WUJNS
Wuhan University Journal of Natural Sciences

Vol.11 No.1 2006 193-197

Article ID: 1007-1202(2006)01-0193-05

A New ID-Based Proxy Multi-Signature Scheme from Bilinear Pairings

☐ GU Chun-xiang, PAN Heng, ZHU Yue-fei†

Network Engineering Department, Information Engineering University, Zhengzhou 450002, Henan, China

Abstract: ID-based public key cryptosystem can be a good alternative for certificate-based public key setting. This paper provides an efficient ID-based proxy multi-signature scheme from pairings. In the random oracle model, we prove that our new scheme is secure against existential delegation forgery with the assumption that Hess's scheme-1 is existential unforgeable, and that our new scheme is secure against existential proxy multi-signature forgery under the hardness assumption of the computational Diffie-Hellman problem.

Key words: ID-based signature; proxy multi-signature; ID-based proxy multi-signature; bilinear pairings; provable security

CLC number: TN 918; TP 309

Received date: 2005-04-24

Foundation item: Supported by the National Key Basic Research and Development Program (973 Program G1999035804), the National Natural Science Foundation of China (90204015, 60473021) and the Elitist Youth Foundation of Henan Province (021201400)

Biography: GU Chun-xiang (1976-), male, Ph. D. candidate, research direction: cryptography and information security. E-mail: gexiang5209@yahoo.com.cn

† To whom correspondence should be addressed. E-mail: zyfo136@sina.com

0 Introduction

In 1984, Shamir[1] first proposed the idea of ID-based public key cryptography (ID-PKC). In ID-PKC, an entity's public key is directly derived from certain aspects of its identity, such as an IP address belonging to a network host or an e-mail address associated with a user. Private keys are generated for entities by a trusted third party called a private key generator (PKG). The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the problems associated with them. The ID-PKC can be an alternative for certificate-based PKI, especially when efficient key management and moderate security are required.

The first practical and secure ID-based public key encryption scheme was presented in Ref. [2]. Since then, a rapid development of ID-PKC has taken place. Using bilinear pairings, people proposed many new ID-based signature schemes[3-5]. With these ID-based signature schemes, a lot of new extensions, such as ID-based proxy signature scheme, ID-based ring signature scheme, etc[6], have also been proposed.

Since Mambo *et, al*[7] first introduced the concept of proxy signature scheme, many new schemes have been proposed. At the same time, various extensions of basic proxy signature primitive have also been considered. Recently, Yi Li-jiang[8] *et al.* proposed a proxy multi-signature scheme. Later, Li Ji-guo[9] *et al.* proposed two nonrepudiable proxy multi-signature schemes. Proxy multi-signature allows a designated person, called a proxy signer, to sign on behalf of two or more original signers. Such proxy multi-signature can be widely used in many practical applications. For instance, a trusted secretary can sign authorized documents on behalf of

all members of a committee.

In this paper, we present a new ID-based proxy multi-signature scheme (ID-PMSS). Our new scheme gives a secure and efficient solution for proxy multi-signature in ID-based public key cryptosystems.

1 Bilinear Pairings

Let $(G_1,+)$, $(G_2,\cdot)$ be two cyclic groups of order q, Bilinear pairing $\hat{e}:G_1\times G_1\to G_2$ is a map with the following properties:

① Bilinearity: $P,Q\in G_1,\alpha,\beta\in Z_q$, $\hat{e}(\alpha P,\beta Q)=\hat{e}(P,Q)^{\alpha\beta}$;

② Non-degenerate: If P is a generator of G_1, then $\hat{e}(P,P)$ is a generator of G_2;

③ Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for any $P,Q\in G_1$.

The Computational Diffie-Hellman problem (CDHP) is to compute abP for any given P, aP, $bP\in G$. We assume through this paper that there is no polynomical time algorithm to solve CDHP with non-negligible probability.

2 Proposed ID-PMSS

In this paper, if there is no special statement, let $L=\{A_1,\cdots,A_n\}$ be the set of original signers with identity $ID_1,\cdots,ID_n$ and private key $d_1,\cdots,d_n$ respectively. They jointly delegate their signing rights to a proxy signer B with identity ID_B and private key d_B. We use warrants to delegate signing rights.

2.1 Description

The ID-PMSS is consists of eight polynomial-time algorithms:

● Setup: Given $G_1,G_2,q,\hat{e},P$, return a master key s and system parameters $\chi=(G_1,G_2,q,\hat{e},P,P_{\text{pub}},H_1,H_2)$, where $P_{\text{pub}}=sP$, $H_1:\{0,1\}^*\to G_1^*$ and $H_2:\{0,1\}^*\times G_1\to Z_q$ are hash functions.

● Extract: Given an identity $\text{ID}\in\{0,1\}^*$, computes $Q_{\text{ID}}=H_1(\text{ID})\in G_1^*$, $d_{\text{ID}}=sQ_{\text{ID}}$. PKG uses this algorithm to extract the user secret key d_{ID}, and gives d_{ID} to the user by a secure channel. (In the following description, denote $Q_x=H_1(\text{ID}_x)$.

● PD: For input secret key d_i and a warrant ω_i, A_i chooses $k_i\in Zq^*$ at random and computes $r_i=\hat{e}(P,P)^{k_i}$, $c_i=H_2(\omega_i,r_i)$, $U_i=c_id_i+k_iP$, and lets (ω_i,r_i,U_i) be the delegation to B.

● PV: Once B receives (ω_i,r_i,U_i), he computes $c=H_2(\omega_i,r_i)$, and accepts the delegation if and only if $r_i=\hat{e}(U_i,P)(\hat{e}(Q_i,P_{\text{pub}})^{-c}$

● PSKG: If B accepts all the delegations $\{(\omega_i,r_i,U_i)\}_{A_i\in L}$, he computes the proxy multi-signing key d_P as $d_p=c\cdot d_B+\sum_{A_i\in L}(c/c_i)U_i$, where $c_i=H_2(\omega_i,r_i)$, $c=\prod_{A_i\in L}c_i$.

● MSign: For a message m, B chooses $k\in Z_q^*$ at random and computes $r_P=\hat{e}(P,P)^k$, $c_P=H_2(m,r_P)$, $U_P=c_Pd_P+kP$, and lets $(m,r_P,U_P,\{(\omega_i,r_i)\}_{A_i\in L})$ be the proxy multi-signature for m on behalf of L.

● Verify: For a proxy multi-signature $(m,r_P,U_P,\{(\omega_i,r_i)\}_{A_i\in L})$, a recipient first checks if the proxy signer and the message conform to $\{\omega_i\}_{A_i\in L}$. Then he computes $c_P=H_2(m,r_P)$ and verifies whether $r_P=\hat{e}(U_P,P)(\hat{e}(\sum_{A_i\in L}Q_i+Q_B,P_{\text{pub}})^c\cdot\prod_{A_i\in L}r_i^{c/c_i})^{-c_P}$ If both steps succeed, the signature is a valid proxy multi-signature on behalf of A.

● ID: The proxy signer's identity ID_B can be revealed by $\{\omega_i\}_{A_i\in L}$.

If $\omega_1=\omega_2=\cdots=\omega_n=\omega$, the proxy multi-signature may be $(m,r_P,U_P,\omega,\{r_i\}_{A_i\in L})$. This can efficiently reduce the length of signatures.

Readers can see that (**Setup**, **Extract**, **PD**, **PV**) constitute an ID-based signature scheme of Hess's scheme-1[4], where **PD** and **PV** act as signing algorithm and verifying algorithm respectively. If $\#L=1$, this scheme constitute an ID-based proxy signature scheme of Zhang *et al*[6].

2.2 Correctness Analysis

As an ID-based proxy multi-signature scheme, it first should be correct. That is, for $m,\omega_i\in\{0,1\}^*$, $1\leqslant i\leqslant n$, it should have the following properties:

● $\forall 1\leqslant i\leqslant n,\text{PV}(\text{PD}(\omega_i,d_i),\text{ID}_i)=1$

● For $W_{i\to B}=\text{PD}(\omega_i,d_i),A_i\in L$, let $d_p=\text{PSKG}(\{W_{i\to B}\}_{A_i\in L},d_B)$, then Verify (MSign ($m$, d_p), $\{\text{ID}_i\}_{A_i\in L})=1$, and $\text{ID}(\text{MSign}(m,d_p))=\text{ID}_B$.

The correctness is easily proved as follows: If (ω_i,r_i,U_i) is a valid delegation of A_i to B, let $c_i=H_2(\omega_i,r_i)$, then $\hat{e}(U_i,P)(\hat{e}(Q_i,P_{\text{pub}}))^{-c_i}=\hat{e}(P,U_i-c_isQ_i)=r_i$

If $(m,r_P,U_P,\{(\omega_i,r_i)\}_{A_i\in L})$ is a valid multi-signature on message m of proxy signer B on behalf of L, let $c_i=H_2(\omega_i,r_i),c=\prod_{A_i\in L}c_i$, then,

$$\hat{e}(\sum_{A_i\in L}Q_i+Q_B,P_{\text{pub}})^c\prod_{A_i\in L}r_i^{c/c_i}$$
$$=\hat{e}(\sum_{A_i\in L}sQ_i+sQ_B,P)^c\prod_{A_i\in L}\hat{e}(k_iP,P)^{c/c_i}$$
$$=\hat{e}(\sum_{A_i\in L}(c/c_i)(c_id_i+k_iP)+cd_B,P)$$
$$=\hat{e}(\sum_{A_i\in L}(c/c_i)U_i+cd_B,P)=e(d_p,P)$$

$\hat{e}(U_P,P)(\hat{e}(d_P,P)^{-c_P})=\hat{e}(U_P-c_PP,P)=r_P$. That is,

$$r_P=\hat{e}(U_P,P)(\hat{e}(\sum_{A_i\in L}Q_i+Q_B,P_{\text{pub}})^c\cdot\prod_{A_i\in L}r_i^{c/c_i})^{-c_P}$$

2.3 Efficiency Analysis

Let T_P, T_S and T_E be the times for computing pairing, scalar multiplication in G_1 and modular exponentiation in G_2 respectively. We do not take other operations into account. The time complexity required by **MSign** and **Verify** are $1T_P+2T_S$ and $2T_P+(n+2)T_E$ respectively, where n is the number of original signers.

3 Security Proof

The general known security notion of an ID-based signature is existential unforgeable under adaptively chosen message and ID attacks (**EUF-ACMIA**) proposed by Ref. [3]. An ID-based digital signature scheme (**Setup**, **Extract**, **Sign**, **Verify**) is said to be EUF-ACMIA, if no polynomial time adversary $\mathcal{F}$, has a non-negligible success probability in the following game:

① A challenger C runs **Setup** of the scheme to generate the system parameters χ and gives it to $\mathcal{F}$.

② $\mathcal{F}$ can issue queries to the **Extract** oracle $E(.)$ and the **Sign** oracle $S(.)$, adaptively.

③ $\mathcal{F}$ outputs (ID,m,δ), where ID is an identity, m is a message, and δ is a signature, such that ID and (ID, m) are not equal to the inputs of any query to $E(.)$ and $S(.)$ respectively. $\mathcal{F}$ succeeds in the game if δ is a valid signature of ID for m.

3.1 Attack Model for ID-PMSS

We consider an adversary $\mathcal{F}$, which is assumed to be a probabilistic Turing machine which takes as input the global scheme parameters and a random tape. Formally, we model the adversary's capabilities by providing the adversary access to the following oracles:

- Extract(.): Takes input a user's ID_i, and returns the corresponding private key d_i.
- PD(.): Takes input the designator's identity ID_i and a warrant ω_i, and outputs a delegation $W_{i\to B}$.
- PSKG(.): Takes input the proxy signer's identity ID_B and a set of delegation information $\{W_{i\to B}\}_{A_i\in L}$ (we may also denote the set as $W_{L\to B}$), and outputs a proxy multi-signing key d_p.
- MSign(.): Takes input $W_{L\to B}$ and message m, and outputs a proxy multi-signature created by the proxy signer B on behalf of L.

Definition 1 An ID-PMSS is said to be secure against existential delegation forgery, if no polynomial time adversary $\mathcal{F}$, has a non-negligible success probability in the following game:

① A challenger C runs **Setup** of the scheme to generate the system parameters χ and gives it to $\mathcal{F}$.

② $\mathcal{F}$ can issue queries to the Extract(.) oracle, the PD(.) oracle, the PSKG(.) oracle and the MSign(.) oracle, adaptively.

③ $\mathcal{F}$ outputs (ID,ω,W), where ID is an identity, ω is a warrant message, and W is a delegation, such that ID, (ID, ω) and (ID,.) are not equal to the inputs of any query to $E(.)$, PD(.) and PSKG(.) respectively. $\mathcal{F}$ succeeds if W is a valid delegation of ID for ω.

Definition 2 An ID-PMSS is said to be secure against existential proxy multi-signature forgery, if no polynomial time adversary $\mathcal{F}$, has a non-negligible success probability in the following game:

① A challenger C runs **Setup** of the scheme to generate the system parameters χ and gives it to $\mathcal{F}$.

② $\mathcal{F}$ can issue queries to the Extract(.) oracle, the PD(.) oracle, the PSKG(.) oracle and the MSign(.) oracle, adaptively.

③ $\mathcal{F}$ outputs $(W_{L\to B},m,\tau)$, where $W_{L\to B}$ is a valid delegation, m is a message, τ is a proxy multi-signature, such that $(W_{L\to B},m)$, ID_B and $(\text{ID}_B, W_{L\to B})$ are not equal to the inputs of any query to MSign(.), Extract(.) and PSKG(.) respectively. $\mathcal{F}$ succeeds in the game if τ is a valid proxy multi-signature of ID_B with the delegation $W_{L\to B}$.

An secure ID-PMSS should be secure against existential delegation forgery and existential proxy multi-signature forgery.

3.2 The Security Proofs of Our ID-PMSS

Theorem 1 In the random oracle model, if there is an adversary $\mathcal{F}_0$ which performs, within a time bound T_0, an existential delegation forgery against our ID-PMSS with probability ε_0, then there is an adversary $\mathcal{F}_1$ which performs an existential forgery against Hess's scheme-1 within almost the same time, with probability

no less than ε_0.

Proof From the adversary $\mathcal{F}_0$, we can construct the adversary $\mathcal{F}_1$ as follows:

① A challenger C runs **Setup** and gives the system parameters χ to $\mathcal{F}_1$.

② $\mathcal{F}_1$ gives χ to $\mathcal{F}_0$ and runs $\mathcal{F}_0$. During the execution, $\mathcal{F}_1$ emulates $\mathcal{F}_0$'s oracles as following:

● $H_2(.)$: For input (m, r), $\mathcal{F}_1$ checks if $H_2(m, r)$ is defined. If not, $\mathcal{F}_1$ picks a random $c \in Z_q$, sets $H_2(m,r) \leftarrow c$. $\mathcal{F}_1$ returns $H_2(m,r)$ to $\mathcal{F}_0$.

● Extract(.): For input ID, F_1 request to his own Extract oracle, and let the response be the reply to $\mathcal{F}_0$.

● PD(.): For input ID and warrant ω, F_1 requests to his own Sign oracle with (ID,ω). If the reply is δ, $\mathcal{F}_1$ let $W=(\omega,\delta)$ be the reply to $\mathcal{F}_0$.

● PSKG(.): For input ID_B and delegations $(\omega_i, r_i, U_i)_{i\in I}$, where I is the index of designators, $\mathcal{F}_1$ requests to his Extract oracle with ID_B and gets the response d_B, $\mathcal{F}_1$ computes $c_i = H_2(\omega_i, r_i)$, $c = \prod_{i\in I} c_i, d_p = c \cdot d_B + \sum_{i\in I}(c/c_i)U_i$, and lets d_p be the reply to $\mathcal{F}_0$.

● MSign(.): For input $W_{I\to B} = (\omega_i, r_i, U_i)_i \in I$ and m, $\mathcal{F}_1$ simulates B's proxy signature on behalf of $\{ID_i\}_i \in I$ as follow:

⊟ Pick randomly $U \in G_1$, $c_p \in Z_q$.

⊟ For all $i \in I$, if $H_2(\omega_i, r_i)$ is not defined, request $H_2(.)$ with $(\omega_i, r_i,)$ and get response c_i. Let $H_2(\omega_i, r_i,) = c_i$. ,$c = \prod_{i\in I} c_i$

⊟ Compute

$$r = \hat{e}(U,P)(\hat{e}(\sum_{i\in I} Q_i + Q_B, P_{\text{pub}})^c \cdot \prod_{i\in I} r_i^{c/c_i})^{-c_p}$$

⊟ If $H_2(m,r)$ is defined, then abort (a collision appears). Otherwise, set $H_2(m,r)=c_p$.

⊟ Let $(m, r, U, \{(\omega_i, r_i,)\}_{i\in I})$ be the reply to $\mathcal{F}_0$.

③ If $\mathcal{F}_0$'s output is $(ID,\omega,(\omega,\delta))$ where ID is an identity, ω is a warrant, and (ω,δ) is a valid delegation, then $\mathcal{F}_1$ outputs an signature forgery of Hess's scheme-1: (ID,ω,δ), where δ is a valid signature of identity ID for message ω.

Obviously, if $\mathcal{F}_0$ succeeds in existential delegation forgery, then ID and (ID,ω) are not equal to the inputs of any query of $\mathcal{F}_1$ to his Extract oracle and Sign oracle. On the other hand, collisions appear with negligible probability, as mentioned in Ref. [10]. So we can see that $\mathcal{F}_1$ succeeds in the existential forgery against Hess's scheme-1 with probability no less than that of ε_0.

Theorem 2 In the random oracle mode, let $\mathcal{F}_0$ be an adversary, which performs, within a time bound T_0, an existential proxy multi-signature forgery against our ID-PMSS with probability ε. We denote by n_{h_1}, n_{h_2} and n_s the number of queries that $\mathcal{F}_0$ can ask to the oracles $H_1(.)$, $H_2(.)$ and MSign(.) respectively. Assume that $\varepsilon \geqslant 10(n_s+1)(n_{h_2}+n_s)n_{h_2}/q$, then there is polynomial time Turing machine $\mathcal{F}_1$, which can solve CDHP within expected time less than $120686 \cdot n_s \cdot n_{h_2} \cdot n_{h_1} \cdot T/\varepsilon$.

We define a related public key signature scheme (not an IDbased scheme), called **PKSS**, as follows:

● Kgen: Given a security parameter $\lambda \in N$,

ⅰ) Run **Setup** to generate a random number s and $(G_1, G_2, q, \hat{e}, P, P_{\text{pub}}, H_2)$, where $P_{\text{pub}} = sP$.

ⅱ) Pick randomly Q and set $d = sQ$. For $i=1$ to n, pick randomly $Q_i \in G_1^*$, $\omega_i \in \{0,1\}^*$, and set $d_i = sQ_i$, and compute $(\omega_i, r_i, U_i) = \text{PD}(d_i, \omega_i)$.

ⅲ) Compute $d_p = c \cdot d + \sum_{i=1}^{n}(c/c_i)U_i$, where $c_i = H_2(\omega_i, r_i)$ $c = \prod_{i=1}^{n} c_i$

ⅳ) The public key is $(G_1, G_2, q, \hat{e}, P, P_{\text{pub}}, H_2, Q, c, \{(Q_i, \omega_i, r_i, c_i)\}_{i=1,\cdots,n})$. The private key is d_P.

● Sgn: To sign on a message m, choose a random $k \in Z_q^*$ and compute $r_P = \hat{e}(P,P)^k$, $c_P = H_2(m, r_P)$, $U_P = c_P d_P + kP$. Let (r_P, U_P, c_P) be the signature of m.

● Verify: For a signature (m, r_P, U_P, c_P), a recipient verifies whether

$$r_P = \hat{e}(U_P, P)(\hat{e}(\sum_{i=1}^{n} Q_i + Q, P_{\text{pub}})^c \cdot \prod_{i=1}^{n} r_i^{c/c_i})^{-c_P}.$$

Obviously, PKSS is a generic digital signature scheme[10].

Proof Without any loss of generality, we may assume that for any ID, $\mathcal{F}_0$ queries $H_1(.)$ and Extract(.) at most once, and $\mathcal{F}_0$ queries $H_1(.)$ with ID before ID is used as (part of) an input of any query to $H_2(.)$, Extract(.) PD(.), PSKG(.) and MSign(.).

From $\mathcal{F}_0$, we can construct $\mathcal{F}_1$ which computes aQ on input of any given $P, aP, Q \in G_1^*$ as follows:

① A challenger C runs **Setup** to generate $\chi = (G_1, G_2, q, \hat{e}, P, P_{\text{pub}}, H_1, H_2)$, and gives χ to $\mathcal{F}_1$

② $\mathcal{F}_1$ sets $P_{\text{pub}} = aP$ and $v=1$, and picks randomly $t, 1 \leqslant t \leqslant n_{h_1}$ and $x_i \in Z_q$, $i=1,2,\cdots,n_{h_1}$.

③ $\mathcal{F}_1$ runs $\mathcal{F}_0$ with input χ. During the execution, $\mathcal{F}_1$ emulates $\mathcal{F}_0$'s oracles as following:

● $H_1(.)$: For input ID, $\mathcal{F}_1$ checks if $H_1(\text{ID})$ is

defined. If not, he sets $ID_v \leftarrow ID, v \leftarrow v+1$, and defines

$$H_1(ID) = \begin{cases} Q, & v = t \\ x_v P, & v \neq t \end{cases}$$

$\mathcal{F}_1$ returns $H_1(ID)$ to $\mathcal{F}_0$.

● $H_2(.)$: The same as that in Theorem 2's proof.

● Extract (.): For input ID_i, if $i=t$, $\mathcal{F}_1$ aborts. Otherwise, $\mathcal{F}_1$ lets $d_i = x_i P_{pub}$ be the reply to $\mathcal{F}_0$.

● PD(.): For input ID_i and ω_i, if $i \neq t$, $\mathcal{F}_1$ computes $d_i = x_i P_{pub}$, $(\omega_i, r_i, U_i) = PD(d_i, \omega_i)$. Otherwise,

▤ Pick randomly $U_i \in G_1$, $c_i \in Z_q$;

▤ Compute $r_i = \hat{e}(U_i, P)(\hat{e}(Q, P_{pub}))^{-c_i}$;

▤ If $H_2(\omega_i, r_i)$ has been defined, then aborts (a collision appears). Otherwise, set $H_2(\omega_i, r_i) = c_i$;

Let (ω_i, r_i, U_i) be the reply to $\mathcal{F}_0$.

● PSKG(.): For input ID_j and $(\omega_i, r_i, U_i)_{i \in I}$, if $j=t$, then abort. Otherwise, $\mathcal{F}_1$ computes $c_i = H_2(\omega_i, r_i), c = \prod_{i \in I} c_i, d_p = c \cdot d_j + \sum_{i \in I} (c/c_i) U_i$, and lets d_p be the reply to $\mathcal{F}_0$.

● MSign(.): For input $W_{I \to j} = \{(\omega_i, r_i, U_i)\}_{i \in I}$ and m, if $j \neq t$, $\mathcal{F}_1$ computes the signature (m, τ) on m with secret multi-singing key $d_P = PSKG(ID_j, W_{I \to j})$. Otherwise, $\mathcal{F}_1$ simulates ID_t's proxy multi-signature on behalf of $\{ID_i\}_{i \in I}$ the same as that of the proof of Theorem 1 and gets (m, τ). Let (m, τ) be the reply to $\mathcal{F}_1$.

④ If $\mathcal{F}_0$ succeeds in existential multi-signature forgery and $\mathcal{F}_0$'s output is (W, m, τ) with $W = W_{I \to t} = \{(\omega_i, r_i, U_i)\}_{i \in I}$, $(m, \tau) = (m, r, U, \{(\omega_i, r_i)\}_{i \in I})$, then $\mathcal{F}_1$ can get a nontrivial forgery (m, r, U, c_p) of **PKSS** corresponding to private key $d_P = \alpha Q + \sum_{i \in I} \frac{c}{c_i} U_i$, where $c_i = H_2(\omega_i, r_i), c = \prod_{i \in I} c_i$, $c_p = H_2(m, r)$.

⑤ If $\mathcal{F}_1$ gets two **PKSS** signatures corresponding to the private key d_P: (m, r, U, c_p) and (m, r, U', c_p'), $\mathcal{F}_1$ can compute and outputs aQ as follow:

$$\xi_1 \leftarrow (c_p - c_p')^{-1} \bmod q, \ \xi_2 \leftarrow e^{-1} \bmod q,$$

$$d_P \leftarrow \xi_1 (U - U'), \ \alpha Q \leftarrow \xi_2 (d_P - \sum_{i \in I} \frac{c}{c_i} U_i).$$

Otherwise, for all $i \in I$, set $H_2(\omega_i, r_i) = c_i$, $v=1$, and goto step ③ with the same random tape but different choices of $H_2(.)$.

As mentioned in Ref. [10], collisions appear with negligible probability. So $\mathcal{F}_1$'s simulations are indistinguishable from $\mathcal{F}_0$'s oracles. Because t is chosen randomly, $\mathcal{F}_1$ can output a forgery of **PKSS** of private key $d_P = \alpha Q + \sum_{i \in I} \frac{c}{c_i} U_i$ within expected time T with probability ε / n_{h_1}. based on the **Forking Lemma**[10], $\mathcal{F}_1$ can produce two valid signatures (m, r, U, c_P) and (m, r, U', c_P') such that $c \neq c'$ within expected time less than $120686 \cdot n_s \cdot n_{h_2} \cdot n_{h_1} \cdot T/\varepsilon$. So $\mathcal{F}_1$ can output aQ.

4 Conclusion

This paper provides a new ID-PMSS with provable security in the random oracle model. The time complexity required by **MSign** and **Verify** of our scheme are $1T_P + 2T_S$ and $2T_P + (n+2)T_E$ respectively, where T_P, T_S and T_E are the times for computing pairing, scalar multiplication in G_1 and modular exponentiation in G_2 respectively, n is the number of original signers. So our new scheme gives an efficient and practical solution for proxy multi-signature in ID-based public key cryptosystem.

References

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes. *Advances in Cryptology - CRYPTO'84* (LNCS 196). Berlin: Springer-Verlag, 1984. 47-53.

[2] Boneh D, Franklin M. Identity-Based Encryption From The Weil Pairing. *Advances in Cryptology-CRYPTO'01*(LNCS 2139). Berlin: Springer-Verlag, 2001. 213-229.

[3] Cha J C, Cheon J H. An Identity-based Signature from Gap Diffie-Hellman Groups. *Public Key Cryptography - PKC* 2003(LNCS 2567). Berlin: Springer-Verlag, 2002. 18-30.

[4] Hess F. Efficient Identity Based Signature Schemes Based on Pairings. *Selected Areas in Cryptography-SAC* 2002(LNCS 2595). Berlin: Springer-Verlag, 2002. 310-324.

[5] Yi X. An Identity-Based Signature Scheme From the Weil Pairing. *IEEE Communications Letters*, 2003, **7**(2):76-78.

[6] Zhang F, Kim K. Efficient ID-based Blind Signature And Proxy Signature from Bilinear Pairings. *ACISP* 03 (LNCS 2727). Berlin: Springer-Verlag, 2003. 312-323.

[7] Mambo M, Usuda K, Okamoto E. Proxy Signatures for Delegating Signing Operation. *3rd AC- Conference on Computer and Communications Security* (CCS'96), New York: AC- Press, 1996. 48-57.

[8] Yi L J, Bai G Q, Xiao G Z. Proxy Multi-Signature Scheme: A New Type of Proxy Signature Scheme. *Electron Lett*, 2000, **36**:527-528.

[9] Li Ji-guo, Cao Zhen-fu, Zhang Yi-chen. Nonrepudiable Proxy-Ulti-Signature Scheme. *Journal of Computer Science and Technology*, 2003, **18**(3):399-402.

[10] Pointcheval D, Stern J. Security Arguments For Digital Signatures and Blind Signatures. *Journal of Cryptology*, 2000, **13**(3):361-369.

□