma_3, u_0 \cdot \prod_{i=1}^{n_1} u_i^{(ID\|pk)[i]}) \cdot e(g_1, g_2) \cdot e(pk_1, pk_2)
\end{aligned}
$$

5. SECURITY PROOF

In this section, we give the security proof of our scheme. In order to resist the attack of Xia's public key replacement adversary A_{I}^{+}, we bind the signer's public key and his/her identity to his partial secret key, which is inherited the idea of Pang *et al.*'s scheme [38]. In order to resist the attack of malicious-but-passive KGC adversary A_{II}, we set some values generated by cooperation of the signer and the KGC to ensure that there is no trapdoor information for KGC. Next, we prove our scheme can resist the attack mentioned in subsection 2.3. The proof of resisting the attack of public key replacement adversary A_{I} is described in subsection 5.1, and the proof of resisting the attack of malicious-but-passive KGC adversary A_{II} is described in subsection 5.2.

5.1 Resisting the Attack of Public Key Replacement Adversary

Theorem 1: If there is public key replacement adversary A_{I}, who can break our proposed scheme in polynomial time with the success probability ε. Then there is an algorithm, which interacting with A_{I}, can solve the SCDH problem with the probability $\varepsilon' \geq \frac{\varepsilon}{16 \cdot (q_{psk} + q_s) \cdot q_s \cdot (n_1 + 1) \cdot (n_2 + 1)}$, where q_{psk} is the number of queries made to partial-secret-key-extract-queries, and q_s is the number of queries made to sign-queries respectively.

***Proof*:** given a SCDH problem instance g^{β}, challenger C tries to output g^{β^2}, with the help of the adversary A_{I}. The challenger C does the following steps.

Setup: C sets G_1, G_2, e, p, g as same as subsection 4.1, $l_1 = 2(q_{psk} + q_s)$, $l_2 = 2q_s$, and two random integers k_1 and k_2, with $0 \leq k_1 \leq n_1$, and $0 \leq k_2 \leq n_2$. $l_1 \cdot (n_1+1) < p$, and $l_2 \cdot (n_2+1) < p$ for the given values q_{pk}, q_s, n_1, n_2; chooses randomly $\alpha_0, \alpha_1, \ldots, \alpha_{n1} \in Z_{l1}$, $\beta_0, \beta_1, \ldots, \beta_{n1} \in Z_p$, $\gamma_0, \gamma_1, \ldots, \gamma_{n2} \in Z_{l2}$, $\omega_0, \omega_1, \ldots, \omega_{n2} \in Z_p$; constructs the functions $F(\varsigma) = \alpha_0 + \sum_{i=1}^{n_1} \alpha_i \cdot \varsigma[i] - l_1 \cdot k_1$, $J(\varsigma) = \beta_0 + \sum_{i=1}^{n_1} \beta_i \cdot \varsigma[i]$, $K(\xi, Y) = Y_0 \cdot \gamma_0 + \sum_{i=1}^{n_2} Y_i \cdot \gamma_i \cdot \xi[i] - Y_0 \cdot l_2 \cdot k_2$, $L(\xi, Y) = Y_0 \cdot \omega_0 + \sum_{i=1}^{n_2} Y_i \cdot \omega_i \cdot \xi[i]$, where $\omega_i = g^{Y_i}$, for $i = 0, 1, \ldots, n_2$; computes the values: $g_2 = g^{\beta}$, $g_1 = g_2^t = g^{t \cdot \beta} = g^{\alpha}$, $u_0 = g_2^{-l_1 k_1 + \alpha_0} \cdot g^{\beta_0}$, $u_i = g_2^{\alpha_i} \cdot g^{\beta_i}$, for $1 \leq i \leq n_1$, $v_0 = g_2^{-l_2 k_2 + \gamma_0} \cdot g^{\omega_0}$, $v_i = g_2^{\gamma_i} \cdot g^{\omega_i}$, for $1 \leq i \leq n_2$; and sends the public parameters $pp = \{G_1, G_2, e, p, g, g_1, g_2, U,$

$V\}$ to A_I, where $U = (u_0, u_1, \ldots, u_{n_1})$, $V = (v_0, v_1, \ldots, v_{n_2})$.

Note that $u_0 \prod_{i=1}^{n_1} u_i^{\varsigma[i]} = g_2^{F(\varsigma)} g^{J(\varsigma)}$, $v_0^{y_0} \prod_{i=1}^{n_2} v_i^{y_i \cdot \xi[i]} = g_2^{K(\xi,Y)} g^{L(\xi,Y)}$.

Create-user-queries: C keeps a list L to store user's ID, public key and secret key. Received a query for a public key on an ID, C searches L to find the corresponding pk and return to A_I. If the pk haven't in L, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L, and sends pk to A_I.

Secret-key-extract-queries: C searches L to find the corresponding sk, otherwise, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L, and sends sk to A_I.

Partial-secret-key-extract-queries: Received an inquiry for the psk on an identity ID and public key pk, C checks if the equation $F(ID||pk) = 0 \bmod p$ is held. If so, aborts. Otherwise, C selects a random number r_1, and computes $psk_1 = g_1^{-J(ID||pk)/F(ID||pk)} = (u_0 \prod_{i=1}^{n} u_i)^{r_1}$, $psk_2 = g_1^{-1/F(ID||pk)} = g^{r_1}$, and sends $psk = (psk_1, psk_2)$ to A_I.

The correctness of psk is because that:

$$psk_1 = g_1^{-J(ID||pk)/F(ID||pk)} (u_0 \prod_{i=1}^{n_1} u_i^{(ID||pk)[i]})^{r_1} = g_2^{\alpha} (g_2^{F(ID||pk)} \cdot g^{J(ID||pk)})^{-\alpha/F(ID||pk)} \cdot (g_2^{F(ID||pk)} \cdot g^{J(ID||pk)})^{r_1}$$

$$= g_2^{\alpha} (g_2^{F(ID||pk)} \cdot g^{J(ID||pk)})^{r_1 - \alpha/F(ID||pk)} = g_2^{\alpha} (u_0 \prod_{i=1}^{n_1} u_i^{(ID||pk)[i]})^{\tilde{r}_1},$$

$$psk_2 = g_1^{-1/F(ID||pk)} g^{r_1} = g^{r_1 - \alpha/F(ID||pk)} = g^{\tilde{r}_1}, \text{ where } \tilde{r}_1 = r_1 - a/F(ID||pk).$$

Note that $F(ID||pk) = 0 \bmod p$ implies that $F(ID||pk) = 0 \bmod l_1$, and $F(ID||pk) \neq 0 \bmod l_1$ implies that $F(ID||pk) \neq 0 \bmod p$.

Public-key-replace-queries: C creates a list L' to for an public key on an ID. C searches L' to find the corresponding pk, otherwise, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L'.

Sign-queries: When C receives an inquiry for the signing on an identity ID and message m, C searches L to check if there is a replaced public key. If so, aborts, otherwise, C searches L to find the corresponding pk, if the ID is not in the L, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L. C checks if the inequation $F(ID||pk) \neq 0 \bmod l_1$ is held. If so, C can generate the psk from partial-secret-key-extract-queries and the sk from L to sign m. Otherwise, if $K(m, sk_2) = 0 \bmod l_1$, aborts, if not, it implies that $K(m, sk_2) \neq 0 \bmod p$. Known the sk from L, C picks two random numbers $r_1, r_2 \in Z_p$, computes $\sigma_1 = (u_0 \prod_{i=1}^{n_1} u_i^{(ID||pk)[i]})^{r_1} \cdot sk_1 \cdot g_1^{-L(m,sk_2)/K(m,sk_2)} \cdot (v_0^{y_0} \cdot$ $\sigma_2 = g_1^{-1/K(m,Y)} g^{r_2}$, $\sigma_3 = g^{r_1}$, $\sigma_4 = (d_0, d_1, \ldots, d_{n_2})$, and sends $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ to A_I. The correctness of σ is because that:

$$\sigma_1 = (u_0 \prod_{i=1}^{n_1} u_i^{(ID||pk)[i]})^{r_1} \cdot sk_1 \cdot g_1^{-L(m,sk_2)/K(m,sk_2)} \cdot (v_0^{y_0} \cdot \prod_{i=1}^{n_2} v_i^{y_i \cdot m[i]})^{r_2}$$

$$=g_2^{\alpha}\cdot(u_0\prod_{i=1}^{n_1}u_i^{(ID\|pk)[i]})^{r_1}\cdot sk_1\cdot(g_2^{K(m,sk_2)}\cdot g_1^{L(m,sk_2)/\alpha})^{-\alpha/K(m,sk_2)}\cdot(v_0^{y_0}\cdot\prod_{i=1}^{n_2}v_i^{y_i\cdot m[i]})^{r_2}$$

$$=g_2^{\alpha}\cdot(u_0\prod_{i=1}^{n_1}u_i^{(ID\|pk)[i]})^{r_1}\cdot sk_1\cdot(g_2^{K(m,sk_2)}\cdot g^{L(m,sk_2)})^{-\alpha/K(m,sk_2)}\cdot(v_0^{y_0}\cdot\prod_{i=1}^{n_2}v_i^{y_i\cdot m[i]})^{r_2}$$

$$=g_2^{\alpha}\cdot(u_0\prod_{i=1}^{n_1}u_i^{(ID\|pk)[i]})^{r_1}\cdot sk_1\cdot(v_0^{y_0}\cdot\prod_{i=1}^{n_2}v_i^{y_i\cdot m[i]})^{-\alpha/(K(m,sk_2)}\cdot(v_0^{y_0}\cdot\prod_{i=1}^{n_2}v_i^{y_i\cdot m[i]})^{r_2}$$

$$=g_2^{\alpha}\cdot(u_0\prod_{i=1}^{n_1}u_i^{(ID\|pk)[i]})^{r_1}\cdot sk_1\cdot(v_0^{y_0}\cdot\prod_{i=1}^{n_2}v_i^{y_i\cdot m[i]})^{r_2-\alpha/(K(m,sk_2)}$$

$$\sigma_2=g_1^{-1/K(m,sk_2)}g^{r_2}=g^{r_2-\alpha/K(m,sk_2)}=g^{\tilde{r}_2},\ \text{where}\ \tilde{r}_2=r_2-\alpha/K(m,sk_2).$$

Solving the SCDH problem:

Finally, A_{I} outputs a forged signature $\sigma^*=(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*)$ with an identity ID^* on message m^*. If C does not terminate during the simulation, and satisfies the following conditions:

1. ID^* was never submitted to the partial-secret-key-extract-queries;
2. ① (ID^*, m^*) was never submitted to the sign-queries, or ② (ID^*, m^*) was submitted to the sign-queries, but the forged signature σ^* forged signature by the replaced pk^*.
3. σ^* is correct signature on message m^*

Note that 2② is for Xia's public key replacement adversary A_{I}^{+}.

If the pk is not replaced, C knows the sk. If the public key is replaced, we discuss the methods for A_{I} to replace pk_3^* in forging signature first. Although we cannot imitate A_{I}'s process of forged signature, note that A_{I} cannot solve the CDH problem, we can explain why A_{I} can provide additional information for the following reasons. If A_{I} selects a random element w_i^* from G_1 to construct pk_3^*, he/she must compute d_i^* for forging signature, *i.e.*, A_{I} can solve the CDH problem. Note the CDH problem is hard, so A_{I} must use the public parameters or the value from required the C to replace pk_3^*. Furthermore, he/she must compute pk_3^* by operations used in our scheme in section 5 such as multiplication, power, *etc.*, otherwise, there is nothing but select random elements from G_1. Then he/she sends the computation methods to C, and C can obtain that $w_i^*=g^{\theta_i}\cdot g_2^{\theta_i}=g^{\theta_i+\rho_i\cdot\beta}$, $0\le i\le n_2$, with the θ_i, ρ_i are known.

If there is a j such that $\rho_j\neq 0$, if $j\neq 0$, C can compute $g^{\beta 2}=(d_j^*\cdot(g^{\theta_j\cdot\omega_j}\cdot g_2^{\theta_j\cdot\gamma_j+\omega_j\cdot\rho_j})^{-1})^{(\rho_j\cdot\gamma_j)^{-1}}$. It is because that $e(v_j, w_i^*)=e(g^{\omega_j}\cdot g_2^{\gamma_j}, g^{\theta_j}\cdot g_2^{\rho_j})=e(g^{\omega_j+\gamma_j\cdot\beta}, g^{\theta_j+\rho_j\cdot\beta})=e(g^{(\theta_j+\rho_j\cdot\beta)(\omega_j+\gamma_j\cdot\beta)}, g)=e(g^{\theta_j\cdot\omega_j+(\theta_j\cdot\gamma_j+\omega_j\cdot\rho_j)\cdot\beta+\rho_j\cdot\gamma_j\cdot\beta^2}, g)$, and $e(v_j, w_i^*)=e(d_j^*, g)$.

If $j=0$, C can compute $g^{\beta 2}=(d_0^*\cdot(g^{\theta_0\cdot\omega_0}\cdot g_2^{\theta_0(-l_2\cdot k_2+\gamma_0)+\omega_0\cdot\rho_0})^{-1})^{(\rho_0\cdot(-l_2\cdot k_2+\gamma_0))^{-1}}$ similarly.

Otherwise, for $i=0$ to n_2, $\rho_i=0$, so $w_i^*=g^{\theta_i}$, $0\le i\le n_2$.

Furthermore, A_{I} uses the same method to replace pk_1^*, pk_2^*. With the same reason, at least one of pk_1^*, pk_2^* is equal to $g^{\theta'}$, where θ' is known by C. Without loss of generality, we set $pk_1^*=g^{\theta'}$. Therefore, regardless of the public key replaced or not, C knows the θ', θ_i of $pk_1^*=g^{\theta'}$, $w_i^*=g^{\theta_i}$, $0\le i\le n_2$. We denote $Y^*=\{\theta_0, \theta_1, \ldots, \theta_{n2}\}$.

If $F(ID^*\|pk^*)\neq 0 \bmod p$, or $K(m^*, Y^*)\neq 0 \bmod p$, aborts. If $F(ID^*\|pk^*)=0 \bmod p$, and $K(m^*, Y^*)=0 \bmod p$, C can compute $g^{\beta 2}=(\sigma_1^*\cdot((\sigma_2^*)^{L(m^*,Y^*)}\cdot(\sigma_3^*)^{J(ID^*\|pk^*)}\cdot(pk_2^*)^{\theta'})^{-1})^{t^{-1}}$. It is because that

$$e(\sigma_1^*, g)=e(\sigma_2^*, (d_0^*\cdot\prod_{i=1}^{n_2}(d_i^*)^{m^*[i]})\cdot e(\sigma_3^*, u_0\cdot\prod_{i=1}^{n_1}u_i^{(ID^*\|pk^*)[i]})\cdot e(g_1, g_2)\cdot e(pk_1^*, pk_2^*)$$

$$=e(\sigma_2^*, g_2^{K(m^*,Y^*)}g^{L(m^*,Y^*)})\cdot e(\sigma_3^*, g_2^{F(ID^*\|pk^*)}g^{J(ID^*\|pk^*)})\cdot e(g^{\alpha}, g^{\beta})\cdot e(g^{\theta'}, pk_2^*)$$

$$= e(\sigma_2^*, g^{L(m^*,Y^*)}) \cdot e(\sigma_3^*, g^{J(ID^*\|pk^*)}) \cdot e(g^{t\cdot\beta}, g^{\beta}) \cdot e(g^{\theta'}, pk_2^*)$$
$$= e((\sigma_2^*)^{L(m^*,Y^*)}, g) \cdot e((\sigma_3^*)^{J(ID^*\|pk^*)}, g) \cdot e(g^{t\cdot\beta^2}, g) \cdot e((pk_2^*)^{\theta'}, g)$$
$$= e((\sigma_2^*)^{L(m^*,Y^*)} \cdot (\sigma_3^*)^{J(ID^*\|pk^*)} \cdot g^{t\cdot\beta^2} \cdot (pk_2^*)^{\theta'}, g)$$

Now, we discuss the success probability of solving the SCDH problem. C will not abort during the proof if the following conditions satisfied simultaneously.

1. $F(ID\|pk) \neq 0$ in the partial-secret-key-queries.
2. $F(ID\|pk) \neq 0 \bmod l_1$ or $K(m, sk_2) \neq 0 \bmod l_2$ in the sign-queries.
3. $F(ID^*\|pk^*) \neq 0 \bmod p$, and $K(m^*, Y^*) = 0 \bmod p$, in the forged signature phase.

For simple, we ignore the condition that $F(ID\|pk) \equiv 0 \bmod l_1$ and $K(m, sk_2) \neq 0 \bmod l_2$ in the sign-queries. Let $ID_1, ID_2, \ldots, ID_{q_1}$ be the identities appearing in either partial-secret-key-extract-queries or sign-queries not involving the challenge identity and $m_1, m_2, \ldots, m_{q_2}$ be the messages appearing in sign-queries involving the challenge identity ID^*. Obviously, $q_1 \leq q_{psk} + q_s$ and $q_2 \leq q_s$. Define the events A_i, A^*, B_j, B^* as

A_i: $F(ID\|pk_i) = 0 \bmod l_1$, A^*: $F(ID^*\|pk^*) = 0 \bmod p$,
B_j: $F(m_j, sk_{2j}) = 0 \bmod l_2$, B^*: $K(m^*, Y^*) = 0 \bmod p$.

Then the probability of C not aborting is $\Pr[\neg abort] \geq pr[\wedge_{i=1}^{q_1} \overline{A}_i \wedge A^* \wedge_{i=1}^{q_2} \overline{B}_i \wedge B^*]$. Note that the events $\wedge_{i=1}^{q_1} \overline{A}_i \wedge A^*$ and $\wedge_{i=1}^{q_2} \overline{B}_i \wedge B^*$ are independent, and the assumption $l_1 \cdot (n_1 + 1) < p$ leads to $F(\varsigma) = 0 \bmod p \Rightarrow F(\varsigma) = 0 \bmod l_1$, so $\Pr[A^*] = \Pr[F(ID^*\|pk^*) = 0 \bmod p \wedge F(ID^*\|pk^*) = 0 \bmod l_1] = l_1^{-1} \cdot (n_1+1)^{-1}$, and $\Pr[\wedge_{i=1}^{q_1} \overline{A}_i] = 1 - \Pr[\vee_{i=1}^{q_1} A_i \mid A^*] \geq 1 - \sum_{i=1}^{q_1} \Pr[A_i \mid A^*] = 1 - \Pr[\vee_{i=1}^{q_1} A_i \mid A^*] \geq 1 - \sum_{i=1}^{q_1} \Pr[A_i \mid A^*] = 1 - q_1 \cdot l_i^{-1}$. Therefore, $\Pr[\wedge_{i=1}^{q_1} \overline{A}_i \wedge A^*] = \Pr[A^*] \cdot \Pr[\wedge_{i=1}^{q_1} \overline{A}_i \wedge A^*] = \Pr[A^*] \cdot \Pr[\wedge_{i=1}^{q_1} \overline{A}_i] \geq l_1^{-1} \cdot (n_1+1)^{-1} \cdot (1 - (q_{spk} + q_s) \cdot l_i^{-1})$. Set $q_1 = q_{spk} + q_s$, then, $\Pr[\wedge_{i=1}^{q_1} \overline{A}_i \wedge A^*] \geq (4 \cdot (q_{spk} + q_s)^{-1}$, similarly, $\Pr[\wedge_{i=1}^{q_2} \overline{B}_i \wedge B^*] \geq (4 \cdot q_s \cdot (n_2 + 1))^{-1}$, therefore, $\Pr[\neg\, abort] \geq (16 \cdot (q_{spk} + q_s) \cdot (n_1+1) \cdot (n_2 + 1))^{-1}$.

5.2 Resisting the Attack of Malice-but-Passive KGC Adversary

Theorem 2: If there is malice-but-passive KGC adversary A_{II}, who can break our proposed scheme in polynomial time with the success probability ε. Then there is an algorithm, which interacting with A_{II}, can solve the CDH problem with the probability $\varepsilon' \geq \frac{(q_{sk} - 1) \cdot \varepsilon}{4 \cdot q_{sk} \cdot q_s \cdot (n_2 + 1)}$, where q_{sk} is the number of queries made to secret-key-extract-queries, and q_s is the number of queries made to sign-queries respectively.

***Proof*:** given a CDH problem instance (g^{α}, g^{β}), challenger C tries to output $g^{\alpha\cdot\beta}$ with the help of the adversary A_{II}. The challenger C does the following steps.

Setup: C sets $l_1 = 2(q_e + q_s)$, $l_2 = 2q_s$, and selects two random integers k_1 and k_2, with $0 \leq k_1 \leq n_1$, and $0 \leq k_1 \leq n_2$. $l_1(n_1 + 1) < p$, and $l_2(n_2 + 1) < p$ for the given values q_e, q_s, n_1, n_2. Then C uses the setup phase in subsection 4.1 to generate the public parameters and the master secret key except U, and chooses randomly $\alpha_0, \alpha_1, \ldots, \alpha_{n_1} \in Z_{l_1}$, computes $u_i = g^{\alpha_i}$, $1 \leq i \leq n_1$, sends the public parameters pp and the master secret key msk to A_{II}. Next,

C chooses randomly $\gamma_0, \gamma_1, \ldots, \gamma_{n_2} \in Z_{l_2}$, $\omega_0, \omega_1, \ldots, \omega_{n_2} \in Z_p$, sets two functions $K(\xi) = x_0 \cdot \gamma_0 + \sum_{i=1}^{n_2} x_i \cdot \gamma_i \cdot \xi[i] - x_0 \cdot l_2 \cdot k_2, L(\xi) = x_0 \cdot \omega_0 + \sum_{i=1}^{n_2} x_i \cdot \omega_i \cdot \xi[i]$. Finally, C picks a target identity ID^*, and sets the public key $pk_1 = g^\alpha$, $pk_2 = g^\beta$, $w_0 = pk_2^{-l_2 \cdot k_2 + \gamma_0} \cdot g^{\omega_0}$, $w_i = pk_2^{\gamma_i} \cdot g^{\omega_i}$, $1 \le i \le n_2$, and sends the use's identity ID^* and his/her public key to A_{II}.

Note that $v_0^{Y_0} \prod_{i=1}^{n} v_i^{Y_i \cdot v[i]} = pk_2^{K(v,Y)} g^{L(v,Y)}$. Furthermore, there is no additional trapdoor information for C. Although C knows the power of u_i, $1 \le i \le n_1$, it cannot give C additional information because that adversary A_{II} has the ability of generation psk.

Public-key-extract-queries: C keeps a list L to stores user's ID, public key and secret key. Received a query for a public key on an ID, C searches L to find the corresponding pk, otherwise, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L, and sends pk to A_{II}.

Secret-key-extract-queries: Received a query for a public key on an ID ($\neq ID^*$), C searches L to find the corresponding pk, otherwise, C generates a public key by using UserKeyGen phase in subsection 4.2 and stores the value (ID, pk, sk) in the L, and sends sk to A_{II}.

Sign-queries: If $ID \neq ID^*$, C searches L to find the corresponding pk, if the ID is not in the L, C generates a public key by using UserKeyGen phase in subsection 4.2, and stores the value (ID, pk, sk) in the L, so C knows the psk, and sk, and can sign any message m.

If $ID = ID^*$, if $K(m, msk_2) = 0 \bmod l_2$ aborts. Otherwise, which implies that $K(m, msk_2) \neq 0 \bmod p$, C knows the psk, and picks two random numbers $r_1, r_2 \in Z_p$, computes $\sigma_1 = psk_1 \cdot pk_1^{-L(m)/K(m)} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2}$, $\sigma_2 = pk_1^{-1/K(m)} \cdot g^{r_2}$, $\sigma_3 = psk_2$, $\sigma_4 = (d_0, d_1, \ldots, d_{n_2})$, and sends $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ to A_{II}. The correctness of σ is because that:

$$
\begin{aligned}
\sigma_1 &= psk_1 \cdot pk_1^{-L(m)/K(m)} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2} \\
&= psk_1 \cdot pk_2^{\alpha} \cdot (pk_2^{K(m)} \cdot pk_1^{L(m)/\alpha})^{-\alpha/K(m)} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2} \\
&= psk_1 \cdot pk_2^{\alpha} \cdot (pk_2^{K(m)} \cdot g^{L(m)})^{-\alpha/K(m)} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2} \\
&= psk_1 \cdot pk_2^{\alpha} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{-\alpha/K(m)} \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2} \\
&= psk_1 \cdot sk_1 \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{r_2 - \alpha/K(m)} \\
&= psk_1 \cdot sk_1 \cdot (w_0^{x_0} \cdot \prod_{i=1}^{n_2} w_i^{x_i \cdot m[i]})^{\tilde{r}_2} \\
\sigma_2 &= pk_1^{-1/K(m)} \cdot g^{r_2} = g^{r_2 - \alpha/K(m)} = g^{\tilde{r}_2}, \text{ where } \tilde{r}_2 = r_2 - \alpha/K(m).
\end{aligned}
$$

Solving the CDH problem:

If A_{II} outputs a forged signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*)$ with an identity ID^* on message m^*, if C does not terminate during the simulation, and satisfies the follows conditions:

1. (ID^*, m^*) is never submitted to the signing queries;
2. σ^* is correct signature on message m^*.

If $K(m^*, msk_2) \neq 0 \bmod p$, aborts. Otherwise $K(m^*) = 0 \bmod p$, C can compute $g^{\alpha \cdot \beta} = \sigma_1^* \cdot ((\sigma_2^*)^{L(m^*)} \cdot (\sigma_3^*)^{\alpha_0 + \sum_{i=1}^{n_1} \alpha_i \cdot (ID^* \| pk^*)[i])} \cdot g_2^{x})^{-1}$. It is because that:

$$
e(\sigma_1, g) = e(\sigma_2^*, (d_0^* \cdot \prod_{i=1}^{n_2} (d_i^*)^{m^*[i]}) \cdot e(\sigma_3^*, u_0 \cdot \prod_{i=1}^{n_1} u_i^{(ID^* \| pk^*)[i]}) \cdot e(g_1, g_2) \cdot e(pk_1^*, pk_2^*)
$$

$$= e(\sigma_2^*, g_2^{K(m^*)} g^{L(m^*)}) \cdot e(\sigma_3^*, g^{\alpha_0} \cdot \prod_{i=1}^{n_1} (g^{\alpha_i})^{(ID^* \| pk^*)[i]}) \cdot e(g^x, g_2) \cdot e(pk_1^*, pk_2^*)$$

$$= e(\sigma_2^*, g^{L(m^*)}) \cdot e(\sigma_3^*, g^{\alpha_0 + \sum_{i=1}^{n_1} \alpha_i \cdot (ID^* \| pk^*)[i])}) \cdot e(g, g_2^x) \cdot e(g^\alpha, g^\beta)$$

$$= e((\sigma_2^*)^{L(m^*)}, g) \cdot e((\sigma_3^*)^{\alpha_0 + \sum_{i=1}^{n_1} \alpha_i \cdot (ID^* \| pk^*)[i])}, g) \cdot e(g_2^x, g) \cdot e(g^{\alpha \cdot \beta}, g)$$

$$= e((\sigma_2^*)^{L(m^*)} \cdot (\sigma_3^*)^{\alpha_0 + \sum_{i=1}^{n_1} \alpha_i \cdot (ID^* \| pk^*)[i])} \cdot g_2^x \cdot g^{\alpha \cdot \beta}, g)$$

Now, we discuss the success probability of solving the CDH problem. *C* Will not abort during the proof if the following conditions satisfied simultaneously.

1. $ID \neq ID^*$ in the secret-key-extract-queries;
2. $ID = ID^*$ and $K(m) \neq 0 \bmod l_2$ or $ID \neq ID^*$ in the sign-queries;
3. $K(m^*) = 0 \bmod p$, in the forged signature phase.

The probability that $ID \neq ID^*$ in the secret-key-extract-queries is $(q_{sk} - 1)/q_{sk}$. Similar to the probability analysis in subsection 5.1, the probability of *C* not abort is at least $(q_{sk} - 1) \cdot (4 \cdot q_{sk} \cdot q_s \cdot (n_2+1))^{-1}$.

6. CONCLUSIONS

In smart city, digital signature is an important cryptographic tool which is used to protect the security and privacy. In this paper, we have reviewed the Pang *et al.*'s certificateless signature scheme, and point out their scheme is vulnerable to the attack of malicious-but-passive KGC adversary. Then we propose a strongly secure certificateless signature scheme, and give the secure proof in standard model. Compared Pang *et al.*'s [38] and other certificateless signature scheme [30, 33, 35] in standard model, Although the computational cost of our proposed scheme is slightly larger, our proposed scheme can resist attack of malicious-but-passive KGC adversary. Furthermore, we give a suggestion for proof the certificateless signature resisting malicious-but-passive KGC attack, *i.e.*, we cannot remain some possible trapdoor information for KGC.

ACKNOWLEDGMENT

This work was supported by the Middle-aged and Young Teacher Education and Scientific Research Project for the Education Department of Fujian Province (Grant No. JA15349), the Natural Science Foundation of Fujian Province of China (No. 2016-J01277), National Natural Science Foundation of China (Nos. 61072080, U1405255), Fujian Normal University Innovative Research Team (No. IRTL1207), Major science and technology project in Fujian province (No. 2014H61010105), Project of Fuzhou Municipal Bureau of Science and Technology (No. 2015-G-59), Project of Industry-Academic Cooperation of Fujian Provincial Department of Science and Technology (No. 2017H6005), Project of the Education Department of Fujian Province (No. JAT-160123), the 13th Five-Year Plan of Fujian Province science of education-the key annual research topics of 2016 (No. FJJKCGZ16-018).

REFERENCES

1. S. Djahel, R. Doolan, G. M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches," *IEEE Communications Surveys and Tutorials*, Vol. 17, 2015, pp. 125-151.
2. Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data overcollection in smart city," *IEEE Transactions on Computers*, Vol. 65, 2016, pp. 1339-1350.
3. S. Ijaz, M. A. Shah, A. Khan, and M. Ahmed, "Smart cities：a survey on security concerns," *International Journal of Advanced Computer Science and Applications*, Vol. 7, 2016, pp. 612-625.
4. N. Saputro and K. Akkaya, "PARP-S: A secure piggybacking-based ARP for IEEE 802.11s-based smart grid AMI networks," *Computer Communications*, Vol. 58, 2015, pp. 16-28.
5. D. M. Menon, and N. Radhika, "Design of a secure architecture for last mile communication in smart grid systems," *Procedia Technology*, Vol. 21, 2015, pp. 125-131.
6. A. Amamra, C. Talhi, and J. M. Robert, "Smartphone malware detection: from a survey towards taxonomy," in *Proceedings of the 7th International Conference on Malicious and Unwanted Software*, 2012, pp. 79-86.
7. L. Sancheza, L. Muñoza, J. A. Galachea, P. Sotresa, J. R. Santanaa, V. Gutierreza, R. Ramdhanyb, A. Gluhakc, S. Krcod, E. Theodoridise, and D. Pfistererf, "SmartSantander: IoT experimentation over a smart city testbed," *Computer Networks*, Vol. 61, 2014, pp. 217-238.
8. S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the 9th International Conference on Theory and Application of Cryptology and Information Security*, 2003, pp. 452-473.
9. H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blazes, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schilier, and B. Schneier, "The risks of key recovery, key escrow, and trusted third-party encryption," http://www.schneier.com/paper-key-escrow.pdf, 1997,
10. A. Shamir, "Identity based cryptosystems and signature schemes," in *Proceedings of the 4th Annual International Cryptology Conference*, 1984, pp. 47-53.
11. Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Towards efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Transactions on Information Forensics and Security*, 2016, DOI: 10.1109/TIFS.2016.2596138.
12. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, 2016, pp. 2546-2559.
13. Q. Zheng , X. Li, and A. Azgin, "CLKS: Certificateless keyword search on encrypted data, " in *Proceedings of the 9th International Conference on Network and System Security*, 2015, pp. 239-253.
14. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel*

and Distributed Systems, Vol. 27, 2016, pp. 340-352.
15. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, Vol. E98-B, 2015, pp. 190-200.
16. T. Y. Wu, T. T. Tsai, and Y. M. Tseng, "Efficient searchable ID-based encryption with a designated server," *Annals of Telecommunications*, Vol. 69, 2014, pp. 391-402.
17. X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from Asiacrypt 2003," in *Proceedings of the 4th International Conference on Cryptology and Network Security*, 2005, pp. 13-25.
18. Z. Zhang and D. Wong, "Certificateless public key signature: Security model and efficient construction," in *Proceedings of the 4th International Conference on Applied Cryptography and Network Security*, 2006, pp. 293-308.
19. M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Proceedings of the 2nd International Conference on Computational and Information Science*, 2005, pp. 110-116.
20. L. Harn, J. Ren, and C. L. Lin, "Design of DL-based certificateless digital signatures," *Journal of Systems and Software*, Vol. 82, 2009, pp. 789-793.
21. D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *International Journal of Communication Systems*, Vol. 25, 2011, pp. 1432-1442.
22. M. M. Tian and L. S. Huang. "Cryptanalysis of a certificateless signature scheme without pairings," *International Journal of Communication Systems*, Vol. 26, 2013, pp. 1375-1381.
23. J. L. Tsai, N. W. Lo, and T. C. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *International Journal of Communication Systems*, Vol. 27, 2014, pp. 1083-1090.
24. P. Gong and P. Li, "Further improvement of a certificateless signature scheme without pairing," *International Journal of Communication Systems*, Vol. 27, 2014, pp. 2083-2091.
25. M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in *Proceedings of the 2nd ACM Symposium on Information*, *Computer and Communications Security*, 2007, pp. 302-311.
26. K. S. Kim and I. R. Jeong, "A new certificateless signature scheme under enhanced security models," *Security and Communication Networks*, Vol. 8, 2015, pp. 801-810.
27. R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, Vol. 51, 2004, pp. 557-594.
28. R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *Proceedings of the 18th Annual International Cryptology Conference*, 1998, pp. 13-25.
29. B. Waters, "Efficient identity based encryption without random oracles," in *Proceedings of EUROCRYPT*, 2005, pp. 114-127.
30. J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," in *Proceedings of the 2nd ACM Symposium on Information*, *Computer and Communications Security*, 2007, pp. 273-283.
31. H. Xiong, Z. Qin, and F. Li, "An improved certificateless signature scheme secure in

the standard model," *Fundamenta Informaticae*, Vol. 88, 2008, pp. 193-206.
32. Q. Huang and D. S. Wong, "Generic certificateless encryption secure against malicious-but-passive KGC attacks in the standard model," *Journal of Computer Science and Technology*, Vol. 25, 2010, pp. 807-826.
33. Y. Yuan, D. Li, L. Tian, and H. Zhu, "Certificateless signature scheme without random oracles," in *Proceedings of the 3rd International Conference on Security Assurance*, 2009, pp. 31-40.
34. Q. Xia, C. X. Xu, and Y. Yu, "Key replacement attack on two certificateless signature schemes without random oracles," *Key Engineering Materials*, 2010, Vol. 439-440, pp. 1606-1611.
35. Y. Yu, Y. Mu, G. Wang, Q. Xia, and B. Yang, "Improved certificateless signature scheme provably secure in the standard model," *IET Information Security*, Vol. 6, 2012, pp. 102-110.
36. L. Cheng, Q. Wen, Z. Jin, and H. Zhang, "On the security of a certificateless signature scheme in the standard model," 2013, https://eprint.iacr.org/2013/153.pdf.
37. Y. Yuan and C. Wang, "Certificateless signature scheme with security enhanced in the standard model," *Information Processing Letters*, Vol. 114, 2014, pp. 492-499.
38. L. Pang, Y. Hu, Y. Liu, K. Xu, and H. Li, "Efficient and secure certificateless signature scheme in the standard model," *International Journal of Communication Systems*, 2015, DOI: 10.1002/dac.3041.
39. U. Parampalli and S. Narayan, "Efficient identity-based signatures in the standard model," *IET Information Security*, Vol. 2, 2008, pp. 108-118.
40. F. Bao, R. H. Deng, and H. F. Zhu, "Variations of Diffie-Hellman problem," in *Proceedings of the 5th International Conference on Information and Communications Security*, 2003, pp. 301-312.

Feng Wang was born in Shandong province, China, in 1978. He received his B.S. degree in Mathematics from Yantai Normal University (now named Ludong University), Yantai, in 2000 and the M.S. degree in Applied Mathematics from the Guangzhou University, Guangzhou, in 2006. He was a visiting scholar in Department of Information Engineering and Computer Science at Feng Chia University from November 2012 to October 2013. Currently, he is an Associate Professor in the College of Mathematics and Physics at Fujian University of Technology, and pursuing his Ph.D. degree in Applied Mathematics from Fujian Normal University. His research interests include computer cryptography, network and information security, *etc.*

Li Xu is a Professor and Doctoral Supervisor at the School of Mathematics and Computer Science at Fujian Normal University. He received his B.S and M.S degrees from Fujian Normal University in 1992 and 2001. He received the Ph.D. degree from the Nanjing University of Posts and Telecommunications in 2004. Now he is the Vice Dean of School of Math and Computer Science and

Director of Key Lab of Network Security and Cryptography in Fujian Province. His interestes include network and information security, wireless network and communication, complex network and system, intelligent information in communication network, *etc.* Prof. Xu has been invited to act as PC chair or member at more than 30 international conferences. He is a member of IEEE and ACM, and a senior member of CCF and CIE in China. His research results have been published in more than 150 papers in international journals and conferences, including IEEE Transactions on Computer, ACM Transactions on Sensor Network, IEEE Transactions on Reliability, IEEE Transactions on Parallel and Distributed Systems, Information Science, and Computer Network. Contact him at email: xuli@fjnu.edu.cn.