INFORMATICA, 2010, Vol. 21, No. 1, 41–56

Identity-Based Threshold Proxy Signature from Bilinear Pairings

Jenshiuh LIU, Shaonong HUANG
Department of Information Engineering and Computer Science
Feng-Chia University, Taichung, Taiwan 407, R.O.C.
e-mail: liuj@fcu.edu.tw

Received: March 2008; accepted: September 2008

Abstract. Delegation of rights is a common practice in the real world. We present two identity-based threshold proxy signature schemes, which allow an original signer to delegate her signing capability to a group of n proxy signers, and it requires a consensus of t or more proxy signers in order to generate a valid signature. In addition to identity-based scheme, privacy protection for proxy singers and security assurance are two distinct features of this work. Our first scheme provides partial privacy protection to proxy signers such that all signers' identities are revealed, whereas none of those t participating signers is specified. On the other hand, all proxy signers remain anonymous in the second scheme. This provides a full privacy protection to all proxy signers; however, each valid signature contains a tag that allows one to trace all the participating proxy signers. Both our proposed schemes are secure against unforgeability under chosen message attack, and satisfy many other necessary conditions for proxy signature.

Keywords: identity-based signature, proxy signature, threshold, privacy protection, authentication.

1. Introduction

Delegation of rights is a common practice in the real world, for example, Alice is a manager of a company, she may delegate her deputy Bob the capability to sign company's document on behalf of her when she is on vacation. The proxy signature was first introduced by Mambo *et al.* (1996). Their proxy signature scheme allows a user (original signer) to delegate her signing capability to another user (proxy signer); after that, the proxy signer can sign messages on behalf of the original signer. Upon receiving a proxy signature on some message, a verifier can validate the delegation of power and the signature by some predefined protocol. Since then proxy signature has received great attention, and some variants have been considered: In the multi-proxy signature scheme (Hwang and Shi, 2000), an original signer authorizes a group of proxy singers, and a cooperation of all the proxy signers is required to generate any proxy signature on behalf of the original signer; on the other hand, the proxy multi-signature (Yi *et al.*, 2000) allows a designated proxy signer to generate a signature on behalf of a group of original signers.

In a certificate-based public key system, users' public keys are kept by some certificate authority; whenever we need someone's public key, we have to extract it from a certificate issued by some certificate authority. The major drawback in this certificate-based

scheme is that the public keys are hard to remember and they might be distorted. The concept of identity(ID)-based cryptosystem was first introduced by Shamir (1984); the main idea of the ID-based cryptosystem (Boneh and Franklin, 2001; Chen, 2007; Cocks, 2001; Libert, 2006) is that one's identity information, such as name, email address and/or telephone number, acts as one's public key. In other words, a user's public key can be obtained directly from her identity rather than by extracting it from a certificate issued by some certificate authority. After the initial work of Shamir, the ID-based cryptosystem has received great attention because it can avoid malicious attacks during public key transmission; moreover, one's public key can be easily verified by human perceptions, which makes key management much more easy for users. A recent study by Paterson and Price (2003) comments that ID-based cryptosystems allow a lightweight implementation at the client end compared to the traditional public key infrastructures. This feature makes the ID-based cryptosystems much more preferable for applications in mobile systems (Tseng *et al.*, 2008) and cyber-physical systems (Lee, 2006; Xu *et al.*, 2008), where computing capability and communication bandwidth are very limited.

Various ID-based signature schemes have been proposed recently (Sakai *et al.*, 2000; Boneh *et al.*, 2001; Cha and Cheon, 2003; Hess, 2002; Kancharla *et al.*, 2007; Paterson, 2002); security issues regarding ID-based signatures have been studied in papers (Bellare *et al.*, 2004; Libert and Quisquater, 2004; Lu and Feng, 2007). Moreover, there are research works on ID-based proxy signature (Wang and Liu, 2005; Xu *et al.*, 2005; Zhang and Kim, 2003), multi-proxy signature (Li and Zhang, 2007), multi-signature (Gangishetti *et al.*, 2006; Wang and Cao, 2007), and multi-proxy multi-signature (Li and Chen, 2005; Guo *et al.*, 2006).

In a (t, n) threshold scheme (Shamir, 1979) a secret D is divided into n pieces such that knowledge of any t or more pieces allows one to compute D easily, and knowledge of any $t-1$ or fewer pieces results in D completely undeterminable. Threshold signatures have motivated by many applications such as to have a group of employees in an organization to reach a common consent on a certain message before signing it, and to protect signature keys from internal and/or external attack. In this work, we present two ID-based threshold proxy signature schemes. We consider an original signer to delegate her signing capability to a group of n proxy signers, and it requires a consensus of t or more proxy signers to generate a valid signature. There are many applications of our proposed schemes, for example, the board of directors (original signer) of an organization delegates its signing capability to the management team (proxy signers) such that every document should be approved (signed) by a certain number (threshold) of executive officers before it becomes official. A second example could be mobile agents in an e-commerce setting, where a buyer delegates her signing capability to a broker and a banker such that both of them have to sign a purchase order before it becomes official to any seller.

Few works on ID-based threshold schemes have been reported: ID-based threshold signature have been studied in Baek and Zheng (2004) and Cheng *et al.* (2005), where a private key associated with one identity is shared among all signature generation servers (signers) such that no individual signer's identity is available to the public. Xu *et al.* (2004) proposed an ID-based threshold proxy signature, in which all proxy signers' identities (public keys) are publicized and required for signature verifications; however, it can

be shown that there is a security flaw in Bao *et al.* (2006) such that a collusion of t signers is able to recover all n proxy signers' private keys. Bao *et al.* (2006) have proposed another ID-based threshold proxy signature scheme with known signers; which requires that the t signers must be specified, in addition to all proxy signers' identities, for signature verifications. This may impose some responsibilities on signers; however, Lu *et al.* (2007) showed that there are security flaws in Bao *et al.* (2006) such that one may impersonate the original signer and forge a valid threshold signature on any message.

In addition to identity-based scheme, privacy protection for proxy singers and security assurance are two distinctive features of our work. Shum and Wei (2002) addressed signer privacy protection in proxy signature scheme; they proposed a method to hide the identity of the proxy signer behind an alias. In this work, we provide two different levels of privacy for each proxy signer. Our first scheme provides partial privacy protection to proxy signers such that identities (public keys) of all (n) proxy signers are required in signature verifications; however, none of those t participating signers' identities needs to be specified. On the other hand, no identity of any proxy signer is revealed in the second scheme, i.e., all proxy signers may remain anonymous. This provides a full privacy protection to all proxy signers; however, each valid signature generated by our second scheme contains a tag, if it is necessary, with some help from a third party, that tag allows one to trace all the proxy signers that sign the threshold signature. Security is always a major issue for any signature scheme. Bellare *et al.* (2004) have presented a framework that enables modular security analysis for ID-based identification and signature schemes. Xu *et al.* (2005) first formalized a notion of security for ID-based proxy signature schemes; following that work, Wu *et al.* (2007) redefined the security model, and presented a new unforgeable ID-based proxy signature scheme. Both our proposed schemes are secure against unforgeability under chosen message attack (uf-cma) (Goldwasser *et al.*, 1988) in the random oracle model. Moreover, our schemes satisfy all other necessary conditions, such as verifiability, proxy signer's deviation, distinguishability, and undeniability, addressed in Mambo *et al.* (1996) for proxy signature.

The rest of this paper is organized as follows. In Section 2, we review some related mathematical properties. Our proposed schemes are presented in Section 3. Security analysis is given in Section 4. Finally, we conclude our work in Section 5.

2. Preliminaries

In this section, we briefly review some background knowledge which includes bilinear pairing, Gap Diffie–Hellman groups, Lagrange interpolating polynomials, and the identity-based signature proposed by Sakai *et al.* (2000; SOK-IBS).

2.1. *Bilinear Pairing*

Bilinear pairing is a key primitive for many ID-based cryptographic schemes, for example, Boneh *et al.* (2001), Boneh and Franklin (2003), Cha and Cheon (2003), Baek and Zheng (2004), Gagne (2002), Cheng *et al.* (2005), Yi (2003). It is defined as follows.

Let $(G_1, +)$ be a cyclic additive group, whose order is a large prime m, and $(G_2, *)$ be a cyclic multiplicative group of the same order m. A bilinear map $\hat{e}$: $G_1 \times G_1 \to G_2$ satisfies the following properties (Boneh and Franklin, 2001; 2003):

1. *Bilinearity*: $\hat{e}(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z$.
2. *Non-degeneracy*: There exists $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $\hat{e}(P, Q)$.

The *modified Weil pairing* over the elliptic curves as defined by Boneh and Franklin (2001, 2003) is one example of a bilinear map. Let $\hat{e}$: $G_1 \times G_1 \to G_2$ be a bilinear map, $a \in Z$, and P, Q and Q_i (for $1 \leqslant i \leqslant n$) members in group G_1. The bilinearity implies that the following equalities hold:

$$\hat{e}(aP, Q) = \hat{e}(P, Q)^a = \hat{e}(P, aQ), \tag{1}$$

$$\hat{e}(P, \sum_{i=1}^{n} Q_i) = \prod_{i=1}^{n} \hat{e}(P, Q_i). \tag{2}$$

2.2. *Gap Diffie–Hellman Groups*

The security of elliptic curve cryptography is mostly based on the apparent intractability of the *elliptic curve discrete logarithm problem* (ECDLP). Let q be a large prime number, $E(F_q)$ denote an elliptic curve over a finite field F_q. The ECDLP is described as follows. Given $E(F_q)$, a point $P \in E(F_q)$ of order m, and another point $Q \in E(F_q)$ known to be an integer multiple of P, determine the integer k ($0 \leqslant k \leqslant m - 1$), such that $Q = kP$. In this work, we assume that the ECDLP is hard (Kanayama *et al.*, 2000).

DEFINITION 1. Decision Diffie–Hellman Problem (DDHP): Given a generator P of a group G and a 3-tuple (aP, bP, cP), decide whether $c = ab (\text{mod } m)$.

DEFINITION 2. Computation Diffie–Hellman Problem (CDHP): Given a generator P of a group G and a 2-tuple (aP, bP), compute abP.

The hardness of CDHP depends on the hardness assumption of ECDLP. However, DDHP (Boneh, 1998) is easy since, with the bilinear pairing, we have $c = ab$ (mod m) if and only if $\hat{e}(aP, bP) = \hat{e}(P, cP)$. The gap Diffie–Hellman group (Boneh *et al.*, 2001; Cha and Cheon, 2003; Chow *et al.*, 2004) is defined as follows.

DEFINITION 3. A group G is a gap Diffie–Hellman (GDH) group if DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP within polynomial time with non-negligible advantage.

In the following, we consider G_1 be a subgroup of points on an elliptic curve over a finite field, and G_2 a subgroup of the multiplicative group of a related finite field. Furthermore, we assume that both G_1 and G_2 are GDH groups.

2.3. *Lagrange Interpolating Polynomial*

The Lagrange interpolating polynomial is the polynomial $f(x)$ of degree $\leqslant n$ that passes through the $n+1$ points, $(x_i, f(x_i))$ for $1 \leqslant i \leqslant n+1$, and is given by $f(x) = \sum_{i=1}^{n+1} f_i(x)$, where $f_i(x) = y_i \prod_{\substack{j=1 \\ j \neq i}}^{n+1} \frac{x-x_j}{x_i-x_j}$. The Lagrange interpolating polynomial can be written explicitly as

$$\begin{aligned} f(x) = & \frac{(x-x_2)(x-x_3)\cdots(x-x_{n+1})}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_{n+1})} y_1 \\ & + \frac{(x-x_1)(x-x_3)\cdots(x-x_{n+1})}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_{n+1})} y_2 \\ & \qquad \vdots \\ & + \frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_{n+1}-x_1)(x_{n+1}-x_2)\cdots(x_{n+1}-x_n)} y_{n+1}. \end{aligned} \tag{3}$$

We call $\prod_{\substack{j=1 \\ j \neq i}}^{n+1} \frac{0-x_j}{x_i-x_j}$ (for $1 \leqslant i \leqslant n+1$) the Lagrange coefficients. It is known that one is able to construct the Lagrange interpolating polynomial with $n+1$ distinct points. However, with n or less points, one is not able to construct the polynomial.

2.4. *SOK Identity-Based Signature*

We briefly review the identity-based signature proposed by Sakai *et al.* (2000; SOK-IBS), which is the basis of our signature schemes. Given a user with her identity ID and a message M, the SOK-IBS on M is $U = rP$ and $V = rH_1(M) + d_{ID}$, where P and H_1 are system parameters, d_{ID} is the private key of the user, r is a random number, similar to what we will define in this work. Lu and Feng (2007) have shown that the original SOK-IBS is secure against unforgeability under chosen message attack (uf-cma) (Goldwasser *et al.*, 1988) in the random oracle model; however, SOK-IBS is not secure against *strong* uf-cma; more precisely, given a valid signature σ on (M, ID) one can forge a *different* but *valid* signature σ' on (M, ID) without knowing the private key of ID (Lu and Feng, 2007). There are two modifications of the SOK-IBS, both redefine the parameters of the hash function (H_1): The first modification (SOK-IBS-1; Bellare *et al.*, 2004) replaces $H_1(M)$ by $H_1(M, U)$, whereas the second modification (SOK-IBS-2; Libert and Quisquater, 2004) replaces $H_1(M)$ by $H_1(ID, M, U)$. Bellare *et al.* (2004) have shown that SOK-IBS-1 is secure against uf-cma. Libert and Quisquater (2004) have shown that SOK-IBS-2 is secure against both uf-cma and strong uf-cma; Lu and Feng (2007) indicated that the technique used in Libert and Quisquater (2004) can be applied to show that SOK-IBS-1 is also secure against strong uf-cma.

3. ID-Based Threshold Proxy Signature

We present two threshold proxy signature schemes in this section. The proposed schemes involve five roles: the private key generator (PKG), an original signers ($\mathcal{OS}$) with identity

A, a set of proxy signers $\mathcal{PS} = \{B_1, B_2, \cdots B_n\}$ with n members (where B_i is the ID of the ith ($1 \leqslant i \leqslant n$) member), a set of signers $\mathcal{S} = \{C_1, C_2, \cdots C_t\}$ with t members (where $\mathcal{S}$ is a subset of $\mathcal{PS}$, and C_i is the ID of the ith ($1 \leqslant i \leqslant t$) member), and a verifier. For the first scheme, all proxy signers' identities (public keys) are required in signature verification, which is referred to as Scheme A; on the other hand, no proxy singer's identity is revealed in the second scheme, which is referred to as Scheme T.

3.1. *All Identify Signature Scheme*

Our first signature scheme (Scheme A) consists of six phases: system setup, user key extraction, proxy certificate generation, proxy shadow generation, signature generation, and signature verification.

3.1.1. *System Setup Phase*

Let G_1 and G_2 be two finite groups both of large prime order m, with $\hat{e}$ a modified Weil pairing such that $\hat{e}$: $G_1 \times G_1 \to G_2$. Let H_1: $\{0,1\}^* \times G_1 \to G_1$, H_2: $\{0,1\}^* \to G_1$, and H_3: $\{0,1\}^* \to Z_m^*$ be three cryptographic hash functions. The PKG is assumed to set up system parameters as specified in the following procedure:

1. Randomly select $s \in Z_m^*$ as the system (secret) master key.
2. Randomly select $P \in G_1$ as a system public parameter, and computes $P_{pub} = sP$ as the system public key.

The system parameters are: params $= \langle G_1, G_2, \hat{e}, P, P_{pub}, H_1, H_2, H_3, m \rangle$; the system master secret key is s.

3.1.2. *User Key Extraction Phase*

Let ID be the identification of a user in our system; she submits her ID to PKG and PKG executes the following procedure to generate a secret key for her:

Compute $Q_{ID} = H_2(ID)$ and $d_{ID} = sQ_{ID}$; send d_{ID} to user ID through a secure channel as her secret key.

3.1.3. *Proxy Certificate Generation Phase*

To delegate the signing capability to the proxy signer group $\mathcal{PS}$, the original signer signs a warrant w and generates the proxy certificate. The warrant w contains all the necessary delegation details, such as the identity information of the original signers, types of documents the proxy group is delegated to sign, and/or the time period for the delegation and *etc.*. The proxy certificate (U, V) is generated by the following procedure:

1. Original signer A chooses a random number $x_a \in Z_m^*$ as her secret value, computes $U = x_a P$.
2. Original signer A signs the warrant by computing computes $V = x_a H_1(w, U) + d_A$, and broadcasts U, V to all members in $\mathcal{PS}$.

3.1.4. *Proxy Shadow Generation Phase*

Each secret shadow consists of two parts: one from $\mathcal{OS}$ and the other from $\mathcal{PS}$. Original signer A executes the following procedure to generate a $\mathcal{OS}$'s secret shadow for each member in $\mathcal{PS}$:

1. Choose a random polynomial of degree $t-1$ with the secret value x_a as its constant term, i.e., $f(x) = x_a + \sum_{k=1}^{t-1} a_k x^k \pmod m$, where $a_k \in Z_m^*$.
2. Compute $A_k = a_k V$ and $\hat{e}(P, A_k)$, then publish $\hat{e}(P, A_k)$ to all members in $\mathcal{PS}$.
3. Compute $K_i = f(H_3(B_i))V + d_A$, and send it through a secure channel to B_i for $1 \leqslant i \leqslant n$.

Each B_i ($1 \leqslant j \leqslant n$) accepts K_i as her secret shadow from $\mathcal{OS}$ if the following equation holds:

$$\hat{e}(P, K_i) = \hat{e}(U, V)\hat{e}(P_{pub}, Q_A) \prod_{k=1}^{t-1} \hat{e}(P, A_k)^{H_3^k(B_i)}.$$

To generate the $\mathcal{PS}$'s secret shadow, each member in $\mathcal{PS}$ executes the following procedure:

1. Each B_j ($1 \leqslant j \leqslant n$) chooses a random number $y_j \in Z_m^*$ as her secret value, computes $W_j = y_j P$, and sends W_j to clerk B[1].
2. After receiving all W_j's, clerk B computes $W = \sum_{j=1}^{n} W_j$, and broadcasts W to all members in $\mathcal{PS}$.
3. Each B_j computes $\hat{e}(P, y_j V)$ and publishes it to all members in $\mathcal{PS}$.
4. Each B_j chooses a random polynomial of degree $t-1$ with the secret value y_j as its constant term, i.e., $g_j(x) = y_j + \sum_{k=1}^{t-1} b_{j,k} x^k \pmod m$, where $b_{j,k} \in Z_m^*$.
5. Each B_j computes $B_{j,k} = b_{j,k} V$, $\hat{e}(P, B_{j,k})$, and publishes $\hat{e}(P, B_{j,k})$ to all members in $\mathcal{PS}$.
6. Each B_j in $\mathcal{PS}$ computes $Y_{i,j} = g_j(H_3(B_i))V + d_{B_j}$, and sends it through a secure channel to B_i for $1 \leqslant i \leqslant n$.

Each member in $\mathcal{PS}$ constructs her second part of secret shadow as follows:

1. B_i ($1 \leqslant i \leqslant n$) accepts $Y_{i,j}$ if the following equation holds:

$$\hat{e}(P, Y_{i,j}) = \hat{e}(P, y_j V) \prod_{k=1}^{t-1} \hat{e}(P, B_{j,k})^{H_3^k(B_i)} \hat{e}(P_{pub}, Q_{B_j}).$$

2. After receiving all $Y_{i,j}$'s, B_i computes $Y_i = \sum_{j=1}^{n} Y_{i,j}$, as her secret shadow from $\mathcal{PS}$.

3.1.5. *Signature Generation Phase*

Assume that a message M is intended to be signed. Each participating proxy signer uses her secret shadow as the signing key to generate a partial signature. All t members in $\mathcal{S}$ execute the following procedure to generate their partial signatures:

1. Each C_i ($1 \leqslant i \leqslant t$) in $\mathcal{S}$ chooses a random number $r_i \in Z_m^*$, computes $R_i = r_i P$, and sends R_i to clerk C[2].

[1] Any one of the proxy signers could be designated as clerk B.

[2] Any one of the signers could be designated as clerk C.

2. After receiving all R_i's, clerk C computes $R = \sum_{i=1}^{t} R_i$, and broadcasts R to all members in $\mathcal{S}$.
3. Each C_i in $\mathcal{S}$ computes $S_i = r_i H_1(M, R) + l_i(K_i + Y_i)$, where $l_i = \prod_{\substack{j \neq i \\ C_j \in \mathcal{S}}} \frac{0 - H_3(C_j)}{H_3(C_i) - H_3(C_j)}$. Then C_i computes $\hat{e}(P, l_i(K_i + Y_i))$ and sends it along with S_i to clerk C.
4. Clerk C accepts S_i if the following equation holds:

$$\hat{e}(P, S_i) = \hat{e}\big(R_i, H_1(M, R)\big)\hat{e}\big(P, l_i(K_i + Y_i)\big).$$

5. Clerk C computes $S = \sum_{i=1}^{t} S_i$ and publishes $(w, (U, V), (S, W, R))$ as a threshold proxy signature on message M.

3.1.6. *Signature Verification Phase*

The verifier applies the following procedure to verify the threshold proxy signature $(w, (U, V), (S, W, R))$ on message M.

1. Check if the message M conforms to the warrant w. Reject the signature if it does not conform. Otherwise continue on the next step.
2. Verify the warrant w against the certificate (U, V) by the following equation:

$$\hat{e}(P, V) = \hat{e}\big(U, H_1(w, U)\big)\hat{e}(P_{pub}, Q_A). \tag{4}$$

   Reject the signature if Eq. (4) does not hold. Otherwise continue on the next step.
3. Accept the signature if and only if the following equation holds:

$$\hat{e}(P, S) = \hat{e}\big(R, H_1(M, R)\big)\hat{e}(U, V)\hat{e}(W, V)\hat{e}\left(P_{pub}, Q_A + \sum_{i=1}^{n} Q_{B_i}\right). \tag{5}$$

3.2. *Traceable Signature Scheme*

Our second scheme (Scheme T) provides a distinctive feature that no proxy signer's identity is revealed in the signature; only original signer's identity is required in signature verifications. However, each signature contains a tag that allows verifiers to trace all the signers in $\mathcal{S}$. To accomplish this, PKG's attention is required in tracing the signers.

This traceable scheme consists of seven phases: In addition to the six phases as in Scheme A, an (optional) trace phase is provided to determine the signers of any signature. The system setup, user key extraction, and proxy certificate generation phases of our traceable signature scheme are the same as Scheme A. The other four phases are as follows.

3.2.1. *Proxy Shadow Generation Phase*

Similar to Scheme A, each secret shadow consists of two parts: one from $\mathcal{OS}$ and the other from $\mathcal{PS}$. The $\mathcal{OS}$'s secret shadow for each proxy signers is generated the same

way as in Scheme A. To hide the identities of the proxy singers, we redefine the $\mathcal{PS}$'s secret shadow as

$$Y_{i,j} = g_j(H_3(B_i))V.$$

Consequently, the validation equation should be modified and becomes:

$$\hat{e}(P, Y_{i,j}) = \hat{e}(P, y_j V) \prod_{k=1}^{t-1} \hat{e}(P, B_{j,k})^{H_3^k(B_i)}.$$

3.2.2. *Signature Generation Phase*

Assume that a message M is intended to be signed. Each participating proxy signer uses her secret shadow as the signing key to generate a partial signature. All t members in $\mathcal{S}$ execute the following procedure to generate their partial signatures:

1. Each C_i in $\mathcal{S}$ chooses a random number $r_i \in Z_m^*$, computes $R_i = r_i P, T_i = r_i d_{C_i}$, and broadcasts R_i and T_i to all other signers in $\mathcal{S}$.
2. After receiving all other $t-1$ R_j's and T_j's, each C_i in $\mathcal{S}$ computes $H = H_1(M, \sum_{i=1}^t R_i + \sum_{i=1}^t T_i)$, $E_i = r_i P_{pub}$ and $S_i = r_i H + l_i(K_i + Y_i)$, where $l_i = \prod_{C_j \in \mathcal{S}}^{j \neq i} \frac{0 - H_3(C_j)}{H_3(C_i) - H_3(C_j)}$, and sends the partial signature (S_i, R_i, T_i, E_i) to clerk C[3].
3. Each C_i computes $\hat{e}(P, l_i(K_i + Y_i))$, and sends them to clerk C.

After receiving all partial signatures, clerk C executes the following procedure to generate the threshold signature.

1. Compute $H = H_1(M, \sum_{i=1}^t R_i + \sum_{i=1}^t T_i)$.
2. Verify each partial signature according to the following two equations:

$$\begin{aligned} &\hat{e}(P, S_i) = \hat{e}(R_i, H)\hat{e}(P, l_i K_i)\hat{e}(P, l_i Y_i), \\ &\hat{e}(P, E_i + T_i) = \hat{e}(R_i, P_{pub})\hat{e}(E_i, Q_{C_i}). \end{aligned} \tag{6}$$

3. After confirming all partial signatures, compute $S = \sum_{i=1}^t S_i$, and publish $(w, (U, V), (S, W, R_1, R_2, \ldots, R_t, T_1, T_2, \ldots, T_t))$ as the traceable threshold proxy signature on message M.

3.2.3. *Signature Verification Phase*

The verifier employs the following procedure to verify the traceable threshold signature $(w, (U, V), (S, W, R_1, R_2, \ldots, R_t, T_1, T_2, \ldots, T_t))$ on message M.

1. Check if the message M conforms to the warrant w. Reject the signature if it does not conform. Otherwise continue on the next step.
2. Verify the warrant w and the certificate (U, V) by Eq. (4). Reject the signature if it does not hold. Otherwise continue on the next step.

[3] Any one of the signers could be designated as clerk C.

3. Compute $R = \sum_{i=1}^{t} R_i$, $H = H_1(M, R + \sum_{i=1}^{t} T_i)$, and accept the signature if and only if the following equation holds:

$$\hat{e}(P, S) = \hat{e}(R, H)\hat{e}(U, V)\hat{e}(P_{pub}, Q_A)\hat{e}(W, V). \tag{7}$$

3.2.4. *Trace Phase*

If any signature becomes controversial and the verifier needs to recover the signers of a certain message M. Then, the verifier sends M together with its signature $(w, (U, V), (S, W, R_1, R_2, \ldots, R_t, T_1, T_2, \ldots, T_t))$ to PKG, who is able to determine all the signers of the message by executing the following procedure:

1. Verify the signature is valid.
2. Compute $O_1 = (s^{-1} \bmod m)T_1$, where s is the system master key.
3. For the pair (R_1, O_1), try all B_j, where $1 \leqslant j \leqslant n$, in $\mathcal{PS}$, and call the one that exactly satisfies the following equation as C_1:

$$\hat{e}\big(H_2(B_j), R_1\big) = \hat{e}(O_1, P). \tag{8}$$

   Then C_1 is the one that leaves the trace pair (R_1, T_1).
4. Repeat the previous two steps and find C_i for all other trace pairs (R_i, T_i) for $2 \leqslant i \leqslant t$.
5. Send $(O_1, O_2, \ldots, O_t)$ and $(C_1, C_2, \ldots C_t)$ to the verifier.

The verifier can confirm the correctness of singers $(C_1, C_2, \ldots C_t)$ by the following equation:

$$\hat{e}\big(H_2(C_i), R_i\big) = \hat{e}(O_i, P)$$

for $1 \leqslant i \leqslant t$.

4. Analysis of Schemes

In this section, we show that our schemes work correctly by presenting some key properties. Then, we give a brief security analysis on our proposed schemes.

4.1. *Correctness*

Let K_i be the proxy shadow from $\mathcal{OS}$ for signer C_i in $\mathcal{S}$. Proposition 1 will enable us to establish the correctness of Eq. (5).

PROPOSITION 1. $\sum_{i=1}^{t} l_i K_i = x_a V + sQ_A$, where l_i and V are defined as in Section 3.

Proof.

$$\begin{aligned}\sum_{i=1}^{t} l_i K_i &= \sum_{i=1}^{t} l_i\big(f\big(H_3(C_i)\big)V + d_A\big)\\ &= \sum_{i=1}^{t} l_i f\big(H_3(C_i)\big)V + \sum_{i=1}^{t} l_i d_A\\ &= f(0)V + d_A\\ &= x_a V + sQ_A.\end{aligned}$$

Similarly, let Y_i be the secret shadow from $\mathcal{PS}$ for signer C_i in $\mathcal{S}$. We can show that:

PROPOSITION 2. $\sum_{i=1}^{t} l_i Y_i = \sum_{j=1}^{n} y_j V + s\sum_{j=1}^{n} Q_{B_j}$ in Scheme A, and $\sum_{i=1}^{t} l_i Y_i = \sum_{j=1}^{n} y_j V$ in Scheme T, where l_i and V are defined as in Section 3.

With Propositions 1 and 2, we then show that Eq. (5) holds for our threshold signature generated by following Scheme A.

Theorem 1. *If all participants honestly follow the Scheme A, then the threshold proxy signature can be successfully verified by Eq. (*5*).*

Proof. Equation (5) can be obtained as follows:

$$\begin{aligned}\hat{e}(P,S) &= \hat{e}\bigg(P, \sum_{i=1}^{t} S_i\bigg)\\ &= \hat{e}\bigg(P, \sum_{i=1}^{t}\big(r_i H_1(M,R) + l_i K_i + l_i Y_i\big)\bigg)\\ &= \hat{e}\bigg(P, \sum_{i=1}^{t} r_i H_1(M,R)\bigg)\hat{e}\bigg(P, \sum_{i=1}^{t} l_i K_i\bigg)\hat{e}\bigg(P, \sum_{i=1}^{t} l_i Y_i\bigg)\\ &= \hat{e}\bigg(\sum_{i=1}^{t} r_i P, H_1(M,R)\bigg)\hat{e}(P, x_a V + sQ_A)\hat{e}\bigg(P, \sum_{i=1}^{n} y_i V + s\sum_{j=1}^{n} Q_{B_j}\bigg)\\ &= \hat{e}\big(R, H_1(M,R)\big)\hat{e}(U,V)\hat{e}\bigg(P_{pub}, Q_A + \sum_{j=1}^{n} Q_{B_j}\bigg)\hat{e}(W,V).\end{aligned}$$

Proposition 3 shows that Eq. (6) holds if each proxy signer follows the signature generation procedure in Scheme T.

PROPOSITION 3. If all participants follow the procedure in the signature generation phase in Scheme T, then each tag (R_i, T_i) and E_i can be verified successfully by clerk C according to Eq.(6).

Proof. Equation (6) can be obtained as follows:

$$\begin{aligned}\hat{e}(P, E_i + T_i) &= \hat{e}(P, E_i)\hat{e}(P, T_i) \\ &= \hat{e}(P, r_i P_{pub})\hat{e}(P, r_i d_{C_i}) \\ &= \hat{e}(R_i, P_{pub})\hat{e}(E_i, Q_{C_i}).\end{aligned}$$

With Propositions 1 and 2, we then show that Eq. (7) holds for our traceable threshold proxy signature.

Theorem 2. *If all participants honestly follow the Scheme T, then the threshold proxy signature can be verified successfully according to Eq. (7).*

Proof. Equation (7) can be obtained as follows:

$$\begin{aligned}\hat{e}(P, S) &= \hat{e}\Big(P, \sum_{i=1}^{t} S_i\Big) \\ &= \hat{e}\Big(P, \Big(\sum_{i=1}^{t} r_i H + l_i K_i + l_i Y_i\Big)\Big) \\ &= \hat{e}\Big(P, \sum_{i=1}^{t} r_i H\Big)\hat{e}\Big(P, \sum_{i=1}^{t} l_i K_i\Big)\hat{e}\Big(P, \sum_{i=1}^{t} l_i Y_i\Big) \\ &= \hat{e}(R, H)\hat{e}(P, x_a V + sQ_A)\hat{e}\Big(P, \sum_{j=1}^{n} y_j V\Big) \\ &= \hat{e}(R, H)\hat{e}(U, V)\hat{e}(P_{pub}, Q_A)\hat{e}(W, V).\end{aligned}$$

Finally, we prove that Eq. (8) holds for our traceable signature.

PROPOSITION 4. Let R_i and O_i be defined as in Section 3.2. Only signer C_i satisfies the following equation: $\hat{e}(H_2(C_i), R_i) = \hat{e}(O_i, P)$ for $1 \leqslant i \leqslant t$.

Proof. We first show that C_i satisfies the equation:

$$\begin{aligned}\hat{e}\big(H_2(C_i), R_i\big) &= \hat{e}\big(H_2(C_i), r_i P\big) \\ &= \hat{e}\big(r_i H_2(C_i), P\big) \\ &= \hat{e}(O_i, P).\end{aligned}$$

The uniqueness of C_i follows from the property of the hashing function H_2, which produces no collision on all members in $\mathcal{PS}$.

4.2. *Security Analysis*

We next show that Scheme T satisfies all the necessary conditions addressed in Mambo *et al.* (1996) for proxy signature with delegation by warrant.

Unforgeability. Both our proposed schemes are based on SOK-IBS-1. More precisely, each proxy signer employs the SOK-IBS-1 in generating her partial signature, and proxy signer C_i uses $l_i(K_i + Y_i)$ as her signing key to sign messages; the summation of all proxy signers' signing keys is the secret key used in generating our threshold signatures. By property of the Lagrange interpolating polynomial, $t - 1$ or less proxy signers cannot reconstruct the proxy secret shadow. Therefore, both schemes are secure against uf-cma and strong uf-cma. Moreover, neither original signer nor third party is able to create a valid signature, since all secret values (y_i's) from $\mathcal{PS}$ are not available to them. Therefore, both our schemes satisfy *strong* unforgeability (Mambo *et al.*, 1996).

Verifiability. This is obvious, because each valid signature comes with a warrant w, and one can verify that the warrant is signed by the original signer using the secure SOK-IBS-1.

Proxy signer's deviation. Though t or more proxy signers may collude to obtain the proxy secret shadow, they are not able to forge a signature as signed by others without their private keys; this is because each proxy signer's private key is required in generating the trace tag. Moreover, Proposition 1 indicates that t or more proxy signers are not able to recover the original singer's secret key because x_a in unknown to them. Therefore, no proxy signer(s) is able to create a valid signature not detected as hers.

Distinguishability. This is obvious, because the format of the proxy signature is different from the self-signing signature.

Identifiability. One can determine the signers from the trace tag in any valid signature.

Undeniability. As mentioned in Mambo *et al.* (1996), this can be deduced from the unforgeability, proxy signer's deviation, and identifiability.

Additionally, we can see that Scheme A satisfies the conditions of unforgeability, verifiability, and distinguishability. Though a cooperation of t or more proxy signers may recover the secret key for our threshold signature schemes, no proxy singer is able to recover other (original/proxy) signer's secret key. Therefore, each valid signature is generated by some t or more members in $\mathcal{PS}$; consequently, Scheme A satisfies the condition of proxy signer's deviation in the sense of that every valid signature is generated by some signers in $\mathcal{PS}$. Similarly, Scheme A also satisfies the condition of identifiability in the sense of that one can verify each valid signature is generated by some signers in $\mathcal{PS}$.

5. Conclusion

Delegation of rights is a common practice in the real world. We have presented two identity-based threshold proxy signature schemes, which allow an original signer to delegate her signing capability to a group of n proxy signers, and it requires a consensus of t or more proxy signers in order to generate a valid signature. In addition to identity-based scheme, privacy protection for proxy singers and security assurance are two distinct features of our work. Scheme A provides a partial privacy protection whereas Scheme T provides a full privacy protection to proxy signers. Both our proposed schemes are secure against unforgeability under chosen message attack. Moreover, both schemes satisfy all

other necessary conditions, such as verifiability, proxy signer's deviation, distinguishability, identifiability, and undeniability, addressed in Mambo *et al.* (1996) for proxy signature.

References

Baek, J., Zheng, Y. (2004). Identity-based threshold signature scheme from the bilinear pairings. In: *ITCC '04*: *Proceedings of the International Conference on Information Technology*: *Coding and Computing* (*ITCC'04*), Vol. 2, pp. 124–128.

Bao, H., Cao, Z., Wang, S. (2006). Identity-based threshold proxy signature scheme with known signers. In: *Proc. Theory and Applications of Models of Computation*, pp. 538–546.

Bellare, M., Namprempre, C., Neven, G. (2004). Security proofs for identity-based identification and signature schemes. In: *Proc. EUROCRYPT 2004*, *Lecture Notes in Computer Science*, Vol. 3027. Springer, pp. 268–286.

Boneh, D. (1998). The decision Diffie–Hellman problem. *Lecture Notes in Computer Science*, Vol. 1423, pp. 48–63.

Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. *Lecture Notes in Computer Science*, Vol. 2139, pp. 213–229.

Boneh, D., Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3), 586–615.

Boneh, D., Lynn, B., Shacham, H. (2001). Short signatures from the Weil pairing. *Lecture Notes in Computer Science*, Vol. 2248, pp. 514–532.

Cha, J. C., Cheon, J. H. (2003). An identity-based signature from gap Diffie–Hellman groups. In: *PKC '03: Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography*. Springer, London, pp. 18–30.

Chen, L. (2007). An interpretation of identity-based cryptography. In: *Foundations of Security Analysis and Design IV*, pp. 183–208.

Cheng, X., Liu, J., Wang, X. (2005). An identity-based signature and its threshold version. In: *AINA '05*: *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, Washington DC, USA. IEEE Computer Society, pp. 973–977.

Chow, S.S., Hui, L.C., Yiu, S. (2004). Identity based threshold ring signature. *Cryptology ePrint Archive*, Report 2004/179.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In: *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pp. 360–363.

Gagne, M. (2002). *Applications of Bilinear Maps in Cryptography*. M.S. thesis, University of Waterloo.

Gangishetti, R., Gorantla, M.C., Das, M.L., Saxena, A. (2006). Identity based multisignatures. *Informatica*, 17(2), 177–186.

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

Guo, S., Cao, Z., Lu, R. (2006). An efficient id-based multi-proxy multi-signature scheme. In: *Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences*, pp. 81–88.

Hess, F. (2002). Efficient identity based signature schemes based on pairings. In: *9th Annual International Workshop on Selected Areas in Cryptography*. Springer, London, pp. 310–324.

Hwang, S.-J., Shi, C.-H. (2000). A simple multi-proxy signature scheme. In: *Proceedings of the Tenth National Conference on Information Security*, Taiwan, pp. 134–138.

Kanayama, N., Kobayashi, T., Saito, T., Uchiyama, S. (2000). Remarks on elliptic curve discrete logarithm problems. *IEICE Trans. on Fundamentals*, E83-A(1).

Kancharla, P.K., Gummadidala, S., Saxena, A. (2007). Identity based strong designated verifier signature scheme. *Informatica*, 239–252.

Lee, E.A. (2006). Cyber-physical systems – are computing foundations adequate? In: *NSF Workshop on Cyber-Physical Systems*.

Li, X., Chen, K. (2005). Id-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings. *Applied Mathematics and Computation*, 169(1), 437–450.

Li, S., Zhang, F. (2007). A new multi-proxy signature from bilinear pairing. *Journal of Electronics*, 90–94.

Libert, B. (2006). *New Secure Applications of Bilinear Maps in Cryptography*. PhD thesis, University of Louvain.

Libert, B., Quisquater, J. (2004). The exact security of an identity based signature and its applications. *Cryptology ePrint Archive*, Report 2004/102.

Lu, X.-M., Feng, D.-G. (2007). Security proof of the original SOK-IBS scheme. *International Journal of Network Security*, 5(2), 176–181.

Lu, R., He, D., Wang, C. (2007). On the security of an identity-based threshold proxy signature scheme with known signers. In: *3rd International Conference on Natural Computation*, pp. 210–214.

Mambo, M., Usuda, K., Okamoto, E. (1996). Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. on Fundamentals*, E79-A(9), 1338–1354.

Paterson, K. (2002). Id-based signatures from pairings on elliptic curves. *Electronics Letters*, 38(18), 1025–1026.

Paterson, K.G., Price, G. (2003). A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report*, 57–72.

Sakai, R., Ohgishi, K., Kasahara, M. (2000). Cryptosystems based on pairing. In: *SCIS 2000*, Okinawa, Japan, pp. 26–28.

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11), 612–613.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In: *Proceedings of CRYPTO 84 on Advances in Cryptology*. Springer, New York, pp. 47–53.

Shum, K., Wei, V.K. (2002). A strong proxy signature scheme with proxy signer privacy protection. In: *11th IEEE International Workshop on Enabling Technologies*: *Infrastructure for Collaborative Enterprises*, pp. 55–56.

Tseng, Y.-M., Wu, T.-Y., Wu, J.-D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 285–302.

Wang, M., Liu, Z. (2005). Identity based threshold proxy signcryption scheme. In: *CIT '05*: *Proceedings the Fifth International Conference on Computer and Information Technology*. Washington, IEEE Computer Society, pp. 695–701.

Wang, Q., Cao, Z. (2007). Identity based proxy multi-signature. *Journal of Systems and Software*, 1023–1029.

Wu, W., Mu, Y., Susilo, W., Seberry, J., Huang, X. (2007). Identity-based proxy signature from pairings. In: *The 4th International Conference on Autonomic and Trusted Computing*, pp. 22–31.

Xu, J., Zhang, Z., Feng, D. (2004). Identity based threshold proxy signature. *Cryptology ePrint Archive*, Report 2004/250.

Xu, J., Zhang, Z., Feng, D. (2005). Id-based proxy signature using bilinear pairings. In: *Parallel and Distributed Processing and Applications*, pp. 359–367.

Xu, Z., Liu, X., Zhang, G., He, W. (2008). A certificateless signature scheme for mobile wireless cyber-physical systems. In: *28th International Conf. on Distributed Computing Systems Workshops*, pp. 489–494.

Yi, X. (2003). An identity-based signature scheme from the Weil pairing. *Communications Letters IEEE*, 7(2), 76–78.

Yi, L., Bai, G., Xiao, G. (2000). Proxy multi-signature scheme: A new type of proxy signature scheme. *Electronic Letters*, 527–528.

Zhang, F., Kim, K. (2003). Efficient ID-based blind signature and proxy signature from bilinear pairings. In: *ACISP*, pp. 312–323.

J. Liu received his BS and MS degrees in nuclear engineering from National Tsing Hua University, also MS and PhD degrees in computer science from Michigan State University in 1979, 1981, 1987 and 1992, respectively. Since 1992, he has been an associate professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taiwan. His research interests include computer system security, parallel and distributed processing, and computer algorithms.

S. Huang received his BS in applied mathematics and MS in information engineering and computer science from Feng Chia University. His research interests include information and computer security. Since 2007, he works as a software engineer for private section in Taiwan.

Identifikatoriumi pagrįstas slenkstinis įgaliotasis parašas naudojantis bitiesinius poravimus

Jenshiuh LIU, Shaonong HUANG

Nagrinėjami du identifikatoriumi pagrįsti slenkstiniai įgaliotųjų parašų algoritmai, kurie įgalina asmenį perduoti savo pasirašymo teisę jo įgaliotiems n asmenims. Tokiu atveju būtinas t arba daugiau įgaliotųjų asmenų susitarimas tam, kad būtų gautas galiojantis parašas. Pirmasis algoritmas užtikrina įgaliotųjų asmenų tik dalinę privatumo apsaug. Tuo tarpu antrasis algoritmas garantuoja visų įgaliotųjų asmenų privatumą. Abu algoritmai yra nesuklastojami esant pasirinktai pranešimo atakai ir tenkina kitas būtinas įgaliotojo parašo sąlygas.