INFORMATICA, 2003, Vol. 14, No. 2, 155–166

Partially Blind Threshold Signature Based on RSA

Hung-Yu CHIEN
Department of Information Management, NanKai College
NanTou, Taiwan, ROC
e-mail: redfish6@ms45.hinet.net

Jinn-Ke JAN
Institute of Computer Science, National Chung Hsing University
Taichung, Taiwan, ROC

Yuh-Min TSENG
Department of Computer Science and Information Engineering
ChaoYang University of Technology
Taichung, Taiwan, ROC

Received: May 2003

Abstract. A partially blind signature scheme allows the signer to inoculate a non-removable common information into his blind signature. This common information may represent the date or the amount of e-cash. Due to its un-traceablility and partial blindness property, the partially blind signature plays an important role in many e-commerce applications. Based on the RSA scheme, we propose a partially blind threshold signature with low-computational load for the client.

Key words: cryptography, blind signature, e-commerce.

1. Introduction

In 1983, based on RSA, D. Chaum first introduced the blind signature (Chaum, 1983). In a blind signature, the client requests the signer to sign on a blinded data. The client then derives the wanted signature from the signed blind data. When the client finally hands in the message and its signature, the signer is able to verify this signature, but is unable to link this signed message to the previous signing process instance. The blind signature, with this unlinkability (blindness or untraceability), is widely used in many e-commerce protocol or voting protocol designs (Ferguson, 1993; Shamir and Schnorr, 1984; Fan and Lei, 1998; Fan *et al.,* 2000; Coron *et al.*, 1999; Abe and Fujisaki, 1996; Lin and Harn, 1999; Juang *et al.*, 1999).

The blindness property of the blind signature also makes the signer no opportunity to impose some common information on the signature. However, in some applications, a blind signature embedded with some common information is required. For example, the common information may represent the amount of an e-cash or the valid term

of the signature (Ferguson, 1993; Camenisch *et al.*, 1995; Juang *et al.*, 1999). Therefore, Chaum (1983) proposed to sign signatures with different secret keys to represent different-amount e-cashes. This approach will, unfortunately, incur complex key management and, therefore, limits the number of different amounts.

Using RSA, Abe and Fujisaki (1996) proposed a partially blind signature scheme in which the signer can impose the common information, for example- date, on the signature such that the verifier needs the message, the common information and the signature to check the validity of this signature (Abe and Fujisaki, 1996). In their scheme, the bank is clearly notified the common information- the expiration date of an e-cash. With the partially blind signature, the bank assures that the signed e-cash carry the agreed common information- expiration date. With this common information, the bank needs only to keep the still-alive e-cashes in the database to prevent double spending (Chaum, 1983; Fan and Lei, 1998; Abe and Fujisaki, 1996). Those expired e-cashes could be eliminated from the database without any trouble. This *partial blindness* property preserves the un-linkability of the blind signature, but imposes the common information on the signature.

Based on the Rabin scheme (Rabin, 1979), Fan and Lei (1998) proposed their low-computation partially blind signature. Their scheme requires low computational load on the client side. This makes it attractive for the low-computing-power client implementation (such as smart card or mobile phone). Because the Abe-Fujisaki's RSA-based partially blind signature incurs lots of computation on the client side, we (Chien *et al.*, 2001) had proposed a novel RSA-based partially blind signature with low computational load on the client side.

Based on the discrete logarithm problem, Miyazaki, Abe and Sakurai (Miyazaki, 1997) proposed a partially blind signature, and proposed an efficient E-cash system (Miyazaki and Sakurai, 1998) using the partially blind signature. Later, Juang and Lei (1999), based on the discrete logarithm problem, proposed a partially blind (t, n) threshold signature scheme in which any t out of n signers in a group can represent the group to sign the partially blind threshold signature.

In this paper, we shall propose an RSA-based partially blind (t, n) threshold signature in which any t out of n signers in a group can represent the group to sign the partially blind threshold signature and the computational load of the client side is very low, based on Desmedt-Frankel's threshold signature (1991). The proposed scheme only requires several modular additions and multiplications for the client to acquire and to verify the partially blind threshold signature. This feature makes it attractive for the smart-card-based devices implementations. The rest of this paper is organized as follows. Section 2 reviews Desmedt-Frankel's RSA-based threshold signature, and Section 3 presents our partially blind threshold signature scheme. Section 4 examines the security properties. Section 5 examines the performance of our scheme. Finally, the conclusion is given in Section 6.

2. Review of Desmedt-Frankel's Threshold Signature

Based on RSA, Desmedt and Frankel (1991) proposed (t, n) threshold signature schemes in which any t out of n signers in a group can represent the group to sign the threshold

signature. The public key of the RSA scheme is $(e,\ N = p \cdot q)$, where p and q are large strong primes. To apply the Lagrange interpolation to have a threshold scheme, it is not trivial to circumvent the problem of calculating inverses in the exponent while the $\phi(N)$ function and the $\lambda(N)$ function (the Carmichael function) must remain secret to the group members. Now we review Desmedt-Frankel's threshold signature as follows.

Let $A = \{Signer_1, Signer_2, \ldots, Signer_n\}$ be the set of group members, where $Signer_i$ has his identity ID_i and ID_i is odd. *Trusted Authority* (TA) chooses $N = p \cdot q$ as the group's RSA public key, where $p = 2p' + 1$ and $q = 2q' + 1$ are two strong primes, p' and q' are two large primes. Now the Carmichael function $\lambda(N) = 2p'q'$. The group secret key d is chosen at random such that $e \cdot d \equiv 1 \bmod \lambda(N)$ and $\gcd(d, \lambda(N)) = 1$. So d is odd. Now (e, N) is the group public key, and d is the group secret key. To secretly share the group secret key among members, TA has a secret polynomial $f(x)$ of degree $t - 1$, where the coefficients are even and $f(0) = d - 1 \bmod \lambda(N)$. TA computes

$$S_i = \frac{f(ID_i)/2}{\Big(\prod\limits_{\substack{j \in A \\ j \neq i}} (ID_i - ID_j)\Big)/2} (\bmod p'q'), \quad 1 \leqslant i \leqslant n. \tag{1}$$

Now TA secretly distributes S_i to $Signer_i$, $1 \leqslant i \leqslant n$, as his secret shadow. Then the polynomial $f(x)$ can be reconstructed by the following equation without the calculating of inverse (the correctness of (1), (2) was proved by Desmedt and Frankel (1991)).

$$f(x) = \sum_{i \in B} S_i \prod_{\substack{j \notin B \\ j \in A}} (ID_i - ID_j) \prod_{\substack{j \in B \\ j \neq i}} (x - ID_j) (\bmod 2p'q'). \tag{2}$$

Let B with $|B| = t$ and $B \subset A$ be the set of members who co-operate to sign the threshold signature. Without lose of generality, we assume $B = \{Signer_1, Signer_2, \ldots, Signer_t\}$. Now the members of B execute the following calculations to have the threshold signature on message m (m is a redundancy-contained message).

1. For each $Signer_i \in B$ computes $q_{i,B} = \prod\limits_{\substack{j \notin B \\ j \in A}} (ID_i - ID_j) \prod\limits_{\substack{j \in B \\ j \neq i}} (0 - ID_j)$ and $s_{i,B} = S_i \cdot q_{i,B}$ (please notice that $\sum\limits_{i \in B} s_{i,B} = d - 1 \bmod \lambda(N)$).
2. For each $Signer_i \in B$ signs the message by computing $Sig_{i,B,m} = m^{s_{i,B}} \bmod N$. Each $Signer_i$ submits his partial signature $Sig_{i,B,m}$ to a combiner (who could be one of the members). Then, the combiner computes $Sig_m = m \cdot \prod\limits_{i \in B} Sig_{i,B,m}$ as the group threshold signature.

3. Partially Blind Threshold Signature

Based on Desmedt-Frankel's threshold signature, we propose a partially blind threshold signature in which the computational load of the client is low. In a partially blind threshold signature scheme, the client would request a partially blind threshold signature from

a group (which may be a company or a joint issuer consists of several banks). Firstly, the client prepares a blinded data and the common information, and sends the data to the group. If the group agrees on this common information, then they sign the blinded data with the common information imposed on the signature, using the threshold signature introduced in Section 2. The client, then, derives the signature from the signed message without being able to remove or change the imposed common information. To successfully verify the signature, the signature holder should hand in the message, the signature and also the agreed common information. So the agreed common information would be genuinely shared among the client, the group and the verifiers. This common information could represent the date or the amount of an e-cash, depending on its applications (Chaum, 1983; Fan and Lei, 1998; Abe and Fujisaki, 1996; Juang *et al.*, 1999).

Our scheme consists of four phases: (1) initialization, (2) requesting, (3) signing, and (4) extraction and verification. TA publishes the necessary information and secretly distributes the shadow S_i to the group members in the initialization phase. In the requesting phase, the client prepares the common information and the blinded data, using some blind factors and the message. The group, then, signs the blinded data with the common information imposed on it. Finally, the client derives the signature from the signed data, and verifies the signature in the extraction and verification phase. We now describe our scheme as follows.

(1) Initialization. TA sets up the system parameters as in Section 2, but $e = 3$ and $\gcd(e, \lambda(N)) = 1$. TA publishes (e, N) as the group public key, and secretly issues S_i to the group member $Signer_i$, where the group is represented by $A = \{Signer_1, Signer_2, \ldots, Signer_n\}$. TA also publishes a secure one-way hash function such as SHA-1 or MD5 (Menezes *et al.*, 1997). *Let $h(\,)$ denotes the one-way hash function, and $h(m)$ denotes the hash value on the message m. Z_N^* denotes the set of positive integers that are smaller than N and co-prime to N. That is, $Z_N^* = \{x | 1 \leqslant x \leqslant N, \gcd(x, N) = 1\}$.*

(2) Requesting. The client prepares the message m and the common information a, according to the predefined format. He also randomly chooses three numbers r, r' and u, where r, r' and $u \in Z_N^*$. The client, then, computes $\alpha = (r^3 r')^e h(m)(u^2 + 1) \bmod N$, and sends the pair (a, α) to the group A.

Assume $B = \{Signer_1, Signer_2, \ldots, Signer_t\} \subset A$ be the set of members of the group who co-operate to sign the threshold signature. After verifying the common information a, the group B randomly chooses a positive integer x less than N and sends it to the client.

Upon receiving x, the client lets $b = r \bmod N$. Finally, he computes $\beta = b^e(u - x) \bmod N$, and sends β to the signers.

(3) Signing. Now the group B computes $\beta^{-1} \bmod N$, and runs the threshold signature introduced in Section 2 to have $T = h(a)^{d-1}(\alpha(x^2 + 1)\beta^{-2})^{2(d-1)} \bmod N$, and then submits (β^{-1}, T) to the client. *Please notice the probability that β has common factor with N and has no inverse is negligible; otherwise, the RSA scheme is not computationally secure.*

(4) Extraction and verification. Upon receiving (β^{-1}, T), the client derives the signature by computing

$$c = (ux+1)\cdot\beta^{-1}\cdot b^e = (ux+1)(u-x)^{-1} \bmod N,$$

and

$$s = T\cdot h(a)\cdot h(m)^2\cdot r^{2e-2}\cdot r'^{(2e-2)}\cdot(c^2+1)^2 \bmod N.$$

The tuple (a, c, s) is a threshold signature on the message m. Any one can verify this signature by checking if

$$s^e \equiv h(a)h(m)^2(c^2+1)^2 \bmod N. \tag{3}$$

Now we show the correctness of the proposed protocol by proving that the signature (a, c, s) of the message m produced by the proposed protocol satisfies $s^e \equiv h(a)h(m)^2(c^2+1)^2 \bmod n$.

Theorem 1. *If (a, c, s) is a threshold signature of the message m produced by the proposed partially blind threshold signature scheme, then*

$$s^e \equiv h(a)h(m)^2(c^2+1)^2 \bmod n.$$

Proof. If (a, c, s) is a signature generated by our scheme, then we have the following equations.

$$\begin{aligned}
s &\equiv T\cdot h(a)\cdot h(m)^2\cdot r^{2e-2}\cdot r'^{(2e-2)}\cdot(c^2+1)^2\\
&\equiv h(a)^{d-1}\left[r^{3e}\cdot r'^{e}\cdot h(m)\cdot(u^2+1)(x^2+1)\beta^{-2}\right]^{2(d-1)}\\
&\quad\times h(a)\cdot h(m)^2\cdot r^{2e-2}\cdot r'^{(2e-2)}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}\left[r^{3e}\cdot r'^{e}\cdot(u^2+1)(x^2+1)\cdot r^{-2e}\cdot(u-x)^{-2}\right]^{2(d-1)}\\
&\quad\times r^{2e-2}\cdot r'^{2e-2}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}\left[(u^2x^2+u^2+x^2+1)\cdot(u-x)^{-2}\cdot r^{e}\cdot r'^{e}\right]^{2(d-1)}\\
&\quad\times r^{2e-2}\cdot r'^{2e-2}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}\left[\left((ux+1)^2+(u-x)^2\right)\cdot(u-x)^{-2}\cdot r^{e}\cdot r'^{e}\right]^{2(d-1)}\\
&\quad\times r^{2e-2}\cdot r'^{2e-2}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}\left[(c^2+1)\cdot r^{e}\cdot r'^{e}\right]^{2(d-1)}\cdot r^{2e-2}\cdot r'^{2e-2}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}(c^2+1)^{2(d-1)}\cdot r^{2-2e}\cdot r'^{(2-2e)}\cdot r^{2e-2}\cdot r'^{2e-2}\cdot(c^2+1)^2\\
&\equiv h(a)^{d}\cdot h(m)^{2d}\cdot(c^2+1)^{2d} \bmod N.
\end{aligned}$$

So, we have $s^e = h(a)\cdot h(m)^2\cdot(c^2+1)^2 \bmod N$, and the proposed protocol provides a partially blind threshold signature scheme. The common information a could represent

the expired date of an e-cash, the amount of an e-cash, or the value amount of an anonymous ticket used in wireless communication, depending on its applications. It could even contain the information for both the value of a ticket and its expired date. If the common information a is used as an expired date of an e-cash, then the tuple (a, c, s, m) represents an anonymous e-cash issued by the banks (signers), where (a, c, s) is a threshold signature of the message m produced by our partially blind threshold signature scheme. Since the signature carries the expired date information, the banks need only keep those un-expired e-cashes in their database to prevent the double-spending. Those expired e-cashes could be removed from the database without any trouble (Fan and Lei, 1998; Abe and Fujisaki, 1996). If the common information a represents the value for an anonymous ticket used in anonymous wireless communication (Juang *et al.*, 1999), then the tuple (a, c, s, m) represents a value-carried anonymous ticket issued by the service providers. Thus, the clients can purchase different anonymous tickets with distinct values, and their service providers will deducts different money accordingly (Juang *et al.*, 1999).

4. Security Analysis

In this section, we discuss some security properties of our proposed scheme. The threshold rule is enforced by applying the Desmedt-Frankel's threshold signature scheme. The other properties are examined as follows.

4.1. *Randomization*

In our scheme, the group (the signers) randomizes the blinded data using the random factor x before signing it in the signing phase. This *randomization property* (Ferguson, 1993) keeps the blind signature scheme away from some chosen-plain-text attacks (Shamir and Schnorr, 1984, Fan and Lei, 1998; Fan *et al.*, 2000; Coron *et al.*, 1999). Our scheme and the blind signature schemes of literatures (Ferguson, 1993; Fan and Lei, 1998; Fan *et al.*, 2000; Camenisch *et al.*, 1995; Pointcheval and Stern, 1996; Chien *et al.*, 2001) have this randomization property, while the blind signature schemes of Chaum (1983); Abe and Fujisaki (1996) do not possess the randomization property.

In the requesting phase, the client submits a and α to the signers, and then the signers return the random factor x to the client. If the client tries to get rid of this random factor x and derives the value T, he has to compute β' such that $\beta'^2 \equiv (x^2 + 1) \bmod N$ in the requesting phase. However, given x and N, it is computationally infeasible to compute the β' without factoring N, which is believed to be a very hard problem (Rabin, 1979).

4.2. *Partial Blindness*

In our partially blind threshold signature scheme, the client has to submit the common information a and the value α to the signers. If the signers agree on this common information a, they sign on the prepared data with the common information embedded. The client

is unable to remove or change the embedded information a while keeping the verification of the signature successful.

To successfully remove or change the common information a embedded in the signature, the client has to compute either α' or β' , and includes them in the submitted values such that they satisfy $\alpha'^2 \equiv h(a)^{-1} \bmod N$ or $\beta'^4 \equiv h(a) \bmod N$. However, it is computationally infeasible to acquire such an α' or β' without factoring N.

4.3. *Unforgability*

The attacker may try to derive some forged signatures with or without some valid signatures. We will show that all of the attacks fail on our scheme. First, we consider the attacks with no given valid signatures. To successfully pass the verification equation $s^e \equiv h(a)h(m)^2(c^2+1)^2 \bmod N$, the attacker has to compute s such that $s \equiv h(a)^d h(m)^{2d}(c^2+1)^{2d} \bmod N$, given the values $h(a), h(m)$ and c. However, it is computationally infeasible to acquire the value d without the factorization of N. On the other hand, given $s, h(a)$ and $h(m)$, it is intractable to compute c such that $c^2 \equiv (s^e \cdot h(a)^{-1} \cdot h(m)^{-2})^{1/2} - 1 \bmod N$ without the factorization of N.

Given a valid signature (a, c, s, m), we will show that the attacker has no way to derive another valid signature (a', c', s') for another m' with $h(m) \neq h(m') \bmod N$. Given the values a and c, he is unable to acquire the value s' such that $s' \equiv s \cdot h(m)^{-2d} h(m')^{2d} \bmod N$ without knowing d. Without the factorization of N, it is intractable to compute c' such that $c'^2 \equiv (s^e \cdot h(a)^{-1} \cdot h(m')^{-2})^{1/2} - 1 \bmod N$. It is also difficult to derive another message m' with $m' \neq m \bmod N$ such that $h(m) \equiv h(m') \bmod N$, since $h()$ is a secure one-way hash function.

Given pairs of valid signatures (a, c_1, s_1, m_1) and (a, c_2, s_2, m_2), then we have $(s_1 s_2)^e \equiv h(a)^2 h(m_1)^2 h(m_2)^2 (c_1^2+1)^2 (c_2^2+1)^2 \bmod N$. If the attacker lets $s_3 \equiv s_1 s_2 \bmod N$ and tries to derive the valid c_3, then he has to compute $c_3^2 \equiv (h(a)h(m_1)^2 h(m_2)^2 h(m_3)^{-2}(c_1^2+1)^2(c_2^2+1)^2)^{1/2} - 1 \bmod N$. However, without the factorization of N, it is computationally infeasible to acquire such a c_3.

4.4. *Unlinkability*

For any given valid signature (a, c, s, m), no one except the client is able to link this signature to its previous signing process instance. This is the *unlinkability* property of a blind signature. We will show that our partially blind threshold signature preserves this property in the following theorem.

Theorem 2. *For any given signature (a, c, s, m) and each signing process instance of the past signing processes, which are represented by the tuple $(a, \alpha_i, x_i, \beta_i, T_i)_{1 \leqslant i \leqslant k}$, the signers can derive b_i, r_i' and u_i such that they satisfy the following equations.*

$$\alpha_i = (b_i^3 \cdot r_i')^e h(m)(u_i^2+1) \bmod N, \tag{4}$$

$$\beta_i = b_i^e (u_i - x_i) \bmod N, \tag{5}$$

$$c = (u_i x_i + 1)(u_i - x_i)^{-1} \bmod N. \tag{6}$$

Proof. From (6), we derive

$$u_i \equiv (cx_i + 1)(c - x_i)^{-1} \bmod N. \tag{7}$$

Substituting (7) into (5), then we have

$$\beta_i = b_i^e((cx_i + 1)(c - x_i)^{-1} - x_i) \bmod N,$$

and then

$$b_i \equiv \beta_i^d \cdot ((cx_i + 1)(c - x_i)^{-1} - x_i)^{-d} \bmod N. \tag{8}$$

Substituting (7)–(8) into (4), we have

$$\begin{aligned}\alpha_i &= (b_i^3 \cdot r_i')^e \cdot h(m)\left((cx_i + 1)^2(c - x_i)^{-2} + 1\right) \\ &= b_i^{3e} \cdot r_i'^e \cdot h(m) \cdot \left((cx_i + 1)^2(c - x_i)^{-2} + 1\right) \bmod N,\end{aligned}$$

and then

$$r_i' \equiv \alpha_i^d \cdot b_i^{-3} \cdot h(m)^{-d} \cdot \left((cx_i + 1)^2(c - x_i)^{-2} + 1\right)^{-d} \bmod N. \tag{9}$$

From (7)–(9), we conclude that for any given signature (a, c, s, m) and each signing process instance with the common information a, the group (the signers) can find the values (b_i, r_i', u_i) that satisfy (4)–(6). This implies that the signers are unable to find the link between the signature and its corresponding signing process instance.

4.5. *Immunity to Low-Exponent RSA Protocol Failure*

Since the low-exponent RSA is adopted in our scheme, we have to examine the possibility of the low-exponent RSA attacks. There are some known attacks to low-exponent RSA (Moore, 1988; Hastad, 1985). The first known attack is: if the same message is encrypted with the same low exponent for several different modulus, then the message could be easily recovered from the cipher texts. Take $e = 3$ as an example. Suppose *User*$_1$ decides to send the same message M to *User*$_2$, *User*$_3$, and *User*$_4$. The cipher texts are as follows.

$$\begin{aligned}C_2 &= M^3 \bmod n_2, \\ C_3 &= M^3 \bmod n_3, \\ C_4 &= M^3 \bmod n_4.\end{aligned}$$

Then the attacker can easily recover the message M from the cipher texts (Moore, 1988). Hastad further showed that even several messages with low-entropy difference are transmitted to different receivers using low-exponent RSA, it is easy for the attacker to recover the message (Hastad, 1985). We can easily see that such kind of attacks do

not work on our scheme due the following reasons. For the applications of our scheme, the message m should contain some random number (Juang *et al.*, 1999). Further, each message transmitted from the client to the signers will be randomized by some random factors. So, our scheme is immune to the low-exponent attacks.

5. Computation Complexity

For a comparison of the performance of different schemes, we adopt the same assumptions as (Fan and Lei, 1998; Dimitrov and Cooklev, 1995). With a modulus N, the computation for a modular exponentiation operation is taken as $0.3246\,|N|$ modular multiplications, where $|N|$ denotes the bit length of N. An inverse computation in Z_N^* demands the same amount of computation time as a modular exponentiation operation. A hashing computation requires no longer time than a modular multiplication computation. *In the following comparisons, let T_e denote the time for one exponentiation computation, T_i the time for one inverse computation, T_m the time for one modular multiplication computation, and T_h the time for one hashing computation. Under a 1024-bit modulus N, one T_e is around 330* T_m.*

For many of the applications of the blind signature schemes, the requesters (the clients) are the smart cards or mobile units; therefore, the computation complexity on the client side deserves special concern. For most of the previous blind signature schemes (Chaum, 1983; Ferguson, 1993; Abe and Fujisaki, 1996; Camenisch *et al.*, 1995; Pointcheval and Stern, 1996; Miyazaki *et al.*, 1997; Juang and Lei, 1999), several modular exponentiation computations and inverse computations are required on the client side. *Based on RSA, Abe-Fujisaki's partially blind signature scheme requires $2T_e + 1T_i + 4T_h + 4T_m$ on the client side. However, based on Rabin's scheme, Fan-Lei's partially blind signature demands only $20T_m + 3T_h$ on the client side. Fan-Lei's scheme reduces the amount of computation time on the client side by almost 98% (Fan and Lei, 1998), under a 1024-bit modulus N. Our previous work (a partially blind signature scheme) (Chien et al., 2001), based on RSA, demands $21T_m + 2T_h$ on the client side. Compared with Abe-Fujisaki's scheme, our previous partially blind signature reduces the amount of computations by almost 98%, under a 1024-bit modulus N.*

Regarding the case of partially blind threshold signature, our current scheme requires $27T_m + 2T_h$ on the client side. Juang-Lei's partially blind threshold signature is based on the discrete logarithm problem. Juang-Lei's scheme requires $(2n + 10)T_e + (2t - 1)T_i + (4n + t + 3)T_m + 2T_h$, where n the group size and t is the threshold value. Compared to Juang-Lei's partially blind threshold signature scheme, our scheme reduces the amount of computations by almost 99.6%, under a 1024-bit modulus N, $n = 5$ and $t = 3$. With $n = 10$ and $t = 5$, our scheme reduces the computations by almost 99.88%.

We summarize the computation complexity of the client and other properties for the partially blind signature schemes in Table 1.

Table 1
Summaries for the partially blind signature schemes

	Fan-Lei's partially blind sig.	Abe-Fujisaki's partially blind sig.	Chien-Jan-Tseng's partially blind sig.	Juang-Lei's partially blind threshold sig.	Chien-Jan-Tseng's partially blind threshold sig.
Mathematical foundation	QR	RSA	RSA	Discrete Logarithm (Elgamal)	RSA
Randomization property	Yes	No	Yes	Yes	Yes
Computations for the client	$20T_m+3T_h$	$2T_e + 1T_i +4T_h+4T_m$	$21T_m+2T_h$	$(2n+10)T_e + (2t-1)T_i + (4n+t+3) \times T_m + 2T_h$	$27T_m+2T_h$

T_e – time for one exponentiation computation; T_i – time for one inverse computation; T_m – time for one modular multiplication computation; T_h – time for one hashing computation.

6. Conclusions

In this paper, based on RSA, we have proposed a partially blind threshold signature scheme. Without modular exponentiation computations and inverse computations, our scheme requires much less computational load on the client side, compared with its counterpart *(Juang-Lei's partially blind theshold signature scheme)*. This low-computation property makes our scheme very attractive in many e-commerce applications.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments. This research is partially supported by National Science Council with project number NSC91-2626-E-252-002.

References

Abe, M., and E. Fujisaki (1996). How to date blind signatures. In *Advances in Cryptology-ASIACRYPT'96, LNCS*, **1163**. Springer–Verlag. pp. 224–251.

Camenisch, J.L., J.M. Pivereau and M.A. Stadler (1995). Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology-EUROCRYPT'94, LNCS*, **950**. Springer–Verlag. pp. 428–432.

Chaum, D. (1983). Blind signatures systems. In *Advances in Cryptology-CRYPTO'83, Plenum*. Springer–Verlag.

Chien, H.Y., J.K. Jan and Y.M. Tseng (2001). RSA-based partially blind signature with low computation. In *Proceedings of the Eighth International Conference on Parallel and Distributed Systems (ICPADS 2001)*. KyonJu, Korea. pp. 385–389.

Coron, J.S., D. Naccache and J.P. Stern (1999). On the security of RSA padding. In *Advances in Cryptology-Crypto'99, LNCS*, **1666**. Springer–Verlag. pp. 1–18.

Desmedt, Y., and Frankel (1991). Shared generation of authenticators and signatures. In *Advances in Cryptology-Crypto'91*. Springer–Verlag. pp. 457–469.

Dimitrov, V., and T. Cooklev (1995). Two algorithms for modular exponentiation using nonstandard arithmetic. *IEICE Trans. Fundamentals*, **E78-A**(1), 82–87.

Fan, C.I., and C.L. Lei (1998). Low-computation partially blind signatures for electronic cash. *IEICE Trans. Fundamentals*, **E-81-A**(5), 818–824.

Fan, C.I., W.K. Chen and Y.S. Yeh (2000). Randomization enhanced Chaum's blind signature scheme. *Computer Communications*, **23**, 1677–1680.

Ferguson, N. (1993). Single term off-line coins. In *Advances in Cryptology-EUROCRYPT'93, LNCS*, **765**. Springer–Verlag. pp. 318–328.

Juang, W.S., and C.L. Lei (1999). Partially blind threshold signatures based on discrete logarithm. *Computer Communications*, **22**, 73–86.

Juang, W.S., C.L. Lei and C.Y. Chang (1999). Anonymous channel and authentication in wireless communications. *Computer Communications*, **22**, 1502–1511.

Hastad, J. (1985). On using RSA with low exponent in a public key network. In *Advances in Cryptography-Crypto'85*. pp. 403–408.

Lin, H.Y., and L. Harn (1999). Authentication protocols with non-repudiation services in personal communication system. *IEEE Communications Letters*, **3**(8), 236–238.

Menezes, A., P.V. Oorschot and S. Vanstone (1997). *Handbook of Applied Cryptography*. CRC Press.

Miyazaki, S., M. Abe and K. Sakurai (1997). Partially blind signature schemes for the DSS and for a discrete log. based message recovery signature. In *Proceedings of the 1997 Korea-Japan Joint Workshop on Information Security and Cryptology*. pp. 217–226.

Miyazaki, S., and K. Sakurai (1998). *A more Efficient Untraceable E-Cash System with Partially Blind Signature Based on the Discrete Logarithm Problem*. Dept. of Computer Science, Kyushu Univ. Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan, 296–307.

Moore, J.H. (1988). Protocol failures in cryptosystems. In *Proceedings of the IEEE*, **76**(5).

Pointcheval, D., and J. Stern (1996). Provably secure blind signature schemes. *Advances in Cryptology-ASIACRYPT'96, LNCS*, **1163**. Springer–Verlag. pp. 252–265.

Rabin, M.O. (1979). *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*. Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass.

Shamir, A., and C.P. Schnorr (1984). Cryptanalysis of certain variants of Rabin' signature scheme. *Information Processing Letters*, **19**, 113–115.

Y.-M. Tseng received the BS degree in computer science and engineering from National Chiao Tung University, Taiwan, Republic of China, in 1988; and the MS degree in computer and information engineering from National Taiwan University in 1990, and the PhD in applied mathematics from National Chung Hsing University in 1999. He is currently an associate professor and the chairman of the Department of Information Management, Nan-Kai College, Taiwan. He is a member of the Chinese Association for Information Security (CCISA). His research interests include cryptography, mobile communication security, network security, and image encryption.

J.-K. Jan was born in Taiwan in 1951. He received the BS degree in physics from Catholic Fu Jen University, Taiwan, Republic of China, in 1974 and the MS degree in information and computer science from Tokyo University in 1980. He studied software engineering and human-computer interface at the University of Maryland, College Park, MD, during 1984–1986. He is presently a professor of the Department of Applied Mathematics at National Chung Hsing University, Taiwan. He is currently also the editor of Information and Education, and an executive member of the Chinese Association for Information Security. His research interests include computer cryptography, network security, human factors of designing software and information systems, database security, and coding theory.

H.-Y. Chien received the BS degree in computer science from National Chiao Tung University, Hsinchu, Taiwan, in 1988 and the MS degree in computer and information engineering from National Taiwan University, Taipei, Taiwan, in 1990. He is currently pursuing his doctoral degree in applied mathematics at National Chung Hsing University. He is a member of the Chinese Association for Information Security. His research interests include cryptography, network security, electronic commerce.

Dalinai aklasis slenkstinis RSA parašas

Hung-Yu CHIEN, Jinn-Ke JAN, Yuh-Min TSENG

Aklojo parašo schemoje klientas paprašo dokumentą pasirašantį asmenį pasirašyti paslėptus duomenis, o po to iš jų gali gauti parašą. Kada klientas pateikia pasirašytą dokumentą, pasirašęs dokumentą asmuo gali jo parašą patikrinti. Aklasis parašas labai svarbus elektoninėje prekyboje. Straipsnyje pasiūlytas nesudėtingas dalinai aklasis slenkstinis RSA parašas.