DOI: 10.1007/s11432-006-2013-7

Provably secure robust threshold partial blind signature

CAO Zhenfu, ZHU Haojin & LU Rongxing

Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, China
Correspondence should be addressed to Cao Zhenfu (email: cao-zf@cs.sjtu.edu.cn)
Received May 24, 2005; accepted October 12, 2005

Abstract Threshold digital signature and blind signature are playing important roles in cryptography as well as in practical applications such as e-cash and e-voting systems. Over the past few years, many cryptographic researchers have made considerable headway in this field. However, to our knowledge, most of existing threshold blind signature schemes are based on the discrete logarithm problem. In this paper, we propose a new robust threshold partial blind signature scheme based on improved RSA cryptosystem. This scheme is the first threshold partial blind signature scheme based on factoring, and the robustness of threshold partial blind signature is also introduced. Moreover, in practical application, the proposed scheme will be especially suitable for blind signature-based voting systems with multiple administrators and secure electronic cash systems to prevent their abuse.

Keywords: threshold signature, blind signature, improved RSA cryptosystem, factoring problem, electronic cash.

1 Introduction

The concept of the blind signature scheme was first introduced by Chaum[1]. Generally speaking, there are two entities in a blind signature scheme, namely the requester and the signer. The requester requests the signer to make a signature on a blind data and derives the signed message from the signed blind data. Then, after the requester finally opens the message and its signature, the signer can verify this signature but unable to link this signed message to the previous signing process instance. Because of its anonymity, the blind signature has been widely used to realize a lot of cryptographic protocols such as secure voting protocol and electronic payment systems[2,3].

Due to the characteristics of electronics, e-cash can be easily duplicated. Hence, to prevent a customer from double-spending his e-cash, the bank has to keep a database which stores all spent e-cash to check whether a specified e-cash has been spent by searching this database. Obviously, without special measures, the database kept by the

bank may grow unlimitedly. This special measure is referred to as the partial blind signature

The notion of partial blind signature was introduced by Abe and Fujisaki[4] in 1996 and formalized by Abe and Okamoto[5] in 2000. The most preponderant advantage of a partial blind signature is that signer can ensure that each signature can contain some common information, which cannot be removed or changed. Because of its excellent characteristics, the technique of partial blind signature makes it possible to prevent the bank's database from growing unlimitedly since the bank (or signer, respectively) can insert expiration date into each e-cash (or signature). Any expired e-cash can be removed from the database periodically.

On the other hand, the voting system or electronic payment system based on blind signature scheme are usually managed by a single administrator, who is always empowered to authorize votes or sign the message. But, a dishonest administrator can abuse this power to cast fraudulent votes for his own sake. To prevent this abuse by a single administrator, we need more than one administrators using threshold signature scheme[6−10] to sign a message. For this request, the threshold blind signature scheme was introduced by Juang and Lei[11]. In their scheme, the power of a single administrator can be distributed to n administrators and any $t(t < n)$ out of n administrators can generate a signature for a given message, but any $t - 1$ or less cannot generate a valid signature.

After Juang and Lei[11] initially proposed (t, n) threshold blind signature scheme, Juang, Lei and Yu[12] also presented a provably secure threshold blind signature scheme based on Okamoto-Schnorr blind signature technique[13,14]. And Kim *et al.*[15] also put forth an efficient and provably secure threshold blind signature scheme, which was claimed more efficient and more secure compared with the former schemes[11,12]. More recently, Vo *et al.*[16] proposed a new threshold blind signature from bilinear parings. However, the existing threshold bind signature schemes[15−17] most are based on the discrete logarithm problems. Therefore, people hope to design threshold blind signature schemes based on other problems, such as factoring problem.

In this paper, we propose a new threshold partial blind signature scheme based on improved RSA cryptosystem[18]. Since the improved RSA cryptosystem[18] is equivalent to factoring problem, the security of our proposed scheme also is relative to the factoring problem.

In addition, in ref. [19], the first author firstly introduced the definition of robust threshold key escrow scheme (RTKES). In an RTKES, malice escrow agency fail to obtain the system secret key or user's secret key, even if the number of malice escrow agency is more than or equal to the value of threshold. Therefore, to meet some special requirements, the notion of robust threshold also can be clearly applied to the threshold blind signature schemes. Hence, the proposed threshold partial blind signature scheme here will also have the property of robustness.

1.1 Our contributions

This paper gives the definition of robust threshold signature and presents a new

robust partial threshold blind signature scheme based on the factoring problem.

Here the property of robustness in a (t, n) threshold signature means that even if t signers (t is assumed to be the threshold value) ally, they still have no chance to arbitrarily sign on a message, because they only recover the equivalent "key" of the original key and cannot extract the original key from the equivalent "key", which is particularly important in many occasions, especially when the original key has other purposes in the whole system.

To achieve this goal, we add a trusted dealer, assumed to be always trustable, to our system. In addition, we need a key management center (KMC) to publicize the system parameters and distribute the sub secret key and a dealer assigned to resend the intermediate information and sign with his secret key in the scheme. Obviously, with the trusted dealer, the system will enjoy more convenience and more security. For example, in a threshold signature scheme, it is obviously inconvenient for a user to send a message to k signers for signature. Thus, a computer can be used as the trusted dealer to deal with the signing process. In addition, due to his secret key, the dealer will make the scheme more robust.

Naturally, the idea of the robust threshold can also be applied to other discrete-log based threshold signature systems.

1.2 Organization

The rest of the paper is organized as follows: In section 2, we will review the related building technologies, such as improved RSA system, blind improved RSA signature and partial blind improved RSA signature. Then we propose our scheme in section 3. In section 4, we will give the security analysis of the new scheme. Finally, concluding remarks are made in section 5.

2 Preliminaries

2.1 Improved RSA cryptosystem

The improved RSA cryptosystem was introduced in ref. [18]. For convenience, we briefly recall the scheme as follows:

Randomly choose two secure large primes p, q satisfying $p = 2p' + 1$ and $q = 2q' + 1$, where p', q' are also two large primes. Let $N = p \cdot q$. Then the Euler totient function $\phi(N) = (p-1)(q-1)$. Take $a \in_R \mathbb{Z}_{\mathbb{N}}^*$ satisfying Jacobi symbol $\left(\frac{a}{N}\right) = -1$. Then choose $e \in \mathbb{Z}$ with

$$\gcd\left(e, \frac{1}{4}\phi(N)\right) = 1, 1 < e < \frac{1}{4}\phi(N).$$

And then compute $d \in \mathbb{Z}$, such that

$$ed \equiv \frac{1}{2}\left(\frac{1}{4}\phi(N) + 1\right) \bmod \frac{1}{4}\phi(N), 1 < d < \frac{1}{4}\phi(N).$$

The public key is (a, e, N), and the private key is d.

Encryption. Suppose that plaintext $x \in \mathbb{Z}_N, \gcd(x, N) = 1$. Then

$$E(x) = \begin{cases} x^{2e} \bmod N, & \text{if } \left(\dfrac{x}{N}\right) = 1; \\ (ax)^{2e} \bmod N, & \text{if } \left(\dfrac{x}{N}\right) = -1. \end{cases}$$

So, the ciphertext is $(E(x), c_1, c_2)$ where

$$c_1 = \begin{cases} 0, & x > \dfrac{N}{2}, \\ 1, & x < \dfrac{N}{2}, \end{cases} \quad c_2 = \begin{cases} 0, & \text{if } \left(\dfrac{x}{N}\right) = 1, \\ 1, & \text{if } \left(\dfrac{x}{N}\right) = -1. \end{cases}$$

Decryption. If $c_2 = 0$, then $x^{2e} \equiv E(x) \pmod N$. Compute

$$E(x)^d \equiv x^{2ed} \equiv x^{1+\frac{1}{4}\phi(N)} \equiv \pm x \pmod N.$$

Then, plaintext x can be obtained from identifier digit c_1.

If $c_2 = 1$, then $(ax)^{2e} \equiv E(x) \pmod N$. Compute

$$E(x)^d \equiv (ax)^{2ed} \equiv (ax)^{1+\frac{1}{4}\phi(N)} \equiv \pm ax \pmod N.$$

That is, $x \equiv \pm a^{-1}(E(x))^d \pmod N$. Then from the identifier digit c_1, the plaintext x can be obtained.

How to prove or disprove that breaking the conventional RSA system is as hard as factoring is still an open problem. In ref. [20], Boneh and Venkatesan have provided evidence that breaking low-exponent RSA cannot be equivalent to factoring integers, while the improved RSA cryptosystem here has been proved based on factorization of a large integer (refer to refs. [18, 19, 21]) for the detailed security proof.) Therefore, the improved RSA scheme will be more secure than the original one[22]. Of course, in order to improve the security in the practical application, Optimal Asymmetric Encryption Padding (OAEP) technique[23] should be applied to the improved RSA primitive. For the multi-dimension RSA please refer to refs. [24, 25].

2.2 Improved RSA signature

Assume that A is a signer who chooses a universal hash function $H_0 : \{0,1\}^* \to \mathbb{Z}_{\mathbb{N}}^*$ in the system. The public key of A is (a, e, N, H_0), and the private key is d as above[1)]. Then, the improved RSA signature is described as follows:

Signing. Suppose that $m \in \{0,1\}^*$ is the message to be signed. A first computes $H_0(m)$, and then computes $c_1 \in \{0,1\}$ and σ, where

$$\left(\frac{H_0(m)}{N}\right) = (-1)^{c_1}, \quad \sigma = (a^{c_1} H_0(m))^{2d} \bmod N.$$

The signature on message m is (c_1, σ).

Verification. Check whether the following equality holds:

$$\sigma^e = \pm a^{c_1} H_0(m) \bmod N.$$

If the equality holds, the signature will be accepted, otherwise rejected,

$$\sigma^e = (a^{c_1} H_0(m))^{2ed} = (a^{c_1} H_0(m))^{\frac{1}{4}\phi(N)+1} = \pm a^{c_1} H_0(m) \bmod N.$$

1) Here, when $e = 1$, it is the improved Rabin signature scheme. See ref. [26] for more details.

2.3 Blind improved RSA signature

Suppose that A is the signer and B is the requester in the system. The public key of A is (a, e, N, H_0), and the corresponding private key is d as above.

Now assume that B wants to get A's blind signature on message m. Then the two-party protocol is as follows:

1. The requester B first computes $c_1 \in \{0, 1\}$ such that $\left(\frac{H_0(m)}{N}\right) = (-1)^{c_1}$, which can ensure the Jacobi symbol $\left(\frac{a^{c_1} H_0(m)}{N}\right) = 1$. Let $m' = a^{c_1} H_0(m) \bmod N$ be the new message to be signed. Choose the blind factor $b \in \mathbb{Z}_{\mathbb{N}}$, satisfying $\left(\frac{b}{N}\right) = 1$. B then computes and sends $M = b^e m' \bmod N$ to the signer A.

2. On receiving the message M, A first checks $\left(\frac{M}{N}\right) = 1$. If it holds, A computes $sig = M^{2d} = (b^e m')^{2d} \equiv \pm b m'^{2d} \bmod N$ and sends sig to the requester B. Otherwise, A terminates.

3. B computes $sign(m) = sig/b = \pm m'^{2d} \bmod N$. Obviously, $(m, sign(m), c_1)$ is a valid signature on m.

4. Later, anyone can verify the signature by checking the following equality

$$(sign(m))^e = \pm m'^{2ed} = \pm m'^{1+\frac{1}{4}\phi(N)} = \pm a^{c_1} H_0(m) \bmod N.$$

2.4 Partial blind improved RSA signature

Suppose that A is the signer and B is the requester in the system. The public key of A is (a, e, N, H_0), and the corresponding private key is $(d, \phi(N))$ as above. In addition, let F be a universal hash function satisfying $F(x) \equiv 1 \bmod 2$ for any x.

Now, assume that the requester B wants to get the signer A's blind signature on message m. They first agree on a common information $info$ in a predetermined way. We set $v = F(info)$. Then, they execute the issuing protocol as follows:

1. The requester B first computes $c_1 \in \{0, 1\}$ such that $\left(\frac{H_0(m)}{N}\right) = (-1)^{c_1}$, which can ensure the Jacobi symbol $\left(\frac{a^{c_1} H_0(m)}{N}\right) = 1$. Let $m' = a^{c_1} H_0(m) \bmod N$ be the new message to be signed. Choose the blind factor $b \in \mathbb{Z}_{\mathbb{N}}$, satisfying $\left(\frac{b}{N}\right) = 1$. B then computes and sends $M = b^{ev} m' \bmod N$ to the signer A.

2. After A receives the message M, A first checks $\left(\frac{M}{N}\right) = 1$. If it does not hold, he terminates. Otherwise, he computes v^{-1} such that $v \cdot v^{-1} \equiv 1 \bmod \frac{1}{4}\phi(N)$. Then he computes $sig = M^{2dv^{-1}} = (b^{ev} m')^{2dv^{-1}} = \pm b m'^{2dv^{-1}} \bmod N$ and sends sig to B.

3. B computes $sign(m) = sig/b = \pm m'^{2dv^{-1}} \bmod N$. Obviously, $(m, sign(m), c_1)$ is a valid signature on m.

4. One can verify the signature by checking the following equality:

$$(sign(m))^{ev} = \pm a^{c_1} H_0(m) \bmod N.$$

If the equality holds, the signature will be accepted, otherwise rejected,

$$(sign(m))^{ev} = \pm m'^{2ed} = \pm m'^{1+\frac{1}{4}\phi(N)} = \pm a^{c_1} H_0(m) \bmod N.$$

2.5 Discrete logarithm equality protocol

In 2000, Shoup[9] proposed a well-known discrete logarithm equality protocol, which allows to demonstrate knowledge of a secret such that no useful information is revealed

in the process. We denote the protocol by DLE protocol. In this subsection, we briefly review the protocol in $\mathbb{Z}_{\mathbb{N}}^*$ of unknown order.

Let H be a hash function. Assume that g_1, g_2 are two random generators in the subgroup of $\mathbb{Z}_{\mathbb{N}}^*$, the prover P owns a secret d, and h_1, h_2 such that $h_1 \equiv g_1^d \bmod N$ and $h_2 \equiv g_2^d \bmod N$. In order to convince the verifier V that he/she indeed owns the secret d but not expose it, the prover P will run DLE(g_1, g_2, h_1, h_2, d) as follows.

1. P selects $w \in \mathbb{Z}_{\mathbb{N}}^*$, computes a_1 and a_2

$$a_1 \equiv g_1^w \bmod N, \quad a_2 \equiv g_2^w \bmod N,$$

then computes $c = H(g_1, g_2, h_1, h_2, a_1, a_2)$ and $r = dc + w$, and then sends (r, a_1, a_2) as the proof of knowing the secret d.

2. V computes $c = H(g_1, g_2, h_1, h_2, a_1, a_2)$, and then checks

$$g_1^r \equiv h_1^c \cdot a_1 \bmod N, \quad g_2^r \equiv h_2^c \cdot a_2 \bmod N.$$

If they both hold, V can be convinced that P indeed knows the secret d. The DLE $(g_1, g_2,\ h_1, h_2, d)$ protocol is an efficient knowledge proof protocol. For its security please refer to ref. [9].

3 The proposed scheme

We now give a full description of our robust threshold partial blind signature scheme in this section. The scheme is composed of four parts: the system setting, key generation protocol, sub key verifying protocol and signature generation protocol. We describe each of them in turn.

3.1 System setting

Key management center (KMC) chooses two secure large primes p, q satisfying $p = 2p' + 1$ and $q = 2q' + 1$, where p', q' are also two large primes. Then, it computes the improved RSA modulus $N = pq$, the Euler totient function $\phi(N) = (p-1)(q-1)$ and $e, d \in \mathbb{Z}$, where

$$ed \equiv \frac{1}{2}\left(\frac{1}{4}\phi(N) + 1\right) \bmod \frac{1}{4}\phi(N).$$

KMC also takes $\alpha \in_R \mathbb{Z}_{\mathbb{N}}^*$ satisfying Jacobi symbol $\left(\frac{\alpha}{N}\right) = -1$, an element g with order $\frac{1}{4}\phi(N)$ and chooses three universal hash functions $H_0 : \{0,1\}^* \to \mathbb{Z}_{\mathbb{N}}^*$, H and F, where $F(x) \equiv 1 \bmod 2$ for any x. Then, the public key is $(\alpha, g, e, N, H_0, H, F)$ and the private key is $(d, \phi(N))$. Moreover, KMC also prepare some common information $info$ that represents the date or the amount of an e-cash.

3.2 Key generation protocol

KMC first randomly selects d_1 satisfying $\gcd(d_1, \frac{1}{4}\phi(N)) = 1$ and let $d_1 d \equiv d_2 \bmod \frac{1}{4}\phi(N)$, where $1 < d_1, d_2 < \frac{1}{4}\phi(N)$ and $d_1 \neq d_2$. Here d_2 is also called the shadow of the system key d.

Then KMC chooses a polynomial $f(x) \in \mathbb{Z}_{\frac{1}{4}\phi(N)}[x]$ of degree $t-1$ with $d_2 = f(0)$ and randomly chooses and publishes $x_1, x_2, \ldots, x_n \in \mathbb{Z}_{\frac{1}{4}\phi(N)}$ satisfying

$$\gcd\left(x_i - x_j, \frac{1}{4}\phi(N)\right) = 1, (i \neq j). \tag{1}$$

Then $f(x) = d_2 + c_1 x + \ldots + c_{t-1}x^{t-1}$. In the initial stage, KMC can compute $y_i = f(x_i)$ over $\mathbb{Z}_{\frac{1}{4}\phi(N)}$, $i = 1, 2, \ldots, n$. Clearly, if $y_{i_l}(l = 1, 2, \ldots, t)$ are known, then from the interpolation formula we can get

$$d_2 \equiv f(0) \equiv \sum_{1 \leqslant l \leqslant t} y_{i_l} \prod_{1 \leqslant w \leqslant t, w \neq l} (-x_{i_w})(x_{i_l} - x_{i_w})^{-1} \bmod \frac{1}{4}\phi(N). \tag{2}$$

Eq. (1) shows that $(x_{i_l} - x_{i_w})^{-1} \bmod \frac{1}{4}\phi(N)$ exists and so eq. (2) is computable under the condition that $\frac{1}{4}\phi(N)$ is known.

And then KMC chooses the following parameters: $N, e, b, (i, x_i)(i = 1, 2, \ldots, n)$, and computes

$$z_i \equiv y_i a^{-1} \bmod \frac{1}{4}\phi(N), (i = 1, 2, \ldots, n), \tag{3}$$

where $a = \prod_{1 \leqslant j < i \leqslant n}(x_i - x_j)$ and a^{-1} satisfying $a \cdot a^{-1} \equiv 1 \bmod \frac{1}{4}\phi(N)$. By eq. (1), $a^{-1}(\bmod \frac{1}{4}\phi(N))$ is computable. KMC secretly sends $(i, z_i), (i = 1, 2, \ldots, n)$ to n players $P_i(i = 1, 2, \ldots, n)$.

Finally, KMC computes $v = F(info)$, and sends $(vd_1)^{-1} \bmod \frac{1}{4}\phi(N)$ to a special trustee T (for example, the dealer in e-cash or administrator in electronic voting) in a secure way. Clearly only T knows the value of $(vd_1)^{-1} \bmod \frac{1}{4}\phi(N)$.

3.3 Sub key verifying protocol

Each player $P_i(i = 1, 2, \ldots, n)$ can verify his/her key $z_i(i = 1, 2, \ldots, n)$ by executing the following steps:

1. KMC computes and broadcasts $h(z_i) \equiv g^{z_i} \bmod N$, $(i = 1, 2, \ldots, n)$.
2. Each player $P_i(i = 1, 2, \ldots, n)$ can use his/her own (i, z_i) to verify the equation:

$$g^{z_i} \equiv h(z_i) \bmod N. \tag{4}$$

If eq. (4) holds, his/her key is accepted, otherwise rejected.

3.4 Signature generation protocol

Now assume that a requester B requests the trustee T to make a blind signature on message m. For simplicity, we will only discuss the case where $\left(\frac{H_0(m)}{N}\right) = 1$. For the other case where $\left(\frac{H_0(m)}{N}\right) = -1$, $H_0(m)$ can be easily turned into the default case by multiplying $H_0(m)$ with the factor α. Then, $\left(\frac{H_0(m)\cdot\alpha}{N}\right) = 1$.

The signature issuing protocol is executed as follows:

1. B first computes $v = F(info)$ and chooses the blind factor $b \in \mathbb{Z}_{\mathbb{N}}$, satisfying $(\frac{b}{N}) = 1$, and then sends $B(m) \equiv b^{ev} H_0(m) \bmod N$ to T.

2. On receiving the blinded message $B(m)$, T checks $\left(\frac{B(m)}{N}\right) = 1$. If it does not hold, T refuses the signing operation. Otherwise, T uses $(vd_1)^{-1} \bmod \frac{1}{4}\phi(N)$ to compute $B'(m) \equiv (B(m))^{2(vd_1)^{-1}} \bmod N$, and sends it to t players $P_{i_l}(1 \leqslant l \leqslant t)$. Meanwhile

T must obtain the license that is empowered by some authority organization and show the license to these players.

3. After verifying the license, each player $P_{i_l}(1 \leqslant l \leqslant t)$ computes

$$B'(m)^{z_{i_l}} = (B(m))^{2(vd_1)^{-1}z_{i_l}} \equiv (b^{ev}H_0(m))^{2(vd_1)^{-1}z_{i_l}} \bmod N, \tag{5}$$

and responds it to T. At the same time, P_{i_l} must prove that it is correctly generated. In other words, he should prove $\log_{(B'(m))}(B'(m))^{z_{i_l}} = \log_g g^{z_{i_l}}$ by the discrete logarithm equality protocol $\mathrm{DLP}(B'(m), g, B'(m)^{z_{i_l}}, g^{z_{i_l}}, z_{i_l})$ in section 2.5.

4. Once t partial signatures $B'(m)^{z_{i_l}}$, $l = 1, 2, \cdots, t$ are received and verified, T can compute a'' and b_l, $(l = 1, 2, \ldots, t)$, where

$$a' = \prod_{1\leqslant l,w\leqslant t, w<l}(x_{i_l} - x_{i_w}), a'' = \frac{a}{a'}, b_l = \frac{a'\prod_{1\leqslant w\leqslant t, w\neq l}(-x_{i_w})}{\prod_{1\leqslant l,w\leqslant t, w\neq l}(x_{i_l} - x_{i_w})}. \tag{6}$$

By eqs. (5) and (6), T can compute

$$\begin{aligned} sign' &= \left(\prod_{l=1}^{t}\left((b^{ev}H_0(m))^{2(vd_1)^{-1}z_{i_l}}\right)^{b_l}\right)^{a''} \\ &= (b^{ev}H_0(m))^{2(vd_1)^{-1}a''\sum_{1\leqslant l\leqslant t} z_{i_l}\frac{a'\prod_{1\leqslant w\leqslant t, w\neq l}(-x_{i_w})}{\prod_{1\leqslant l,w\leqslant t, w\neq l}(x_{i_l}-x_{i_w})}} \\ &= (b^{ev}H_0(m))^{2(vd_1)^{-1}a''a^{-1}a'd_2} \\ &= (b^{ev}H_0(m))^{2v^{-1}d} \equiv \pm bH_0(m)^{2v^{-1}d} \bmod N. \end{aligned}$$

5. T then sends $sign'$ to the requester B.

6. Since the blind factor b is chosen by B, B can gain T's signature on message m by dividing $sign'$ with b:

$$sign = sign'/b \equiv \pm H_0(m)^{2v^{-1}d} \bmod N.$$

And then, $(sign, m, v)$ constitutes a valid signature on m issued by T and t players.

7. To verify $(sign, m, v)$, any one can examine the following equality:

$$(sign)^{ev} = \pm H_0(m)^{2ev\cdot v^{-1}d} \equiv \pm H_0(m)^{1+\frac{1}{4}\phi(N)} \equiv \pm H_0(m) \bmod N.$$

4 Security discussion

In this section, we discuss some security properties of our proposed scheme. Precisely, we mainly focus on the properties of *blindness*, *unforgeability* and *robustness*.

4.1 Blindness

Blindness is the main property of a blind signature, which ensures both the user privacy and data authenticity. Our proposed threshold partial blind signature scheme is essentially to extend the partial blind signature. Therefore, to examine its blindness, we first prove the following two lemmas.

Lemma 1. The proposed blind improved RSA signature in subsection 2.3 is blind if the blind factor b is chosen at random.

Proof. To prove the scheme is blind, we should prove there exists some random value, which can map a view of signer during the issuing protocol into a signature.

Observe the issuing protocol, the requester B picks a blind factor $b \in \mathbb{Z}_{\mathbb{N}}$ to compute the blinded message $M = b^e m'(\bmod N)$ and sends it to signer A. As the blind factor b is randomly chosen and kept secret only by the requester B, the signer A cannot get the message m' from blinded message M. Therefore, the property of blindness can be satisfied.

Lemma 2. The proposed partial blind improved RSA signature in subsection 2.4 is blind if the blind factor b is chosen at random.

Proof. Observe the issuing protocol. The only difference between the partial blind improved RSA signature and the blind improved RSA signature is that there is a negotiated common information $v = F(\text{info})$ such that $v \equiv 1 \bmod 2$ in the former scheme.

From the blinded message $M = b^{ev} m' \bmod N$, the negotiated common information $v = F(\text{info})$ does not affect the randomness of blinded message M. Therefore, signer A still cannot know the message m', and the lemma holds immediately.

With the above two lemmas, we can easily show that the proposed threshold partial blind signature scheme also satisfies the blindness.

Theorem 1. The proposed partial blind threshold signature scheme in subsection 3 is blind if the blind factor b is chosen at random.

Proof sketch. Since the requester B chooses a random blind factor $b \in \mathbb{Z}_{\mathbb{N}}$ and computes $B(m) \equiv b^{ev} H_0(m) \bmod N$ to T, similar to the above lemmas' proof, the blindness obviously follows.

4.2 Unforgeability

The widely admitted security notion for digital signature is the existential unforgeability under an adaptive chosen message attack[27]. This notion notices the fact that an adversary cannot produce a valid signature, even he has obtained the signature of polynomially many messages of his choice. Since all blind signature schemes here are based on the improved RSA signature. Therefore, we will use the Coron's idea[24] to prove that the improved RSA signature is secure in the random oracle model[29].

Theorem 2. Suppose that the improved RSA is a (τ', ϵ')-secure. Then, for any q_s, q_h, the improved RSA signature scheme in subsection 2.2 is $(\tau, q_s, q_h, \epsilon)$-secure, where

$$\epsilon \leqslant \exp(1) \cdot (q_s + 1) \cdot \epsilon',$$

$$\tau = \tau' - (q_s + q_h + 1) \cdot Cost(\cdot),$$

and q_h, q_s denote the number of queries to the random oracle H_0 and to the signature oracle, and $Cost(\cdot)$ denotes the main time cost.

Proof. Suppose $\mathcal{A}$ is an adversary who can $(\tau, q_s, q_h, \epsilon)$-break the improved RSA signature scheme. We assume that q_h queries to H_0 are all distinct. Then, we will use $\mathcal{A}$ to construct another algorithm $\mathcal{B}$, who can break the improved RSA with another non-negligible ϵ' and within a running time τ',

$$\epsilon' \geqslant \frac{1}{\exp(1)(q_s + 1)} \cdot \epsilon,$$

$$\tau' = \tau + (q_s + q_h + 1) \cdot Cost(\cdot).$$

At first, the algorithm $\mathcal{B}$ is given a challenge as follows:

Given $(N, e, y = x^e \bmod N)$*, compute* x*.*

Then, the algorithm $\mathcal{B}$ will simulate the challenger of $\mathcal{A}$ and interact with $\mathcal{A}$ in the following game.

Setup: The algorithm $\mathcal{B}$ chooses a hash function $H_0 : \{0,1\}^* \to \mathbb{Z}_{\mathbb{N}}^*$, then sets and gives the public key (N, e, H_0) to $\mathcal{A}$. And in order to achieve the perfect simulation, H_0 behaves as a random oracle controlled by $\mathcal{B}$.

***H_0*-queries:** At any time, $\mathcal{A}$ provides a message m_i for H_0 oracle query. To respond to such H_0-queries, $\mathcal{B}$ should maintain an $\mathcal{H}$-list, which is initially empty and records all responses to previous H-queries. $\mathcal{B}$ selects a random $r_i \in \mathbb{Z}_{\mathbb{N}}^*$ satisfying Jacobi symbol $\left(\frac{r_i}{N}\right) = 1$, and then

1. with probability λ, computes $r_i^e \bmod N$, adds $< m_i, r_i, r_i^e >$ to an $\mathcal{H}$-list, and responds to $\mathcal{A}$ with $H_0(m_i) = r_i^e \bmod N$, where λ is a fixed probability determined later[24];

2. with probability $1-\lambda$, computes $y \cdot r_i^e \bmod N$, adds $< m_i, r_i, y \cdot r_i^e >$ to an $\mathcal{H}$-list, and responds to $\mathcal{A}$ with $H_0(m_i) = y \cdot r_i^e \bmod N$.

Signing-queries: When $\mathcal{A}$ makes a signature oracle query on a message m_i, which has been asked for H_0 oracle query, $\mathcal{B}$ looks up the $\mathcal{H}$-list. If $H_0(m_i) = r_i^e \bmod N$, $\mathcal{B}$ responds to r_i as the signature. Otherwise, $\mathcal{B}$ terminates the game and admits failure.

Solving the improved RSA: Finally, the adversary $\mathcal{A}$ terminates the game and outputs a valid forgery (m, σ). Here we assume that the hash value $H(m)$ of m has been asked and existed in $\mathcal{H}$-list. If $H(m) = y \cdot r_i^e \bmod N$, we will have $\sigma = H(m)^{2d} = (y \cdot r_i^e)^{2d} = \pm y^{2d} \cdot r_i \bmod N$. Then $x = y^{2d} = \pm\sigma / r_i \bmod N$. Otherwise, $\mathcal{B}$ also terminates the game and admits failure.

Now, we study the probability of $\mathcal{B}$ to solve the improved RSA. From the above construction, we know the probability that $\mathcal{B}$ response to all signature queries is at least λ^{q_s}. Then he outputs the expected x with probability $1-\lambda$.

And thus, $\mathcal{B}$ solves the improved RSA with probability at least $\lambda^{q_s}(1-\lambda)$. Therefore, we obtain

$$\epsilon' \geqslant \lambda^{q_s}(1-\lambda)\epsilon.$$

Since the maximum value of $\lambda^{q_s}(1-\lambda)$ is $\frac{1}{q_s+1} \cdot \left(\frac{1}{1+\frac{1}{q_s}}\right)^{q_s}$, when $\lambda = \frac{q_s}{q_s+1}$, we will have

$$\epsilon' \geqslant \frac{1}{q_s+1} \cdot \left(\frac{1}{1+\frac{1}{q_s}}\right)^{q_s} \cdot \epsilon.$$

And for large enough q_s, $\left(\frac{1}{1+\frac{1}{q_s}}\right)^{q_s} \approx \frac{1}{\exp(1)}$, so

$$\epsilon' \geqslant \frac{1}{\exp(1)(q_s+1)} \cdot \epsilon.$$

The main cost of algorithm $\mathcal{B}$ is that of running the adversary $\mathcal{A}$, hash oracle queries and signing oracle queries. Thus we can add these values and write the running time as

$$\tau' = \tau + (q_s + q_h + 1) \cdot Cost(\cdot).$$

This completes the proof.

Since blind improved RSA signature, partial blind improved RSA signature and threshold partial blind signature are all based on the improved RSA signature, we can safely draw a conclusion that they also satisfy the property of unforgeability.

4.3 Robustness

The robust threshold idea in our scheme is an innovative concept, which can be suitable to many application occasions, especially when the system key has some other purposes.

Theorem 3. The proposed threshold partial blind signature scheme in section 3 is robustness.

Proof sketch. Same as the general threshold signature schemes, our proposed partial blind threshold signature scheme also satisfies two basic properties: any $t(t < n)$ or more sub-secrets can make a valid signature easily, while any $t - 1$ or fewer sub-secrets cannot make a valid signature. Besides these, our proposed scheme also satisfies robustness. That is, the system key d is not exposed during any valid signature courses. We can see, even though n players ally, they still cannot reconstruct the system secret key d but the shadow $d_2 \bmod \frac{1}{4}\phi(N)$, since $\frac{1}{4}\phi(N)$ is unknown. In order to gain the system secret key d from $d_1 d \equiv d_2 \bmod \frac{1}{4}\phi(N)$, they must obtain the random d_1. But just as the proof in ref. [18], without knowing the factorization of large integer N, they cannot do that. Therefore, the system secret key d is secure and the scheme is robust.

5 Conclusion

A perfect threshold partial blind signature should satisfy the properties of *blindness*, *unforgeability* and *robustness*. In this paper, we have proposed such a threshold partial blind signature based on improved RSA cryptosystem. Thanks to its superior characteristics, the proposed scheme can have a bright future in many practical applications such as e-cash and e-voting systems. We partially proved the security of our scheme in the random oracle model.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grants Nos. 60225007 and 60572155), the National Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20020248024), and the Science and Technology Research Project of Shanghai (Grant Nos. 04JC14055 and 04DZ07067).

References

1 Chaum D. Blind signatures for untraceable electronic cash. Advances in Cryptology-CRYPTO'82, 1983, 199–203

2 Chaum D, Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24: 84–88

3 Chaum D, Fiat A, Naor M. Untraceable electronic cash. Advances in Cryptology-CRYPTO'88, 1988, 403: 319–327

4 Abe M, Fujisaki E. How to date blind signatures. Advances in Cryptology-ASIACRYPT'96, 1996, 1163: 244–251

5 Abe M, Okamoto T. Provably secure partially blind signatures. Advances in Cryptology-CRYPTO'00, 2000, 1880: 271–286

6 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613

7 Desmedt Y, Frankel Y. Threshold cryptosystems. Advances in Cryptology-CRYPTO'89, 1990, 335: 307–315

8 Gennaro R, Jarecki S, Krawczyk H, et al. Robust threshold DSS signatures. Advances in Cryptology-EUROCRYPTO'96, 1996, 1070: 354–371

9 Shoup V. Practical threshold signatures. Advances in Cryptology-EUROCRYPTO'00, 2000, 1807: 207–220

10 Jarecki S, Lysyanskaya A. Adaptively secure threhold cryptography. Advances in Cryptology-EUROCRYPTO'00, 2000, 1807: 221–242

11 Juang W S, Lei C L. Blind threshold signatures based on discrete logarithm. Proceedings of the 2nd Asian Computing Science Conference, 1996, 1179: 172–181

12 Juang W S, Lei C L, Yu P L. Provably secure blind threshold signatures based on discrete logarithm. Proceedings of 1999 National Computer Symposium, 1999, 198–205

13 Schnorr C P. Efficient identification and signatures for smart cards. Advances in Cryptology-CRYPTO'89, 1990, 435: 235–251

14 Okamoto T. Provably secure and practical identification schemes and corresponding signature schemes. Advances in Cryptology-CRYPTO'92, 1992, 740: 31–53

15 Kim J, Kim K, Lee C. An efficient and provably secure threshold blind signature. International Conference on Information Security and Cryptology-ICISC'01, 2002, 2288: 318–327

16 Vo D L, Zhang F, Kim K. A new threshold blind signature scheme from pairings. Symposium on Cryptography and Information Security-SCIS'03, 2003, 1(2): 233–238

17 Stinson D R, Strobl R. Provably secure distributed Schnorr signatures and a (t, n) threshold scheme for implicit certificates. Information Security and Privacy-ACISP'01, 2001, 2119: 417–434

18 Cao Z F. A threshold key escrow scheme based on public key cryptosystem, Sci China Ser E-Tech Sci, 2001, 44(4): 441–448

19 Cao Z F. Two classes of robust threshold key escrow schemes. Journal of Software, 2003, 14(6): 1164–1171

20 Boneh D, Venkatesan R. Breaking RSA may not be equilvalent to factoring. Advances in Cryptology-EUROCRYPTO'98, 1998, 1402: 59–71

21 Lu R X, Cao Z F, Zhu H J. A robust $(k, n)+1$ threshold proxy signature scheme based on factoring. Applied Mathematics and Computation, 2005, 166(1): 35–45

22 Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21: 120–126

23 Bellare M, Rogaway P. Optimal asymmetric encryption-how to encrypt with RSA. Advances in Cryptology-EUROCRYPTO'94, 1994, 950: 92–111

24 Cao Z F. The multi-dimension RSA and its low exponent security. Sci China Ser E-Tech Sci, 2000, 43(4): 349–354

25 Cao Z F. On the security of the RSA based on a polynomial over finite fields $\mathbb{F}_p$ and a new analog of the RSA. Journal of China Institute of Communications, 1999, 20(6): 15–18

26 Lu R X, Cao Z F. Efficient remote user authentication scheme using smart card. Computer Networks, 2005, 49(4): 535–540

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

28 Coron J. On the exact security of full domain hash, Advances in Cryptology-CRYPTO'00, 2000, 1880: 229–235

29 Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols. Proceeding of the 1st Computer & Communication Security, 1993, 62–73