Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A secure threshold Paillier proxy signature scheme

Pei-yih TING†, Xiao-wei HUANG, Jun-hui WU, Chia-huei HSEU

(*Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung 20224, Taiwan, China*)

†E-mail: pyting@mail.ntou.edu.tw

Received Aug. 11, 2009; Revision accepted Dec. 10, 2009; Crosschecked Jan. 12, 2010

Abstract: As e-commerce applications and the underlying public key infrastructure have become more popular over time, many digital mechanisms emulating traditional business activities have been developed and deployed. To build a full-fledged secure digital world, secure implementations of more commercial activity primitives are required. In this paper, we present a secure proxy signature scheme and its threshold version based on the homomorphic Paillier cryptosystem, which can be used in many e-commerce applications such as e-voting, e-bidding/auction, and privacy-preserving data mining. These two schemes are existentially unforgeable against chosen-message attacks and chosen-warrant attacks in the random oracle model. Although it is based on factoring, the threshold Paillier proxy scheme operates without requiring any trusted dealer or combiner. Thus, these two schemes are practical for integration in modularized secure multi-party protocols.

Key words: Paillier proxy signature, Threshold scheme, Secure multi-party protocols, Cryptographic primitives
doi:10.1631/jzus.C0910493 **Document code:** A **CLC number:** TP309.7

1 Introduction

As e-commerce applications and the underlying public key infrastructure have become more popular over time, many digital mechanisms emulating traditional business activities have been developed and deployed, e.g., the digital signature scheme (Rivest *et al*., 1978; ElGamal, 1985; Paillier, 1999; Sun *et al*., 2008), which mimics the signing process. The accompanying security and trust issues have been analyzed extensively. In order to build a full-fledged secure digital world, secure implementations of more commercial activities primitives are required.

In this paper, we present the proxy signature mechanism (Mambo *et al*., 1996) based on the homomorphic Paillier cryptosystem (Paillier, 1999; Jiang *et al*., 2008). Proxy schemes can be used in applications such as e-voting, contract signing, e-bidding/auction, private information retrieval, and privacy-preserving data mining. In these applications, a party (the original signer) responsible for a task may be preoccupied in some other business and wish to delegate his/her signing capacity to a designated person (the proxy signer) such that both will be responsible for the documents approved by the proxy signer. Over the past several years, there have been many extensions on the basic proxy scheme. For example, Yi *et al*. (2000) enabled multiple signers to delegate their joint signing capacity to one proxy signer. Shum and Wei (2002) proposed a scheme that protected the proxy signer's identity. Wang and Pieprzyk (2003) proposed an efficient one-time proxy signature scheme. Lu and Cao (2004) presented a Schnorr-based proxy signature scheme based on the discrete logarithm problem over a conic group. Boldyreva *et al*. (2003) formalized the security notion for proxy signature and presented a provably secure scheme. Schdult *et al*. (2008) further completed the security model for a proxy signature scheme under the proxy key exposure attack. In a proxy scheme, the original signer has to trust the discerning capability of the proxy signer for the period of delegation. Although 'trust' is so convenient an assumption for running protocols efficiently, it is a double-edged sword that could endanger the security of many applications designed based on assumptions of the good will of participants. To alleviate the severity of abused trust, the responsibility is usually shared over a group of representatives. For example, in a threshold proxy signature scheme (Sun *et*

al., 1999), a valid proxy signature can be produced only when a group of proxy signers, satisfying a specific access structure, approves the contents of documents.

In the past, threshold proxy signature schemes based on the factoring problem faced more difficulties than schemes (Sun *et al*., 1999; Javier and German, 2004) based on the discrete logarithm problem. For example, Hwang's threshold RSA proxy signature scheme (Hwang *et al*., 2003) breaks down when d colluding proxy signers derive the private key of the original signer (Wang *et al*., 2004), where d is the threshold. Later, Lu *et al*. (2005) proposed a threshold proxy signature scheme that required a trusted dealer. Chang and Chang (2007) also proposed an RSA-based threshold proxy signature scheme to fix the security flaws of Hwang's scheme. However, the latter scheme required a trusted combiner to avoid the leakage of the secret key. Contrary to the above unsuccessful approaches, Shoup's threshold RSA signature scheme (Shoup, 2000) which requires minimal trust assumption is provably secure and is efficient in that every participant can proceed signing a document independently. In our previous work (Ting and Huang, 2008), we developed an efficient RSA threshold proxy scheme following Shoup's methodology.

In this paper, we first propose a provably secure proxy signature scheme for the factoring-based Paillier cryptosystem then extend it to a distributed threshold proxy scheme. The additive homomorphism of the Paillier system is preserved in both schemes and allows various goals to be accomplished securely in applications like e-auction (Abe and Suzuki, 2002), e-voting (Baudron *et al*., 2001), private information retrieval (Chang, 2004), or privacy-preserving data mining (Zhang *et al*., 2005; Magkos *et al*., 2008; Li *et al*., 2009). The proposed proxy scheme is designed parallel to both the Schnorr signature scheme (Schnorr, 1991) and the Guillou-Quisquater signature scheme (Guillou and Quisquater, 1988). The proposed threshold scheme extends the ideas of Shoup's threshold RSA scheme (Shoup, 2000) to the group of quadratic residues $\mathbb{QR}_{n^2}$. In addition, since a proxy signature scheme has the same architecture as an identity based signature scheme, both schemes can be suitably modified for those applications.

2 Paillier signature scheme

In the following, we briefly summarize the Paillier probabilistic signature scheme (Paillier, 1999). The choice of parameters deviates slightly from the original scheme due to the proposed extensions to the proxy and the threshold proxy signature schemes.

Key generation Let the public key of a signer be (n,g), where $n=p\cdot q$, $p=2p'+1$, $q=2q'+1$ (the constraints $p=2p'+1$ and $q=2q'+1$ are required only in the threshold proxy signature scheme such that generators in $\mathbb{QR}_{n^2}$ can be easily selected without the knowledge of p or q), p, q, p', q' are large prime numbers, and $g\in\mathbb{QR}_{n^2}$ (let $\mathbb{QR}_{n^2}$ denote the set of quadratic residues in $\mathbb{Z}_{n^2}$) satisfies $\mathrm{ord}_{n^2}(g)=n\cdot p'\cdot q'$. The corresponding private key is $m=p'\cdot q'$.

Signing Given an arbitrary message M, the corresponding signature (s,t) is computed as follows:

$$s\equiv\frac{L(h(M)^m \bmod n^2)}{L(g^m \bmod n^2)} \pmod n,$$

$$t\equiv\left(h(M)\cdot g^{-s}\right)^{n^{-1}\,(\bmod m)} \pmod n,$$

where $L(u)\triangleq(u-1)/n$ for $u\equiv 1 \pmod n$ and $h(\cdot)$ is a collision-resistant hash function that maps a message of arbitrary length to an element in $\mathbb{QR}_{n^2}$. Practically, one can use a collision-resistant hash function $h'(\cdot)$ that maps $\{0,1\}^*$ to $\mathbb{Z}_n^*$ and let $h(M)\equiv h'(M)^2 \pmod{n^2}$ for a message M.

Verification A verifier checks that $h(M)\stackrel{?}{\equiv}g^s\cdot t^n \pmod{n^2}$. If this congruence equation is satisfied, the pair (s,t) is a valid signature for the message M.

Please refer to (Paillier, 1999, Theorems 14 and 15) for the correctness and security issues of this scheme. Based on the intractability assumption of breaking the RSA function, the above Paillier signature scheme is proven existentially unforgeable against chosen-message attacks in the random oracle model (Paillier, 1999, Corollary 18).

3 Paillier proxy signature scheme

3.1 The proposed Paillier proxy signature scheme

In this section, we present the Paillier proxy signature scheme, the security proof of which will be provided in Section 5.

Key generation The choices for the public and private keys are the same as described in Section 2.

Delegation The public key of the original signer P_0 is (n,g) and the corresponding private key is m. The proxy signer P_1 is associated with a unique identification number ID_1. The original signer P_0 prepares the warrant

W_1 for the proxy signer P_1 and computes the proxy key (x,y) as follows:

$$x \equiv \frac{L(h(0||W_1||\mathrm{ID}_1)^m \bmod n^2)}{L(g^m \bmod n^2)} \pmod n,$$
$$y \equiv (h(0||W_1||\mathrm{ID}_1)\cdot g^{-x})^{n^{-1} \pmod m} \pmod n,$$

where '||' denotes the concatenation of two strings.

The original signer P_0 publishes the warrant W_1 and sends the proxy key pair (x,y) to the proxy signer P_1 via a secure channel. The proxy signer P_1 verifies the received proxy key pair by the following:

$$h(0||W_1||\mathrm{ID}_1) \equiv g^x \cdot y^n \pmod{n^2},$$

which is essentially the verification equation of a standard Paillier signature scheme.

Proxy signing The proxy signer P_1 signs a message M on behalf of the original signer P_0 as follows:

1. P_1 picks a pair of random numbers (a,b), where $a \in \mathbb{Z}_{n^3}, b \in \mathbb{QR}_n$, and computes and publishes $R \equiv g^a \cdot b^n \pmod{n^2}$.

2. P_1 computes s and t as follows:

$$\begin{cases} s = x \cdot h(1||M||R) + a, \\ t \equiv y^{h(1||M||R)} \cdot b \pmod n. \end{cases} \tag{1}$$

The proxy signature is (s,t,R).

Verification Anyone can verify the validity of a proxy signature (s,t,R) of a message M with the public key (n,g) of the original signer, the warrant W_1, and the identification ID_1 of the proxy signer P_1 through the following congruence:

$$g^s \cdot t^n \stackrel{?}{\equiv} h(0||W_1||\mathrm{ID}_1)^{h(1||M||R)} \cdot R \pmod{n^2}.$$

Note that

$$\begin{aligned} g^s \cdot t^n &\equiv (g^x)^{h(1||M||R)} \cdot g^a \cdot (y^n)^{h(1||M||R)} \cdot b^n \\ &\equiv h(0||W_1||\mathrm{ID}_1)^{h(1||M||R)} \cdot R \pmod{n^2}. \end{aligned}$$

3.2 Threshold extension

In order to derive the threshold version, we further modify the components of Eq. (1) as follows:

$$\begin{cases} s = x \cdot h(1||M||R) + a\Delta, \\ t \equiv y^{h(1||M||R)} \cdot b^{\Delta} \pmod n, \\ R \equiv (g^a \cdot b^n)^{\Delta} \pmod{n^2}, \end{cases}$$

where $\Delta = \ell!$ for a (d,ℓ)-threshold scheme and the proxy signature (s,t,R) satisfies the verification equation

$$g^s \cdot t^n \equiv h(0||W||\mathrm{ID})^{h(1||M||R)} \cdot R \pmod{n^2}.$$

Since both $f_1(a) \equiv \Delta a \pmod{mn}$ and $f_2(b) \equiv \Delta \log_g b \pmod m$ are permutations provided that $\gcd(\Delta, mn) = 1$ and $\gcd(\Delta, m) = 1$, the values $a\Delta \pmod{mn}$ and $b^{\Delta} \pmod n$ are still randomly distributed over $\mathbb{Z}^*_{mn}$ and $\mathbb{QR}_n$, respectively.

In a (d,ℓ)-threshold proxy scheme, we would like to share secretly the proxy key (x,y) to a set of proxy signers $\{P_i\}_{i=1,2,\ldots,\ell}$ ($\ell << n$) such that any subset S of these signers $\{P_i\}_{i\in S}$ with $\ell \geq |S| \geq d$ can jointly sign a document M on behalf of the original signer P_0.

Using Shamir's polynomial secret sharing (Shamir, 1979), the first part of the proxy key x is shared among $\{P_i\}_{i=1,2,\ldots,\ell}$ as $\{x_i\}_{i=1,2,\ldots,\ell}$ such that $x \equiv \sum_{i\in S} x_i L_i(0) \pmod{mn}$. Each proxy signer P_i later individually calculates the signature share $s_i = x_i \cdot h(1||M||R) + a_i\Delta$. The first part of the proxy signature, s, can be reconstructed later from $\{s_i\}_{i\in S}$, i.e., $s\Delta = \left(\sum_{i\in S} s_i L_i(0)\right)\Delta = h(1||M||R)\left(\sum_{i\in S} x_i L_i(0)\right)\Delta + \Delta^2\left(\sum_{i\in S} a_i L_i(0)\right)$, where $L_i(x) \triangleq \prod_{j\in S\setminus\{i\}} \frac{x-j}{i-j}$ is the ith term of the Lagrange interpolation polynomial. In this procedure, the shared secret x_i is not revealed at the time a document is signed and can be reused later. Note that Δ introduced here cancels all those $i-j$ denominators in $L_i(x)$ such that the reconstruction can be done without the secret modulus mn.

On the other hand, the second part of the proxy key y should not be shared among $\{P_i\}_{i=1,2,\ldots,\ell}$ as $\{y_i\}_{i=1,2,\ldots,\ell}$ in a similar way such that $y \equiv \sum_{i\in S} y_i L_i(0) \pmod n$. In that way, each proxy signer would not be able to produce proxy signature share independently and the proxy key y is exposed after signing one proxy signature.

To avoid this problem, we pick an arbitrary element $D \in \mathbb{Z}^*_m$ as the exponent to be shared among $\{P_i\}_{i=1,2,\ldots,\ell}$ as $\{D_i\}_{i=1,2,\ldots,\ell}$ such that $D \equiv \sum_{i\in S} D_i L_i(0) \pmod m$. One calculates the inverse of $D \pmod m$, i.e., $G \equiv D^{-1} \pmod m$, calculates $C \equiv y^G \pmod n$, and publishes C as the base. The second part of the proxy signature becomes $t \equiv C^{D\cdot h(1||M||R)} \cdot b^{\Delta} \pmod n$ and can be reconstructed from individual signature shares by calculating $\prod_{i\in S}\left(\left(C^{h(1||M||R)}\right)^{D_i} \cdot b_i^{\Delta}\right)^{\Delta L_i(0)} \equiv$

$$\left(y^{h(1||M||R)}\cdot\prod_{i\in S}b_i^{\Delta L_i(0)}\right)^{\Delta}\pmod n.$$

4 Threshold Paillier proxy signature scheme

The setup of this scheme consists of an original signer P_0, ℓ proxy signers $\{P_i\}_{i=1,2,\ldots,\ell}$, and a verifier. For a proxy protected threshold scheme, each proxy signer, P_i, associated with a unique identifier ID_i, also has his/her own secret key m_i of a Paillier cryptosystem with public key (n_i,g_i).

Key generation The choices of the public and private keys are the same as described in Section 2.

Delegation P_0 computes the proxy key (x_i,D_i) for each P_i:

1. P_0 calculates the master proxy key (x,y):

$$x\equiv\frac{L(h(0||W||\mathrm{ID})^m \bmod n^2)}{L(g^m \bmod n^2)}\pmod n,$$
$$y\equiv\left(h(0||W||\mathrm{ID})g^{-x}\right)^{n^{-1}\,(\mathrm{mod}\,m)}\pmod n,$$

where $\mathrm{ID}=\mathrm{ID}_1||\mathrm{ID}_2||\cdots||\mathrm{ID}_\ell$ and W is the group warrant.

2. P_0 picks a random element $D\in\mathbb{Z}_m^*$, computes $G\equiv D^{-1}\pmod m$, calculates $C\equiv y^G\pmod n$, and publishes C.

3. P_0 picks two degree-$(d-1)$ polynomials $f(X)=x+r_1X+r_2X^2+\cdots+r_{d-1}X^{d-1}$ and $F(X)=D+R_1X+R_2X^2+R_3X^3+\cdots+R_{d-1}X^{d-1}$, where $r_i\in\mathbb{Z}_{mn}$ and $R_i\in\mathbb{Z}_m$ are random numbers.

4. P_0 sends the proxy key pair $x_i\equiv f(i)\pmod{mn}$ and $D_i\equiv F(i)\pmod m$ to P_i in a secure manner for $i=1,2,\cdots,\ell$.

5. P_0 computes the public verification key pair $u_i\equiv g^{x_i}\pmod{n^2}$ and $v_i\equiv\left(C^{D_i}\right)^n\pmod{n^2}$ for $i=1,2,\cdots,\ell$ and publishes $\{u_i\}_{i=1,2,\cdots,\ell}$ and $\{v_i\}_{i=1,2,\cdots,\ell}$.

Proxy key verification P_i checks whether the following congruences are satisfied:

$$u_i\equiv g^{x_i}\pmod{n^2},$$
$$v_i\equiv\left(C^{D_i}\right)^n\pmod{n^2},$$
$$h(0||W||\mathrm{ID})^{\Delta}\equiv\prod_{i=1}^{\ell}(u_i\cdot v_i)^{\Delta L_i(0)}$$
$$\left(\equiv(g^x\cdot y^n)^{\Delta}\right)\pmod{n^2}.$$

Proxy signature share generation A set S of at least d proxy signers jointly sign a message M as follows:

1. A proxy signer P_i $(i\in S)$ picks two random numbers (a_i,b_i) secretly such that $a_i\in\mathbb{Z}_{n^3/4}$, $b_i\in\mathbb{QR}_n$.

2. P_i computes and publishes commitments A_i and B_i as follows:

$$A_i\equiv g^{a_i}\pmod{n^2},$$
$$B_i\equiv b_i^n\pmod{n^2}.$$

3. A public commitment value R is derived from the set of public commitments $\{A_i,B_i\}_{i\in S}$ by

$$R\equiv\prod_{i\in S}(A_i\cdot B_i)^{\Delta L_i(0)}\pmod{n^2}.$$

4. P_i computes and publishes his/her signature share (s_i,t_i) as

$$s_i=x_i\cdot h(1||M||R)+a_i\Delta,$$
$$t_i\equiv(C^{h(1||M||R)})^{D_i}\cdot b_i^{\Delta}\pmod n.$$

5. If the scheme is proxy protected, each P_i chooses a collision-resistant hash function $H_i(\cdot)$, which maps messages of arbitrary length to elements in $\mathbb{QR}^*_{n_i^2}$, and signs $H_i(s_i||t_i)$ with his/her own Paillier secret key m_i, i.e., $\sigma_i\equiv\dfrac{L(H_i(s_i||t_i)^{m_i}\bmod {n_i}^2)}{L({g_i}^{m_i}\bmod {n_i}^2)}\pmod{n_i}$ and $\tau_i\equiv(H_i(s_i||t_i)\cdot {g_i}^{-\sigma_i})^{{n_i}^{-1}\,(\mathrm{mod}\,m_i)}\pmod{n_i}$.

Proxy signature share verification P_i's proxy signature share (s_i,t_i) should satisfy the following congruence equations:

$$g^{s_i}\equiv {u_i}^{h(1||M||R)}\cdot {A_i}^{\Delta}\pmod{n^2},$$
$$t_i^n\equiv {v_i}^{h(1||M||R)}\cdot {B_i}^{\Delta}\pmod{n^2}.$$

The proxy-signing protocol aborts if the number of valid signature shares is less than d.

Proxy signature combination The proxy signature (s,t) is computed from the proxy signature shares as follows:

1. Calculate s from $\{s_i\}_{i\in S}$ as follows:

$$S_1=\sum_{i\in S}s_i\cdot(\Delta\cdot L_i(0))=(x\cdot h(1||M||R)+a)\Delta,$$
$$s=S_1/\Delta=x\cdot h(1||M||R)+a,$$

where $a\triangleq\sum_{i\in S}a_i\cdot(\Delta\cdot L_i(0))$.

2. Calculate t from $\{t_i\}_{i\in S}$ as follows:

(1) Calculate T_1 from $\{t_i\}_{i\in S}$:

$$T_1\equiv\prod_{i\in S}t_i^{\Delta L_i(0)}\pmod n,$$
$$\left(\equiv C^{h(1||M||R)D\Delta}\cdot b^{\Delta}\equiv\left(y^{h(1||M||R)}\cdot b\right)^{\Delta}\right)$$

where $b \stackrel{\triangle}{\equiv} \prod_{i \in S} b_i^{\Delta L_i(0)} \pmod{n}$. Note that the public commitment value $R \equiv \prod_{i \in S} (A_i \cdot B_i)^{\Delta L_i(0)} \equiv g^a \cdot b^n \pmod{n^2}$.

(2) Calculate T_2 from W, ID, M, R and s:

$$\begin{aligned} T_2 &\equiv h(0||W||\mathrm{ID})^{h(1||M||R)} \cdot R \cdot g^{-s} \\ &\equiv (g^x y^n)^{h(1||M||R)} \cdot (g^a b^n) \cdot g^{-s} \\ &\equiv \left(y^{h(1||M||R)} \cdot b\right)^n \pmod{n}. \end{aligned}$$

(3) Since $\gcd(\Delta, n) = 1$, there exist two integers c_1 and c_2 such that $c_1\Delta + c_2 n = 1$. The combined signature component t is calculated as follows:

$$\begin{aligned} t &\equiv (T_1)^{c_1} \cdot (T_2)^{c_2} \\ &\equiv \left(y^{h(1||M||R)} \cdot b\right)^{\Delta c_1 + n c_2} \\ &\equiv y^{h(1||M||R)} \cdot b \pmod{n}. \end{aligned}$$

3. $(M, W, \mathrm{ID}, s, t, R)$ is the proxy signature on message M.

Proxy signature verification The proxy signature is verified through the following congruence:

$$R \cdot h(0||W||\mathrm{ID})^{h(1||M||R)} \equiv g^s \cdot t^n \pmod{n^2}.$$

In order to protect each proxy signer against a malicious original signer, a verifier could check for every $i \in S$ that

$$H_i(s_i||t_i) \stackrel{?}{\equiv} g_i^{\sigma_i} \cdot \tau_i^{n_i} \pmod{{n_i}^2}.$$

5 Security analysis

In this section, we give a definition of an unforgeable proxy signature and prove that our proxy signature scheme is existentially unforgeable under a chosen-message and chosen-warrant attack.

Definition 1 An adversary F is a probabilistic polynomial-time algorithm with accesses to a random oracle $\mathcal{H}$, a proxy signing oracle Σ for the proxy signer P_1 with identifier ID_1 and warrant W_1, and a delegation oracle $\mathcal{D}$ for the original signer P_0. The output of F is $(M, W_1, \mathrm{ID}_1, s, t, R)$. We say that F successfully forges a proxy signature of P_1 for some message M if its output $(M, W_1, \mathrm{ID}_1, s, t, R)$ satisfies the verification equation, $g^s \cdot t^n \equiv h(0||W_1||\mathrm{ID}_1)^{h(1||M||R)} \cdot R \pmod{n^2}$, where (W_1, ID_1) has not been asked of $\mathcal{D}$ and M has not been asked of Σ. The proxy signature scheme is existentially unforgeable against a chosen-message and chosen-warrant attack in the random oracle model if for every adversary F the probability of any successful forgery is computationally negligible.

Theorem 1 The Paillier proxy signature scheme described in Section 3 is existentially unforgeable against chosen-message attacks and chosen-warrant attacks in the random oracle model.

Proof Consider the proposed Paillier proxy signature scheme. Suppose F is an adversary that can forge a Paillier proxy signature with non-negligible success probability. F is given accesses to a random oracle $\mathcal{H}$, a signing oracle Σ, and a delegation oracle $\mathcal{D}$. We construct a probabilistic polynomial-time algorithm $Q((n,g),C)$ using F as a black box to invert an arbitrary Paillier ciphertext C with non-negligible probability, where (n,g) is the corresponding encryption public key. This in turn contradicts with the computational composite residuosity assumption that there exists no polynomial-time algorithm for solving the composite residuosity class problem (Paillier, 1999, Conjecture 13). As F is a chosen-message and chosen-warrant attacker, Q has to simulate indistinguishably the hash oracle $\mathcal{H}$, the signing oracle Σ, and the delegation oracle $\mathcal{D}$ for F and invokes F with warrant $W_1||\mathrm{ID}_1$ and public key (n,g).

Q simulates the random oracle $\mathcal{H}$ as follows:

1. $\mathcal{H}$ keeps a list $\mathcal{L} = \{(u_1,h_1),(u_2,h_2),\cdots\}$, where $u_i \in \{0,1\}^*$ is the query and $h_i \in \mathbb{QR}_{n^2}$ is the corresponding hash value.

2. For a query $u = 0||W_1||\mathrm{ID}_1$, where $(u,\cdot) \notin \mathcal{L}$, $\mathcal{H}$ appends (u,C) to $\mathcal{L}$ and returns C.

3. For a query $u = 0||W||\mathrm{ID} \neq 0||W_1||\mathrm{ID}_1$, where $(u,\cdot) \notin \mathcal{L}$, $\mathcal{H}$ randomly chooses $x \in \mathbb{Z}_n, y \in \mathbb{Z}_n^*$ and returns $g^x y^n \pmod{n^2}$. $\mathcal{H}$ appends $(u, g^x y^n \pmod{n^2})$ to $\mathcal{L}$ and keeps (x,y) for answering possible delegation queries later.

4. If a query u has already been asked of such that $(u_i = u, h_i) \in \mathcal{L}$, $\mathcal{H}$ returns the corresponding h_i.

Because Q is in full control of the random oracle $\mathcal{H}$, Q simulates the proxy signing oracle Σ together with $\mathcal{H}$ to answer F's signing queries as follows:

1. When a message M is queried of, Σ randomly picks $s \in \mathbb{Z}_{n^3}$ (in Eq. (1), $s = x \cdot h(1||M||R) + a$, where $x \in \mathbb{Z}_n$, $h(1||M||R) \in \mathbb{QR}_{n^2}$, $a \in \mathbb{Z}_{n^3}$. To simulate the distribution of a real s, we randomly pick a number in $\mathbb{Z}_{n^3}$), $t \in \mathbb{QR}_n$, and $h \in \mathbb{QR}_{n^2}$, queries $\mathcal{H}$ of $0||W_1||\mathrm{ID}_1$ to obtain C, and computes $R \equiv g^s t^n \cdot C^{-h} \pmod{n^2}$.

2. Σ checks if $(1||M||R,\cdot) \notin \mathcal{L}$, appends $(1||M||R,h)$ to $\mathcal{L}$, and returns (s,t,R); otherwise, if $(1||M||R,\cdot) \in \mathcal{L}$, aborts.

Similarly, Q simulates the delegation oracle $\mathcal{D}$ with

full control of the random oracle $\mathcal{H}$ as follows:

Let $W||\mathrm{ID}$ denote the query to $\mathcal{D}$. If $(0||W||\mathrm{ID},\cdot)\in\mathcal{L}$, $\mathcal{D}$ returns the corresponding (x,y) such that $g^x y^n = \mathcal{H}(0||W||\mathrm{ID})$ as in Step 3 of the simulation of $\mathcal{H}$; else if $(0||W||\mathrm{ID},\cdot)\notin\mathcal{L}$, $\mathcal{D}$ randomly chooses $x\in\mathbb{Z}_n, y\in{\mathbb{Z}_n}^*$, returns (x,y), and appends $(0||W||\mathrm{ID}, g^x y^n \pmod{n^2})$ to $\mathcal{L}$ for the random oracle query.

Assume that, with non-negligible probability, F outputs for a message M the valid proxy signature (s,t,R), satisfying $R\cdot h(0||W_1||\mathrm{ID}_1)^{h(1||M||R)} \equiv g^s\cdot t^n \pmod{n^2}$. F must have asked the queries $0||W_1||\mathrm{ID}_1$ and $1||M||R$ of the random oracle $\mathcal{H}$. Let $(1||M||R,h)$ be the βth (query, response) pair in $\mathcal{L}$. By the oracle replay attack (Pointcheval and Stern, 2000), Q invokes F again with the same random tape, the same input, the same responses of the random oracle $\mathcal{H}$, the signing oracle Σ, and the delegation oracle $\mathcal{D}$ up to the $(\beta-1)$th random oracle query. Q replaces the βth response of $\mathcal{H}$ by randomly choosing an $h'\in\mathbb{QR}_{n^2}$ such that $h'\neq h$, and continues to simulate randomly $\mathcal{H}$, Σ, and $\mathcal{D}$ thereafter. Thus, F succeeds with non-negligible probability in forging another signature (s',t',R) with respect to the same commitment R according to the forking lemma (Pointcheval and Stern, 2000). These two signatures (s,t,R) and (s',t',R) satisfy

$$R\equiv g^s\cdot t^n\cdot h(0||W_1||\mathrm{ID}_1)^{-h}\equiv g^s\cdot t^n\cdot C^{-h}, \tag{2}$$

$$R\equiv g^{s'}\cdot (t')^n\cdot h(0||W_1||\mathrm{ID}_1)^{-h'}\equiv g^{s'}\cdot (t')^n\cdot C^{-h'}, \tag{3}$$

where $h(0||W_1||\mathrm{ID}_1)=C$ is guaranteed by the $\mathcal{H}$ oracle.

From Eqs. (2) and (3), we obtain:

$$g^s\cdot t^n\cdot C^{-h}\equiv g^{s'}\cdot (t')^n\cdot C^{-h'} \pmod{n^2},$$
$$\Rightarrow C^{h-h'}\equiv g^{s-s'}\cdot (t\cdot (t')^{-1})^n \pmod{n^2}.$$

As $mn=p\cdot q\cdot p'\cdot q'$, $\gcd(h-h',mn)=1$ with overwhelming probability, $(h-h')^{-1} \pmod{mn}$ exists. The above congruence can be rewritten as

$$C\equiv g^{M'}\cdot (T')^n \pmod{n^2},$$

where $M'\equiv (s-s')(h-h')^{-1} \pmod{mn}$, $T'\equiv \left(t\cdot (t')^{-1}\right)^{(h-h')^{-1}} \pmod{n}$, $M'\in\mathbb{Z}_{mn}$, and $T'\in\mathbb{Z}_n$. Let $M\equiv (s-s')(h-h')^{-1} \pmod{n}$, where $M\in\mathbb{Z}_n$. It is clear that $M\equiv M' \pmod{n}$. Also, this means that there exists a unique integer b such that $M'=M+bn$. Therefore,

$$C\equiv g^{M+bn}(T')^n\equiv g^M(g^bT')^n \pmod{n^2}.$$

As any Paillier ciphertext $C\in\mathbb{Z}_{n^2}$ can be uniquely decrypted, the decrypted message corresponding to C is M from the above equation. Thus, the algorithm Q has successfully found the corresponding plaintext M of C. This contradicts with the computational composite residuosity assumption.

In the following, the above is extended to prove the security of the (d,ℓ)-threshold Paillier proxy signature scheme.

Theorem 2 The (d,ℓ)-threshold Paillier proxy signature scheme is existentially unforgeable against a chosen-message and chosen-warrant attack.

Proof (Sketch) A construction of algorithm Q to break the underlying Paillier cryptosystem similar to the previous one is used to prove that the (d,ℓ)-threshold Paillier proxy signature scheme is existentially unforgeable against a chosen-message and chosen-warrant attack. The primary difference of the adversary F', which breaks the (d,ℓ)-threshold Paillier proxy signature scheme, from the previous adversary F is that F' knows the set S^- of proxy signing keys of the corrupted signers in the threshold scheme, where the number of corrupted signers is less than d. We describe how the algorithm Q chooses S^- for F' and the remaining parts of Q are the same as the previous construction. Without loss of generality, let $\{P_i\}_{i=1,2,\cdots,d-1}$ be the set of corrupted signers. In a real protocol, the proxy key (x_i,D_i) of a proxy signer P_i is uniformly distributed in the sets $\{0,1,\cdots,mn-1\}$ and $\{0,1,\cdots,m-1\}$, respectively. However, since m is unknown to Q, Q can pick only from the sets $\{0,1,\cdots,\lfloor n^2/4\rfloor-1\}$ and $\{0,1,\cdots,\lfloor n/4\rfloor-1\}$ two random numbers x_i,D_i as the proxy keys for P_i. Let $S^-=\{(x_i,D_i)\}_{i=1,2,\cdots,d-1}$ be the proxy keys for the corrupted set of signers and be part of the input of F'. The statistical distances between simulated and real (x_i,D_i) are both $O(n^{-\frac{1}{2}})$, which are polynomially negligible, since

$$\frac{n^2}{4}-mn=(\frac{p'+q'}{2}+\frac{1}{4})n\approx O(n^{\frac{3}{2}}),$$
$$\frac{n}{4}-m=\frac{p'+q'}{2}+\frac{1}{4}\approx O(n^{\frac{1}{2}}).$$

Because the dth proxy key (x_d,D_d), given the information $\{(x_i,D_i)\}_{i=1,2,\cdots,d-1}$, is completely unconstrained, the adversary F' gains from S^- insignificant advantage. Hence, as in the previous proof, we construct Q using F' as a black box: If F' is given S^- and F' forges with non-negligible probability a set of proxy signature shares $\{s_i,t_i\}_{i=1,2,\cdots,d}$ corresponding to a commitment R, Q obtains a proxy signature (s,t,R) through the proxy signature combining protocol. By the oracle replay attack, Q

invokes F' again with a similar setting as in the previous proof and F' forges with non-negligible probability another set of proxy signature shares $\{s_i', t_i'\}_{i=1,2,\cdots,d}$ for the same commitment R. Then Q obtains another proxy signature (s', t', R). These two proxy signatures (s, t, R) and (s', t', R) satisfy Eqs. (2) and (3). By using the same method as in the previous proof, the Paillier ciphertext C can be inverted again. This contradicts the computational composite residuosity assumption.

6 Conclusion

In this paper, we present a secure Paillier proxy signature scheme and its threshold version. These two schemes are proven existentially unforgeable against a chosen-message and chosen-warrant attack in the random oracle model. Although it is based on the integer factoring problem, the round efficiency of the threshold scheme is comparable with a discrete-log based scheme without requiring a trusted dealer or combiner. Thus, both schemes are practical in modularized secure multi-party protocols.

In the presented proofs, the efficiency of reduction (Bellare and Rogaway, 1996) of both schemes is omitted. In general, the application of the forking lemma (Pointcheval and Stern, 2000) in a security proof decreases the 'exactness of security' being proven for the target scheme. Nonetheless, the proofs presented above still provide a lower bound for the security of the proposed scheme and provide direction for further extensions and applications of the proposed schemes.

References

Abe, M., Suzuki, K., 2002. M+1-st price auction using homomorphic encryption. *LNCS*, **2274**:115-124. [doi:10.1007/3-540-45664-3_8]

Baudron, O., Fouque, P., Pointcheval, D., Stern, J., Poupard, G., 2001. Practical Multi-Candidate Election System. ACM 20th Symp. on Principle of Distributed Computing, p.274-283. [doi:10.1145/383962.384044]

Bellare, M., Rogaway, P., 1996. The exact security of digital signatures—how to sign with RSA and Rabin. *LNCS*, **1070**:399-416. [doi:10.1007/3-540-68339-9_34]

Boldyreva, A., Palacio, A., Warinschi, B., 2003. Secure Proxy Signature Schemes for Delegation of Signing Rights. Available from http://eprint.iacr.org/2003/096 [Accessed on Jan. 18, 2010].

Chang, Y.C., 2004. Single private information retrieval with logarithmic communication. *LNCS*, **3108**:50-61. [doi:10.1007/b98755]

Chang, Y.F., Chang, C.C., 2007. An RSA-Based (t, n) threshold proxy signature scheme with free-will identities. *Int. J. Inf. Comput. Secur.*, **1**(1/2):201-209. [doi:10.1504/IJICS.2007.012250]

ElGamal, T., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, **IT-31**(4):469-472. [doi:10.1109/TIT.1985.1057074]

Guillou, L.C., Quisquater, J.J., 1988. A 'paradoxical' identity-based signature scheme resulting from zero-knowledge. *LNCS*, **403**:216-231. [doi:10.1007/0-387-34799-2]

Hwang, M.S., Lu, J.L., Lin, I.C., 2003. A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem. *IEEE Trans. Knowl. Data Eng.*, **15**(6):1552-1560. [doi:10.1109/TKDE.2003.1245292]

Javier, H., German, S., 2004. Revisiting fully distributed proxy signature schemes. *LNCS*, **3348**:356-370. [doi:10.1007/b104579]

Jiang, Z.T., Liu, J.W., Wang, Y.M., 2008. Improvement on Paillier-Pointcheval probabilistic public-key encryption scheme. *Comput. Eng.*, **34**(3):38-39.

Li, F., Ma, J., Li, J.H., 2009. Distributed anonymous data perturbation method for privacy-preserving data mining. *J. Zhejiang Univ.-Sci. A*, **10**(7):952-963. [doi:10.1631/jzus.A0820320]

Lu, R., Cao, Z., 2004. A Proxy-Protected Signature Scheme Based on Conic. ACM 3rd Int. Conf. on Information Security, p.22-26. [doi:10.1145/1046290.1046296]

Lu, R.X., Cao, Z.F., Zhu, H.J., 2005. A robust (k,n)+1 threshold proxy signature scheme based on factoring. *Appl. Math. Comput.*, **166**(1):35-45. [doi:10.1016/j.amc.2004.04.104]

Magkos, E., Maragoudakis, M., Chrissikopoulos, V., Gridzalis, S., 2008. Accuracy in privacy-preserving data mining using the paradigm of cryptographic elections. *LNCS*, **5262**:284-299. [doi:10.1007/978-3-540-87471-3_24]

Mambo, M., Usuda, K., Okmamoto, E., 1996. Proxy Signatures for Delegating Signing Operation. Proc. 3rd ACM Conf. on Computer and Communication Security, p.48-57. [doi:10.1145/238168.238185]

Paillier, P., 1999. Public-key cryptosystems based on composite degree residuosity classes. *LNCS*, **1592**:223-238. [doi:10.1007/3-540-48910-X_16]

Pointcheval, D., Stern, J., 2000. Security arguments for digital signatures and blind signatures. *J. Cryptol.*, **13**(3):361-396. [doi:10.1007/s001450010003]

Rivest, R.L., Shamir, A., Adleman, L.M., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, **21**(2):120-126. [doi:10.1145/359340.359342]

Schdult, J.C.N., Matsuura, K., Paterson, K.G., 2008. Proxy signatures secure against proxy key exposure. *LNCS*, **4939**:344-359. [doi:10.1007/978-3-540-78440-1_9]

Schnorr, C.P., 1991. Efficient signature generation by smart card. *J. Cryptol.*, **4**(3):161-174. [doi:10.1007/BF00196725]

Shamir, A., 1979. How to share a secret. *Commun. ACM*, **22**(11):612-613. [doi:10.1145/359168.359176]

Shoup, V., 2000. Practical threshold signatures. *LNCS*, **1807**:207-220. [doi:10.1007/3-540-45539-6]

Shum, K., Wei, V.K., 2002. A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection. 11th IEEE Int. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, p.55-56. [doi:10.1109/ENABL.2002.1029988]

Sun, H.M., Lee, N.Y., Hwang, T., 1999. Threshold proxy signatures. *IEE Proc.-Comput. Dig. Techn.*, **146**(5):259-263. [doi:10.1049/ip-cdt:19990647]

Sun, X., Li, J.H., Yang, S.T., Chen, G.L., 2008. Non-interactive identity-based threshold signature scheme without random oracles. *J. Zhejiang Univ.-Sci. A*, **9**(6):727-736. [doi:10.1631/jzus.A0720028]

Ting, P.Y., Huang, X.W., 2008. An RSA-based (t,n) threshold proxy signature scheme without any trusted combiner. *LNCS*, **5222**:277-284. [doi:10.1007/978-3-540-85886-7_19]

Wang, G., Bao, F., Zhou, J., Deng, R.H., Lin, I.C., 2004. Comments on "A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem". *IEEE Trans. Knowl. Data Eng.*, **16**(10):1309-1311. [doi:10.1109/TKDE.2004.52]

Wang, H.X., Pieprzyk, J., 2003. Efficient one-time proxy signatures. *LNCS*, **2894**:507-522. [doi:10.1007/b94617]

Yi, L., Bai, G., Xiao, G., 2000. Proxy multi-signature scheme: a new type of proxy signature scheme. *Electron. Lett.*, **36**(6):527-528. [doi:10.1049/el:20000422]

Zhang, N., Wang, S., Zhao, W., 2005. A New Scheme on Privacy-Preserving Data Classification. Proc. ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, p.374-383. [doi:10.1145/1081870.1081913]