J. Shanghai Jiaotong Univ. (Sci.), 2011, 16(5): 577-585
DOI: 10.1007/s12204-011-1192-6

Certificateless Message Recovery Signatures Providing Girault's Level-3 Security

TSO Ray-lin[1*] (左瑞麟), *KIM Cheonshik*[2], *YI Xun*[3] (易 训)
(1. Department of Computer Science, National Chengchi University, Taipei 11605;
2. Department of Computer Engineering, Sejong University, Seoul 143-747, Korea;
3. School of Engineering and Science, Victoria University, Melbourne 8001, Australia)

Abstract: A digital signature with message recovery is a signature that the message itself (or partial of the message) is not required to be transmitted together with the signature. It has the advantage of small data size of communication comparing with the traditional digital signatures. In this paper, combining both advantages of the message recovery signatures and the certificateless cryptography, we propose the first certificatelss signature scheme with message recovery. The remarkable feature of our scheme is that it can achieve Girault's Level-3 security while the conventional certificateless signature scheme only achieves Level-2 security. The security of the scheme is rigorously proved in the random oracle model based on the hardness of the k bilinear Diffie-Hellman inverse (k-BDHI) problem.
Key words: bilinear pairing, certificateless, digital signature, message recovery, random oracle
CLC number: TP 309 **Document code:** A

0 Introduction

A digital signature scheme with message recovery[1-3] is a special kind of signature scheme. In such a scheme, one encodes a part of the message into the signature. The encoded part of the message is not required to be transmitted together with the signature since it can be recovered according to the verification/message-recovery process. In this way, the total length of the message and the appended signature can be reduced. This kind of signatures are useful for an organization where bandwidth is one of the main concerns, or useful for the applications in which small messages should be signed. Message recovery signatures are also useful on wireless devices such as personal digital assistants (PDAs), cell phones, radio frequency identification (RFID) chips and sensors. This is because battery life is usually the main limitation on these devices so an efficient communication protocol is always required. Message recovery signatures can reduce the number of bits for communication. For example, a 320-bit signature is enough for a 100-bit message. In this way, we can save the power and increase battery life for such devices.

On the other hand, certificateless cryptography, which was first introduced by Al-Riyami and Paterson[4], is intended to solve the key escrow problem inherent in ID-based cryptography[5-6] in which users have to fully trust on the ID-based key generation center (KGC). Moreover, certificateless cryptography can also eliminate the use of certificates as in the conventional public key infrastructure (PKI) which is usually considered to be costly to use and manage. Following the pioneer work of Al-Riyami and Paterson, many researches have been done in the field of certificateless cryptography[7-11].

Other than the message recovery signatures, the other technique to shorten the total length of a signature and the corresponding message is called "short signatures". The technique of this kind of signatures is to shorten the signature directly while preserving the same level of security. It was first proposed by Boneh et al[5]. Comparing with the message recovery signatures, one disadvantage of short signatures is the deterministic signing algorithm. This means that given a particular message as input to a short signature scheme, it will always produce the same output as the signature. On the other hand, the signing algorithm of a message recovery signature scheme is randomized, which means that the output (i.e., signatures) will always be different even if the input (i.e., message) remains the same. Taking advantage of the certificateless cryptography, some certificateless short signature schemes have been proposed[8-9].

Received date: 2011-02-10
∗**E-mail:** raylin@cs.nccu.edu.tw

Additionaly, Girault[12] described three security levels to classify the level of trust to the trusted third party (TTP). In the context of the certificcteless cryptograpy, KGC is the TTP. The three levels are defined as follows. Level-1: the KGC knows the secret of any user. Level-2: the KGC cannot find out all the information of a user's secret. However, the KGC can generate a contradictory public key (or contradictory certificate) and impersonate the user to generate signatures with respect to the contradictory public key. Level-3: the KGC cannot find out all the information of a user's secret nor generate the contradictory public key. The KGC can only generate a valid public key (or valid certificate).

The higher the security level is, the lower the trust to the KGC is assumed. ID-based cryptography can achieve only Level-1 security since the KGC knows all the secret of any user. PKI-based cryptography can achieve Level-3 security since certificates are used in PKI and certificates can only be generated by the certificate authority (CA). Hence, if there are two certificates with their corresponding public keys for the same user, we know that the CA must have misbehaved. However, a conventional certificateless cryptography can achieve Level-2 security only. That is because the KGC can actually generate user public/secret key pair to impersonate a user and there is no way for the user to show that the KGC is misbehaving if the same user already has a user public key published. This inspires us to have a certificateless message recovery signature scheme that can achieve the Girault's Level-3 security.

In this paper, we propose the first message recovery signatures in the certificateless setting. Moreover, our certificateless message recovery signature scheme can satisfy the Girault's Level-3 security while the conventional certificateless cryptography can achieve only Level-2 security. Based on the hardness of the k bilinear Diffie-Hellman inverse (k-BDHI) problem and the unforgeability of some ID-based signatures, the security is regiously proved in the random oracle model.

1 Preliminaries

1.1 Bilinear Pairings and the Related Computational Assumptions

Let G and G_T be two multiplicative cyclic groups of order q (q is a large prime number). Our certificiteless message recovery signature scheme makes use of the bilinear map $\hat{e} : G \times G \to G_T$ between these two groups. The bilinear map should be satisfied with the following properties.

Bilinear A map $\hat{e} : G \times G \to G_T$ is bilinear if $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$ for all $g, h \in G$ and $a, b \in \mathbf{Z}_q^*$. Here $\mathbf{Z}_q^* = \{1, 2, \cdots, q-1\}$.

(1) Non-degenerate. The map does not send all pairs in $G \times G$ to the identity in G_T. Since G and G_T are groups of prime order, this implies that if g is a generator of G, $\hat{e}(g, g)$ is a generator of G_T.

(2) Computable. There is an efficient algorithm to compute $\hat{e}(g, h)$ for any $g, h \in G$.

A bilinear map satisfying the two properties above is said to be an admissible bilinear map. We can make this map using the Weil pairing or the Tate pairing[5,13-14].

Next, we describe a hardness problem related to bilinear pairing which is named the bilinear Diffie-Hellman inverse (BDHI) problem[8]. It is required for the security proof of our scheme.

Definition 1 (k-BDHI problem) Let g be a generator of the multiplicative cyclic group G described above, and $a \in \mathbf{Z}_q^*$. Given $(g, g^a, \cdots, g^{a^k}) \in G_1^{k+1}$, output $\hat{e}(g, g)^{a^{-1}} \in G_T$.

The k-BDHI problem is believed to be hard and many cryptographic protocols[3,15-16] have been introduced based on this problem.

1.2 Scheme Model

A certificateless signature scheme with message recovery is defined by five polynomial-time algorithms. Note that the input of the user partial private key generation algorithm is different from the conventional certificateless signature schemes in order to satisfy the Girault's Level-3 security.

(1) Setup. On input a security parameter $\lambda \in \mathbf{N}$, the randomized algorithm generates a master secret key msk of KGC and the system parameter, params. The system parameter params is then made public to users of the system while msk is made secret and is only known by KGC.

(2) UserKeyGen. On input the system parameter params and a user identity ID$\in \{0, 1\}^*$, the randomized algorithm generates a user public key $\mathrm{PK_{ID}}$ and the corresponding secret value x_{ID} for ID.

(3) PartialKeyGen. On input params, the secret key msk of KGC, a user identity ID and the user public key $\mathrm{PK_{ID}}$, the randomized algorithm generates a user partial private key D_{ID} of ID.

Remark 1 In the version of conventional certificateless cryptography, the user public key $\mathrm{PK_{ID}}$ is not required as an input of the algorithm.

(4) Sign. On input params, a user identity ID, the user secret value x_{ID}, the user partial private key D_{ID} and a message $m \in \{0, 1\}^*$, the randomized algorithm generates a message recovery signature σ.

(5) Ver. On input params, a user identity ID, a user public key $\mathrm{PK_{ID}}$, a message m and a signature σ, the randomized algorithm returns 1 for accept or 0 for reject the signature.

For correctness, it is required that if

$$(\text{params, msk}) \leftarrow \text{Setup}(1^{\lambda}),$$
$$(\text{PK}_{\text{ID}}, x_{\text{ID}}) \leftarrow \text{UserKeyGen}(\text{params, ID}),$$
$$D_{\text{ID}} \leftarrow \text{PartialKeyGen}(\text{msk, ID, PK}_{\text{ID}}),$$

and

$$\sigma \leftarrow \text{Sign}(x_{\text{ID}}, D_{\text{ID}}, m),$$

then

$$\text{Ver}(\text{params, ID, PK}_{\text{ID}}, m, \sigma) = 1.$$

1.3 Security Definition

For certificateless cryptosystems, there are two types of adversaries with different capabilities according to the widely-accepted notion of security defined by Al-Riyami and Paterson[4].

Type I Adversary This type of adversary A_{I} models a possible cheating user who is able to compromise the user secret value or replace the user public key, but is not able to access the master secret key msk and the user partial private key.

Type II Adversary This type of adversary A_{II} models a possible cheating KGC who is able to know the master secret key msk and the user partial private key, but cannot know the user secret value or replace the user public key.

Additionally, there are five oracles that can be accessed by the adversaries according to the game specifications which will be given shortly.

(1) CreateUser. On input an identity ID $\in \{0, 1\}^*$, if ID has been created, nothing is to be carried out. Otherwise, the oracle generates

$$D_{\text{ID}} \leftarrow \text{PartialKeyGen}(\text{msk, ID, PK}_{\text{ID}}),$$
$$(\text{PK}_{\text{ID}}, x_{\text{ID}}) \leftarrow \text{UserKeyGen}(\text{params, ID}).$$

In this case, ID is said to be created and in both cases, PK_{ID} is returned.

(2) PartialKeyExtract. On input an identity ID, the oracle returns the corresponding partial private key D_{ID} if ID has been created. Otherwise, returns an error symbol $\perp$.

(3) SecretValueExtract. On input an identity ID, it returns the corresponding user secret value x_{ID} if ID has been created. Otherwise, returns an error symbol $\perp$.

(4) ReplaceKey. On input an identity ID and a user public key PK_{ID^*}, the original user public key PK_{ID} of ID is replaced with PK_{ID^*} if ID has been created. Otherwise, nothing will be taken.

(5) Sign. On input an identity ID and a message $m \in \{0, 1\}^*$, it returns a valid signature σ if ID has been created. The signature is valid if Ver(params, m, σ, ID, PK_{ID}) = 1. Here PK_{ID} is the original public key generated from the oracle CreateUser. Otherwise, an error symbol $\perp$ is returned.

We define two games to capture the notion of existential unforgeability against chosen message attack (EUF-CMA)[11] of a certificateless signature, one for the Type I adversary A_{I} and the other one for the Type II adversary A_{II}.

Game 1 Let S_{I} be the game simulator/challenger and λ be a security parameter.

(1) Setup. The algorithm $\text{Setup}(1^{\lambda})$ of the certificateless signature scheme is executed by S_{I} to get the public parameter params and the master secret key msk.

(2) Queries. Simulator/challenger S_{I} runs A_{I} on 1^{λ} and params. During the simulation, A_{I} can adaptively make queries onto all the oracles defined above of this section in a polynomial number of times.

(3) Forgery. Adversary A_{I} outputs a forgery (ID*, PK_{ID^*}, m^*, σ^*) and wins the game if the following conditions hold ture:

① $\text{Ver}(\text{params, ID}^*, \text{PK}_{\text{ID}^*}, m^*, \sigma^*) = 1$;

② (ID*, m^*) has never been submitted to the oracle Sign;

③ A_{I} has never queried PartialKeyExtract(ID*) or SecretValueExtract(ID*) to get the user partial private key or the user secret value.

A certificateless signature scheme is secure against the Type I adversary if for all the probabilistic polynomial time (PPT) algorithm A_{I}, A_{I} wins Game 1 with negligible probability.

Game 2 Let S_{II} be the game simulator/challenger, it simulates the game in a similar way to that of S_{I} in Game 1 with the other adversary A_{II}, except the following differences:

(1) When running A_{II}, besides giving params to A_{II}, the master secret key msk is also given to A_{II}.

(2) At the forgery phase, the third restriction of Game 1 is changed here to require that A_{II} has never queried SecretValueExtract(ID*) to get the secret value nor queried ReplaceKey(ID*) to replace the user public key.

A certificateless signature scheme is secure against the Type II adversary if for all the PPT algorithm A_{II}, A_{II} wins Game 2 with negligible probability.

Definition 2 A certificateless signature scheme is existentially unforgeable against chosen message and chosen identity attack (EUF-CMA-IDA) if it is secure against both the Type I and Type II attacks defined above.

However, a certificateless signature scheme secure against the Type I and Type II adversaries does not mean that it achieves the Girault's Level-3 security. This is because in Game 2, we disallow the KGC to query the oracle ReplaceKey, otherwise KGC will always win the game by the knowledge of both the user partial private key and the user secret value. Remind

that the Girault's Level-3 security says that if the CA misbehaves by generating a contradictory public key for a user who already has generated his public key, then the CA can easily be caught. In the traditional PKI setting, this can be easily achieved since both the two public keys have valid certificates and only the CA can generate certificates. We therefore should have an additional security requirement to capture the model of the Girault's Level-3 security in certificateless setting. That is, we should disallow anyone except the KGC to generate a valid user secret value for every newly-generated user public key. Consequently, if there are two public keys that are valid at the same time, then we know that they must be generated by the KGC instead of the user itself.

Following Hu et al.'s work[7], we define a new game to capture the adversarial model as follows.

Game E Let S_{E} be the game simulator/challenger and λ be a security parameter.

(1) Setup. The algorithm Setup(1^{λ}) of the certificateless signature scheme is executed by S_{E} to get the public parameter params and the master secret key msk.

(2) Queries. Then S_{E} runs adversary A_{E} on 1^{λ} and params. During the simulation, A_{E} can adaptively make queries onto the oracle PartialKeyExtract on input an ID and a public key $\mathrm{PK_{ID}}$ in a polynomial number of times. The output is the corresponding partial private key D_{ID}.

Remark 2 To capture the Girault's Level 3 security, in this game, the oracle PartialKeyExtract is slightly modified on its input (ie., other than ID, the public key $\mathrm{PK_{ID}}$ is also required as one of the input).

(3) Forgery. Adversary A_{E} outputs (ID^*, $\mathrm{PK_{ID^*}}$, D_{ID^*}) and wins the game if following conditions hold true: key D_{ID^*} is in the set of all possible values of the user partial private key generated by PartialKeyGen for some D_{ID^*}; the oracle PartialKeyExtract has never been queried with (ID^*, $\mathrm{PK_{ID^*}}$).

Definition 3 A certificateless signature scheme is said satisfying the Girault's Level-3 security if for all the PPT algorithm A_{E}, the probability of A_{E} to win Game E is negligible.

2 The Proposed Scheme

The following notations will be used throughout this paper: $a\|b$ denotes concatenation of strings a and b; $\oplus$ denotes X-OR operation in the binary system; $_{\ell_2}|\beta|$ denotes the most significant ℓ_2-bit of β; $|\beta|_{\ell_1}$ denotes the least significant ℓ_1-bit of β; $|m|$ denotes the bit-length of a message m.

In this section, we present our certificateless message recovery signature scheme which can be used for messages of arbitrarily length.

(1) Setup. This algorithm is run by KGC. On input the system security parameter 1^{λ}, the KGC generates a bilinear group G of prime order q. Let $\hat{e}: G\times G\to G_T$ be a bilinear pairing. The generator of G is g, and $\hat{e}(g, g)=\mu$. KGC also picks a random number $s\in\mathbf{Z}_q^*$ as its master secret key and then sets $P_{\mathrm{pub}}=g^s$. It then picks four distinct cryptographic hash functions

$$F_1: \{0,1\}^{\ell_1}\to\{0,1\}^{\ell_2},$$
$$F_2: \{0,1\}^{\ell_2}\to\{0,1\}^{\ell_1},$$
$$H_0: \{0,1\}^{*}\to\mathbf{Z}_q^*,$$
$$H_1: \{0,1\}^{*}\to\mathbf{Z}_q^*.$$

It sets

$$\text{params}=\{\lambda, G, G_T, q, \hat{e}, g, \mu, P_{\mathrm{pub}}, F_1, F_2, H_0, H_1\}$$

public as the system parameter and keeps secretly the master secret key msk $=s$.

(2) UserKeyGen. This algorithm is run by a user with identity information ID. On input the system parameter params, a user with identity ID runs this algorithm to get a randomly picked secret value $x\in\mathbf{Z}_q^*$ and then computes $Q_{\mathrm{ID}}=H_0(\mathrm{ID})$ and the public key $\mathrm{PK_{ID}}=(\mathrm{PK}_1, \mathrm{PK}_2)=(g^x, g^{x(s+Q_{\mathrm{ID}})})$. Note that PK_2 can be computed by ID using the form $(P_{\mathrm{pub}}g^{Q_{\mathrm{ID}}})^x$.

(3) PartialKeyGen. This algorithm is run by KGC for a user with identity information ID. On input the system parameter params and the user information (Q_{ID}, $\mathrm{PK_{ID}}$), the output is the partial private key $D_{\mathrm{ID}}=g^{s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1)^{-1}}$. KGC then transmits D_{ID} to ID over a confidential and authentic channel.

(4) Sign. To sign a message $m\in\{0,1\}^*$, the signer with identity ID does the following steps:

① Parse m into $m=m_2\|m_1$. If $|m|=\ell_1$, $m_1=m$ and $m_2=\varnothing$. If $|m|>\ell_1$, $|m_1|=\ell_1$.

② Pick a random number $r_1\in\mathbf{Z}_q^*$, compute $\mu^{r_1}\in G_T$ and

$$\alpha=H_1(\mathrm{ID}\|\mu^{r_1}\|\mathrm{PK_{ID}}\|m_2).$$

③ Compute

$$\beta=F_1(m_1)\|(F_2(F_1(m_1))\oplus m_1).$$

④ Compute $r_2=\alpha\oplus\beta$, $H_0(\mathrm{ID}\|\mathrm{PK_{ID}})$ and

$$U=D_{\mathrm{ID}}^{(r_1+r_2)(x+H_0(\mathrm{ID}\|\mathrm{PK_{ID}}))^{-1}}.$$

⑤ Output the message recovery signature σ on m as $\sigma=(r_2, U)$.

(5) Ver. Given the system parameter params, a partial message m_2 (in case when $|m|>\ell_1$), the signer's identity ID, the public key $\mathrm{PK_{ID}}$ and the signature σ, any verifier first verifies the correctness of $\mathrm{PK_{ID}}$ by

$$\hat{e}=(\mathrm{PK}_1, P_{\mathrm{pub}}g^{Q_{\mathrm{ID}}})=\hat{e}(g, \mathrm{PK}_2).$$

If it holds, the verifier then verifies the signature and recovers the message via the following steps:

① Compute

$$\pi = \hat{e}(U, \mathrm{PK}_2\mathrm{PK}_1^{H_0(\mathrm{ID}\|\mathrm{PK}_1)} \times (P_{\mathrm{pub}} g^{Q_{\mathrm{ID}}} g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)})^{H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})}) \mu^{-r_2}.$$

② Compute

$$\alpha = H_1(\mathrm{ID}\|\pi\|\mathrm{PK}_{\mathrm{ID}}\|m_2).$$

③ Compute

$$\beta = \alpha \oplus r_2.$$

④ Recover

$$m_1 = |\beta|_{\ell_1} \oplus F_2(\ell_2|\beta|).$$

⑤ Accept the signature σ if and only if $\ell_2|\beta| = F_1(m_1)$. Otherwise, reject σ.

⑥ Recover the original message $m = m_2\|m_1$.

Correctness The correctness of the scheme can be verified as

$$\begin{aligned}
&\pi = \hat{e}(U, \mathrm{PK}_2\mathrm{PK}_1^{H_0(\mathrm{LD}\|\mathrm{PK}_1)}(P_{\mathrm{pub}} g^{Q_{\mathrm{ID}}} \times \\
&g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)})^{H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})}) \mu^{-r_2} = \\
&\hat{e}(D_{\mathrm{ID}}^{(r_1+r_2)(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}}))^{-1}}, \\
&\mathrm{PK}_2\mathrm{PK}_1^{H_0(\mathrm{ID}\|\mathrm{PK}_1)}(P_{\mathrm{pub}} g^{Q_{\mathrm{ID}}} \times \\
&g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)})^{H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})}) \mu^{-r_2} = \\
&\hat{e}(g^{(r_1+r_2)(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))^{-1}(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}}))^{-1}}, \\
&\mathrm{PK}_2\mathrm{PK}_1^{H_0(\mathrm{ID}\|\mathrm{PK}_1)}(P_{\mathrm{pub}} g^{Q_{\mathrm{ID}}} \times \\
&g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)})^{H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})}) \mu^{-r_2} = \\
&\hat{e}(g^{(r_1+r_2)(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))^{-1}(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}}))^{-1}}, \\
&g^{x(s+Q_{\mathrm{ID}})} g^{xH_0(\mathrm{ID}\|\mathrm{PK}_1)}(g^s g^{Q_{\mathrm{ID}}} \times \\
&g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)})^{H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})}) \mu^{-r_2} = \\
&\hat{e}(g^{(r_1+r_2)(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))^{-1}(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}}))^{-1}}, \\
&g^{x(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))} \times \\
&\mu^{-r_2} = \hat{e}(g^{(r_1+r_2)((s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}})))^{-1}}, \\
&g^{(s+Q_{\mathrm{ID}}+H_0(\mathrm{ID}\|\mathrm{PK}_1))(x+H_0(\mathrm{ID}\|\mathrm{PK}_{\mathrm{ID}}))}) \mu^{-r_2} = \\
&\hat{e}(g^{(r_1+r_2)}, g)\mu^{-r_2} = \hat{e}(g, g)^{r_1} = \mu^{r_1}.
\end{aligned}$$

If σ is valid, then

$$H_1(\mathrm{ID}\|\pi\|\mathrm{PK}_{\mathrm{ID}}\|m_2) = \alpha$$

and

$$F_1(m_1)\|(F_2(F_1(m_1)) \oplus m_1) = \beta = \alpha \oplus r_2.$$

Hence, we obtain

$$\begin{aligned}
&|\beta|_{\ell_1} \oplus F_2(\ell_2|\beta|) = \\
&\quad (F_2(F_1(m_1)) \oplus m_1) \oplus F_2(F_1(m_1)) = m_1.
\end{aligned}$$

Finally, the integrity of m_1 is justified if

$$\ell_2|\beta| = F_1(m_1).$$

3 Security Proofs

We will show that the scheme is EUF-CMA secure against the Type I and Type II adversaries in the random oracle model, assuming the hardness of k-BDHI problem. In addition, we will show the scheme achieves the Girault's Level-3 security.

Theorem 1 (unforgeability against the Type I adversary) If there exists an adversary A_{I} who can break the unforgeability of the proposed scheme via the Type I attack, then we can construct another adversary F such that F can use A_{I} as a black box and solve the k-BDHI problem.

Let a be a random number of $\mathbf{Z}_q^*$. Adversary F is given parameters of pairing $(g, \hat{e}, G, G_T)$ defined at Section 2 and the challenge $(g, g^a, \cdots, g^{a^k})$. The purpose of F is to find $\hat{e}(g, g)^{a^{-1}} \in G_T$ which is the solution to the k-BDHI problem.

(1) Setup. Adversary F will simulate the environments of the proposed scheme and the oracles which A_{I} can access as follows:

① Adversary F randomly chooses $h_0, h_1, \cdots, h_{k-1} \in \mathbf{Z}_q^*$ and $c_0, c_1, \cdots, c_{k-1} \in \mathbf{Z}_q^*$, and computes

$$f(x) = \prod_{i=0}^{k-1}(x + h_i) = \sum_{i=0}^{k-1} c_i x^i.$$

② Adversary F computes

$$\rho = g^{\sum_{i=0}^{k-1} c_i a^i} = g^{f(a)},$$

$$\rho^a = g^{\sum_{i=0}^{k-1} c_i a^{i+1}}, \quad \rho' = g^{\sum_{i=1}^{k-1} c_i a^{i-1}}.$$

We may assume that $\rho \neq 1_G$, the identity element of G. Otherwise, there must have one $h_i = -a$, hence, F can find the value a and output $\hat{e}(g, g)^{a^{-1}}$. So F can solve the k-BDHI problem directly.

③ Adversary F randomly chooses $d_0, d_1, \cdots, d_{k-1} \in \mathbf{Z}_q^*$, and computes

$$f_i(x) = \frac{f(x)}{x + h_i} = \sum_{j=0}^{k-2} d_j x^j.$$

Obviously,

$$\rho^{(a+h_i)^{-1}} = g^{(a+h_i)^{-1} f(a)} = g^{f_i(a)} = g^{\sum_{j=0}^{k-1} d_j a^j}$$

for $1 \leqslant i \leqslant k$.

④ Adversary F randomly chooses an index t, $1 \leqslant t \leqslant k$.

⑤ Adversary F sets the system parameter

$$\text{params} = (G_1, G_2, \hat{e}, q, \rho, P_{\text{pub}}, \mu, H_0, H_1, F_1, F_2, \ell_1, \ell_2),$$

where $P_{\text{pub}} = \rho^{a-h_0}$ and $\mu = \hat{e}(\rho, \rho)$. The hash functions H_0, H_1, F_1 and F_2 are treated as random oracles controlled by F.

(2) Query. During the simulation, A_{I} is allowed to access the following oracles in a polynomial number of times. These oracles are all simulated by F. In addition, we assume that F keeps a list on all input/output for each oracle in order to maintain consistency and to avoid collision.

(3) CreateUser. By giving an identity ID_i, F chooses x_i, $y_i \in_{\text{R}} \mathbf{Z}_q^*$, and sets

$$Q_{\text{ID}_i} = H_0(\text{ID}_i) = y_i,$$

and

$$\text{PK}_{\text{ID}_i} = (\text{PK}_{\text{ID}_i,1}, \text{PK}_{\text{ID}_i,2}) = (\rho^{x_i}, (P_{\text{pub}}\rho^{y_i})^{x_i}).$$

Moreover, there are two cases:

① If $i \neq t$, selects a random θ with $0 < \theta \leqslant k$, and sets

$$H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1}) = h_\theta + h_0 - y_i.$$

In this case, the corresponding secret key is x_i and the partial private key is

$$D_{\text{ID}_i} = \rho^{(a+h_\theta)^{-1}}.$$

② If $i = t$, sets

$$H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1}) = h_0 - y_i.$$

In this case, the corresponding secret key is x_i and the partial private key is $D_{\text{ID}_i} = \perp$ which means that it cannot compute the partial private key.

In both cases, returns $(Q_{\text{ID}_i}, \text{PK}_{\text{ID}_i})$ to A_{I}; $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1})$ is recorded to the H_0-list. Adversary F keeps a C-list to record all the information.

(4) PartialKeyExtract. On input an identity ID_i, if ID_i has been created and $i \neq t$, F returns $D_{\text{ID}_i} = \rho^{(a+h_\theta)^{-1}}$. Otherwise, outputs $\perp$ and terminates the simulation.

(5) ReplaceKey. Adversary A_{I} can query the oracle by given a new public key PK'_{ID_i} chosen by itself to replace the public key PK_{ID_i} of an entity ID_i. Adversary F replaces PK_{ID_i} with PK'_{ID_i} if ID_i has been created. Otherwise, outputs $\perp$.

(6) H_0 query. This query is separated in three cases:

① On input an identity ID_i, output $Q_{\text{ID}_i} = y_i$ if it has been created. Otherwise, output $\perp$.

② On input an identity ID_i and the public key $\text{PK}_{\text{ID}_i,1}$, output a random number $h' \in \mathbf{Z}_q^*$ if ID_i has been created and $\text{PK}_{\text{ID}_i,1}$ is a replaced key chosen by A_{I} (ie., not generated from the oracle CreateUser). If $\text{PK}_{\text{ID}_i,1}$ is generated from the oracle CreateUser, then output $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1}) = h_\theta + h_0 - d_i$ if $i \neq t$, and $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1}) = h_0 - d_i$ if $i = t$. Output $\perp$ in other cases.

③ On input ID_i and PK_{ID_i}, output a random number $\omega_i \in \mathbf{Z}_q^*$ if ID_i has been created. Otherwise, output $\perp$.

Adversary F records all the results in the H_0-list.

(7) H_1 query. On input an identity ID_i, a random value $\pi_i \in G_T$, a public key PK_{ID_i} of ID_i, and a partial message $m_{2_i} \in \{\varnothing, \{0, 1\}^*\}$, output a random $\alpha \in \mathbf{Z}_q^*$. Adversary F records all the results in the H_1-list.

(8) F_1 and F_2 queries. Adversary F simulates these oracles in a similar way to that of the H_1 oracle. On any input of ℓ_1-bit value, F_1 outputs a random number of ℓ_2-bit, and on any input of ℓ_2-bit value, F_2 outputs a random number of ℓ_1-bit.

All the results are recorded into the F_1-list and F_2-list, respectively.

(9) SecretValueExtract. Adversary A_{I} can ask for the secret value corresponding to the original public key generated via the CreateUser. On input an identity ID_i, if ID_i has been created and $i \neq t$, F returns x_i. Otherwise, F outputs $\perp$ and terminates the simulation.

(10) Sign. For a query on input ID_i and a message m, if $\text{ID}_i \neq \text{ID}_t$, F uses the private information (x_i, D_{ID_i}) of ID_i to generate a valid signature σ_i for the message and the identity. If $\text{ID}_i = \text{ID}_t$, F simulates the signature as follows:

① Pick randomly $U \in G$, $r_2 \in \mathbf{Z}$ with $|r_2| \leqslant |q|$.

② Find the values of $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1})$, Q_{ID_i}, and $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i})$ from the H_0-list.

③ Compute

$$\pi = \hat{e}(U, \text{PK}_{\text{ID}_i,2}\text{PK}_{\text{ID}_{i,1}}^{H_0(\text{ID}|_i \| \text{PK}_{\text{ID}_{i,1}})} \times (P_{\text{pub}}\rho^{Q_{\text{ID}_i}}\rho^{H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1})})^{H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i})})\mu^{-r_2}.$$

④ Compute

$$\alpha = r_2 \oplus F_1(m_1) \| (F_2(F_1(m_1)) \oplus m_1).$$

⑤ Check the H_0-list and restart the simulation if $\alpha = H_1(\text{ID}_i \| \pi \| \text{PK}_{\text{ID}_i} \| m_2)$ already exists for some δ where $\delta \neq \text{ID}_i \| \pi \| \text{PK}_{\text{ID}_i} \| m_2$. Otherwise, set $\alpha = H_1(\text{ID}_i \| \pi \| \text{PK}_{\text{ID}_i} \| m_2)$ and record it to the H_0-list.

⑥ Output the signature $\sigma = (r_2, U)$.

Remark 3 We here assume that A_{I} is well-behaved in the sense that it always queries Q_{ID_i}, $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i})$, and $H_0(\text{ID}_i \| \text{PK}_{\text{ID}_i,1})$ before ID_i is used in any sign query. It is trivial to modify any A_{I} to satisfy this property. Then, according to the verification protocol of the proposed scheme, σ will be a valid signature on m and ID_i.

(11) Forgery. After all the queries, A_{I} does not abort. It wins the game by outputting a forgery (ID*, m^*, $\mathrm{PK}_{\mathrm{ID}^*}$, $\sigma^*(=r_2^*, U^*)$).

Now we show the reduction to solve the k-BDHI problem. If $\mathrm{ID}^* \neq \mathrm{ID}_t$, F outputs $\perp$ and terminates the game. Otherwise, $\mathrm{ID}^* = \mathrm{ID}_t$. In this case, according to the ideal randomness of H_1, with overwhelming probability, A_{I} must have queried $H_1(\mathrm{ID}^*\|\pi^*\|\mathrm{PK}_{\mathrm{ID}^*}\|m^*)$ for some

$$\pi^* = \hat{e}(U^*, \mathrm{PK}_{\mathrm{ID}^*,2}\mathrm{PK}_{\mathrm{ID}^*,1}^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1})}\times (P_{\mathrm{pub}}\rho^{Q_{\mathrm{ID}^*}}\rho^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1})})^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*})})\mu^{-r_2^*}.$$

So the values of π^*, $H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1})$ and $H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*})$ can all be found from the H_0-list and H_1-list, respectively. Adversary F utilizes the General Forking Lemma[17] by replaying of Step 5 with the same random tape but different choices of output of $H_1(\mathrm{ID}^*\|\pi^*\|\mathrm{PK}_{\mathrm{ID}^*}\|m^*)$, F can get another valid forgery $\sigma' = (r_2', U')$ on the same ID*, m^* and $\mathrm{PK}_{\mathrm{ID}^*}$ such that $r_2^* \neq r_2'$ and

$$\hat{e}(U^*, \mathrm{PK}_{\mathrm{ID}^*,2}\mathrm{PK}_{\mathrm{ID}^*,1}^{H_0(\mathrm{ID}^*\|(\mathrm{PK}_{\mathrm{ID}^*,1}))}(P_{\mathrm{pub}}\times \rho^{Q_{\mathrm{ID}^*}}\rho^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1})})^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*})})\mu^{-r_2^*} = \hat{e}(U', \mathrm{PK}_{\mathrm{ID}^*,2}\mathrm{PK}_{\mathrm{ID}^*,1}^{H_0(\mathrm{ID}^*\|(\mathrm{PK}_{\mathrm{ID}^*,1}))}(P_{\mathrm{pub}}\times \rho^{Q_{\mathrm{ID}^*}}\rho^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1})})^{H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*})})\mu^{-r_2'}.$$

Since σ^* and σ' are both successful signatures corresponding to ID*, m^* and $\mathrm{PK}_{\mathrm{ID}^*}$, we have

$$U^* = D_{\mathrm{ID}^*}^{(r_1+r_2^*)(x^*+H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*}))^{-1}},$$

and

$$U' = D_{\mathrm{ID}^*}^{(r_1+r_2')(x^*+H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*}))^{-1}}.$$

Adversary F can compute $\rho^{a^{-1}}(=D_{\mathrm{ID}^*})$ as

$$D_{\mathrm{ID}^*} = (U^*/U')^{(x^*+H_0(\mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*}))(r_2^*-r_2')^{-1}}.$$

Adversary F then computes

$$\hat{e}(D_{\mathrm{ID}^*}, \rho) = \hat{e}(\rho, \rho)^{a^{-1}}$$

and derives the value of $\hat{e}(g, g)^{a^{-1}}$ from

$$\hat{e}(g, g)^{a^{-1}} = \left(\hat{e}(\rho, \rho)^{a^{-1}} \Big/ \hat{e}(\rho', \rho g^{c_0})\right)^{c_0^{-2}}$$

as the solution to the given instance of the k-BDHI problem.

Remark 4 The secret key x^* of $\mathrm{PK}_{\mathrm{ID}^*}$ is required when computing D_{ID^*}. If $\mathrm{PK}_{\mathrm{ID}^*} = \mathrm{PK}_{\mathrm{ID}_t}$ is the original public key generated from the oracle CreateUser, then F can extract x^* from the C-list. On the other hand, if $\mathrm{PK}_{\mathrm{ID}^*}$ is a new public key generated by A_{I}, then using the knowledge of exponent assumption[18-19], F can either extract x^* if

$$\mathrm{PK}_{\mathrm{ID}^*} = (\mathrm{PK}_{\mathrm{ID}^*,1}, \mathrm{PK}_{\mathrm{ID}^*,2}) = (\rho^{x^*}, (P_{\mathrm{pub}}, \rho^{Q_{\mathrm{ID}^*}})^{x^*})$$

is generated basing on $(\rho, (P_{\mathrm{pub}}, \rho^{Q_{\mathrm{ID}^*}}))$ or find $x^* = x_t\gamma$ from extracting γ if

$$(\mathrm{PK}_{\mathrm{ID}^*,1}, \mathrm{PK}_{\mathrm{ID}^*,2}) = ((\rho^{x_t})^{\gamma}, ((P_{\mathrm{pub}}, \rho^{Q_{\mathrm{ID}^*}})^{x_t})^{\gamma})$$

is generated basing on the original public key created by the oracle CreateUser. In either case, F is possible to retrieve x^*.

Remark 5 Note that the original Forking Lemma defined in Ref. [20] cannot be applied in this proof since our scheme is not a generic signature scheme. Due to this reason, we use the general Forking Lemma introduced by Bellare and Neven[17].

The simulation of the game is perfect and the running time of F to solve the k-BDHI problem is in polynomial of that of A_{I}.

The security proof is based on a realistic model in which A_{I} can only query the oracle Sign with the original public key generated from CreatUser. In other words, it cannot receive a valid signature from the oracle Sign by given a false public key chosen by itself. It is realistic since the signatures that a realistic adversary can obtain in real world are generated by a signer using the partial private key and secret value corresponding to its original public key. We emphasize that most of the existing certificateless short signatures[8-9] can only be proved based on this realistic model. More details about a realistic model are shown in Ref. [21].

Next, we show the security against the Type II adversary.

Theorem 2 (unforgeability against the Type II adversary) If there exists an adversary A_{II} who can break the unforgeability of the proposed scheme via the Type II attack, then we can construct another adversary F' such that F' can use A_{II} as a black box and solve the k-BDHI problem.

From the construction of a signature of the proposed scheme, it is not hard to see that a secret value and a partial private key are used in a similar way in the scheme. Thus, the security proof for the Type II adversary is analogous to that for the Type I adversary. Due to the above mentioned reason and the page limitation, the security proof is omitted here.

Now we prove that the proposed scheme achieves the Girault's Level-3 security. This seems to be straightforward since the user public key $\mathrm{PK}_{\mathrm{ID}_i,1}$ of ID_i is added as an input of the user partial private key generation algorithm. This disallows anyone except the KGC to generate a valid user partial private key for every newly-generated user public key. To formally show the security proof of this additional security requirement, we

reduce the security to EUF-CMA security[22] of any ID-based signature scheme having the following user ID-based key generation algorithm.

Assume that g is a generator of order q of a cyclic group G and KGC's public key is $\mathrm{mpk}_{\mathrm{IBS}} = g^s$ with $s \leftarrow_{\mathrm{R}} \mathbf{Z}_q^*$. On input the system parameters (including g, q and P_{pub}) of the scheme, and a user identity $Q_{\mathrm{ID}} \in \mathbf{Z}_q^*$, KGC computes the user ID-based secret key as $D_{\mathrm{ID}} = g^{(s+Q_{\mathrm{ID}})^{-1}}$.

For ID-based signatures having such kind of key generation algorithm, readers can refer to, for example, Refs. [4, 17]. Those schemes are all proved to be EUF-CMA secure in the ID-based setting (denoted by EUF-CMA-IDA).

Theorem 3 (Girault's Level-3 security) If there exists an adversary A_{E} who can break the Girault's Level-3 security of the proposed scheme, then we can construct another adversary F'' such that F'' can use A_{E} as a black box and break the EUF-CMA-IDA security of the above mentioned ID-based signature schemes[3,16].

This security proof follows the idea of Ref. [7]. Let $(\mathrm{mpk}_{\mathrm{IBS}}, \mathrm{msk}_{\mathrm{IBS}})$ be the ID-based master public/secret key pair in the game of EUF-CMA-IDA. Adversary F'' sets the master public key of the proposed scheme as $P_{\mathrm{pub}} = \mathrm{mpk}_{\mathrm{IBS}}$. At any time, A_{E} can query the oracle PartialKeyGen of the proposed scheme on input some identity ID and valid user public key $\mathrm{PK}_{\mathrm{ID}}$. The output of PartialKeyGen is a user partial private key of ID. To simulate the oracle, whenever A_{E} queries with an ID and a $\mathrm{PK}_{\mathrm{ID}} = (\mathrm{PK}_1, \mathrm{PK}_2)$, F'' first queries the oracle CreateUser of itself of the corresponding ID-based signature scheme with identity being set to $\mathrm{ID}\|\mathrm{PK}_1$. Adversary F'' then queries the oracle IDKeyExtract of itself of the corresponding ID-based signature scheme with the identity $\mathrm{ID}\|\mathrm{PK}_1$ to extract the corresponding ID-based secret key of the ID-based signature scheme. The output is then forwarded to A_{E} as the output of the oracle PartialKeyGen. Finally, when A_{E} outputs a triple $(\mathrm{ID}^*, D_{\mathrm{ID}^*}, \mathrm{PK}_{\mathrm{ID}^*})$ and wins the game where $\mathrm{PK}_{\mathrm{ID}^*} = (\mathrm{PK}_{\mathrm{ID}^*,1}, \mathrm{PK}_{\mathrm{ID}^*,2})$, F'' sets a new identity $\mathrm{ID}' = \mathrm{ID}^*\|\mathrm{PK}_{\mathrm{ID}^*,1}$, and queries the oracle CreateUser of itself with identity ID^* to create the user ID'. Then, ID^* will be a valid ID-based user secret key of ID'. Consequently, F'' breaks the EUF-CMA-IDA security of the ID-based signature scheme (ie., F'' can generate a signature on any message that it chosen by using the user secret key). This ends the proof.

4 Performance Evaluation

We evaluate the performance of the proposed scheme from the aspect of communication and computation costs in signature generation and verification.

The signature is about 320-bit and is at approximately the same security as a standard 1 024-bit RSA (which stands for Rivest, Shamir and Adleman who first publicly described the algorithm) signature. As mentioned in Section 1, a 320-bit signature is enough for recovering about a 100-bit message. So the communication cost is quite efficient due to the property of message recovery.

On the other hand, to see the computation cost, we can ignore some operations such as $\mathrm{PK}_1^{H_0(\mathrm{ID}\|\mathrm{PK}_1)}$,

$$\hat{e} = (\mathrm{PK}_1,\ P_{\mathrm{pub}} g^{Q_{\mathrm{ID}}}) = \hat{e}(g,\ \mathrm{PK}_2),$$

and $P_{\mathrm{pub}} g^{Q_{\mathrm{ID}_i}} g^{H_0(\mathrm{ID}\|\mathrm{PK}_1)}$.

This is because those computations require no online information, which means that they can be precomputed or need only be computed once for all the signature generation or verification processes. Hash operation is also quite efficient so does not need to be considered. Therefore, we consider only the heavy operations such as the pairing operation (denoted by $\hat{e}$), the exponentiation in G (denoted by E_G), and the exponentiation in G_T (denoted by E_{G_T}). In signature generation, the computation cost is $E_G + E_{G_T}$. There is no pairing operation (which is the most costly operation) in the signature generation phase. To verify a signature, the computation cost is $\hat{e} + 2E_{G_T}$. The computation cost of the proposed scheme is competitive to most of the efficient signature schemes such as Refs. [3,8-9,16].

5 Conclusion

Message recovery signatures are useful in many applications where low-computation-power devices are used or for systems with low-bandwidth channels. Certificatelss cryptography inherits both the advantages of PKI-based cryptography and ID-based cryptography without the disadvantages of both systems. However, conventional certificateless cryptography can only achieve Girault's Level-3 security. In this paper, we propose the first certificateless message recovery signature that satisfies Level-3 security. The security is regiously proved in the random oracle model.

References

[1] Abe M, Okamoto T. A signature scheme with message recovery as secure as discrete logarithm [J]. *Lecture Notes in Computer Science*, 1999, **1716**: 378-389.

[2] Nyberg K, Tuepple R A. A new signature scheme based on the DSA giving message recovery [C]// *Proceedings of the 1st ACM Conference on Communication and Computer Security*. Fairfax, USA: ACM Press, 1993: 58-61.

[3] Tso R, Gu C, Okamoto T, et al. Efficient ID-based digital signatures with message recovery [J]. *Lecture Notes in Computer Science*, 2007, **4856**: 47-59.

[4] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [J]. *Lecture Notes in Computer Science*, 2003, **2894**: 452-473.

[5] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing [J]. *Lecture Notes in Computer Science*, 2001, **2248**: 514-533.

[6] Shamir A. Identity-based cryptosystems and signature schemes [J]. *Lecture Notes in Computer Science*, 1984, **0196**: 47-53.

[7] Hu B C, Wong D S, Zhang Z, et al. Certificateless signature: A new security model and an improved generic construction [J]. *International Journal of Designs, Codes and Cryptography*, 2007, **42**(2): 109-126.

[8] Huang X, Mu Y, Susilo W, et al. Certificateless signature revisited [J]. *Lecture Notes in Computer Science*, 2007, **4586**: 308-322.

[9] Tso R, Yi X, Huang X. Efficient and short certificateless signatures [J]. *Lecture Notes in Computer Science*, 2008, **5339**: 64-79.

[10] Yap W L, Heng S H, Goi B M. An efficient certificteless signature [J]. *Lecture Notes in Computer Science*, 206, **4097**: 322-331.

[11] Zhang Z, Wong D S, Xu J, et al. Certificateless public-key signature: Security model and efficiet construction [J]. *Lecture Notes in Computer Science*, 2006, **3989**: 293-308.

[12] Girault M. Self-certified public keys [J]. *Lecture Notes in Computer Science*, 1991, **547**: 490-497.

[13] Barreto P S L M, Kim H Y, Lynn B, et al. Efficient algorithm for pairing-based cryptosystems [J]. *Lecture Notes in Computer Science*, 2002, **2442**: 354-369.

[14] Barreto P S L M, Lynn B, Scott M. On the selection of pairing-friendly groups [J]. *Lecture Notes in Computer Science*, 2003, **3006**: 17-25.

[15] Boneh D, Boyen X. Efficient selective ID secure identity based encryption without random oracles [J]. *Lecture Notes in Computer Science*, 2004, **3027**: 223-238.

[16] Barreto P S L M, Libert B, Mccullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps [J]. *Lecture Notes in Computer Science*, 2005, **3778**: 515-532.

[17] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma [C]// *Proceedings of 13th ACM Conference on Computer and Communication Security*. [s.l.]: ACM Press, 2006: 390-398.

[18] Bellare M, Palacio A. The knowledge of exponent assumptions and 3-round zero-knowledge protocols [J]. *Lecture Notes in Computer Science*, 2004, **3152**: 273-289.

[19] Hada S, Tanaka T. On the existence of 3-round zero-knowledge protocols [J]. *Lecture Notes in Computer Science*, 1998, **1462**: 408-423.

[20] Pintcheval D, Stern J. Security arguments for digital signatures and blind signatures [J]. *Journal of Cryptology*, 2000, **13**(3): 361-396.

[21] Tso R, Yi X, Huang X. Efficient and short certificateless signatures secure against realistic adversaries [J]. *Journal of Supercomputing*, 2011, **55**(2): 173-191.

[22] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks [J]. *SIAM Journal of Computing*, 1988, **17**(2): 281-308.