# A Provably Secure Scheme for Partially Blind Signatures

Fuw-Yi Yang and Jinn-Ke Jan*

Department of Applied Mathematics, National Chung Hsing University, Taichung 402, Taiwan, R.O.C., yangfy@ms7.hinet.net

*Department of Computer Science, National Chung Hsing University, Taichung 402, Taiwan, R.O.C., jkjan@cs.nchu.edu.tw

*Abstract:* This paper proposes a new scheme for partially blind signature based on the difficulty in solving the discrete logarithm problem. Under the assumption of the generic model, random oracle model, and intractable ROS-problem, this paper formally proves that the proposed scheme is secure against one-more signature forgery under the adaptively parallel attack. Previous schemes using two signing equations for plain information and commitment. The proposed scheme uses two secret keys to combine these two signing equations, thus it is more efficient than previous schemes in both communicational and computational cost.

*Keywords:* Blind Signature, signatures, partially blind signatures.

*Introduction:* Blind signature schemes [1] allow users to blind the messages being signed and reshape the outside of signatures such that the signer cannot link the signatures and the users. It is a useful building block in applications where anonymity is one of the most significant considerations, such as electronic cash and electronic voting systems.

But it may not be a good idea to blind everything in every application. Considering the setting for electronic cash systems, a database is required to store the deposited coins so as to detect double spending. In the area of electronic cash systems based on

the use of blind signatures, the coins are usually the blind signatures issued from the banks, the database will grow unlimitedly if no explicitly expiring date is specified. In addition, the banks usually issues coins of different denominations in order to allow exact payments, we require clearly inscribing the value of each coin.

The scheme of partially blind signature proposed in [2], which is based on the well-known RSA Cryptosystem, helps a lot to solve the problems stated above. This scheme allows the blind signatures explicitly containing some information that the signer and user have agreed on. Therefore, the pieces of common agreed information can enclose the expiring date, the denominational data and other useful message. Based on the difficulty in solving the problem discrete logarithms, the schemes proposed in [3-5] are provably secure schemes for partially blind signature as long as the issued blind signatures are poly-logarithmic number in the security parameter $|q|$, *i.e.*, the bit length of the group order $q$. By the more complex protocol (a signature scheme with three-party) proposed in [6], those schemes in [3-5] can be modified such that they are secure up to polynomial number of issued blind signatures (The term polynomial number implies polynomial number in the security parameter $|q|$.). However, the final scheme will result in more expensive computations during the interactions between the signer and user. The extra computations are a result of using the technique of cut-and-choose to confirm that the user honestly challenges the signer.

*Contributions:* Based on the hardness of discrete logarithm problem, generic model, random oracle, and intractability of the ROS-problem proposed in [7-8], the paper proposes a provably secure scheme for partially blind signature. The proposed scheme outperforms the schemes in [3, 9] in computation and signature size. Furthermore the proposed scheme is secure up to polynomial number of issued blind signatures.

*Notation:* Let $G$ be an arbitrary group with prime order $q$ and $g$ be the generator of the group. $M$ is an arbitrary message space. $a||b$ denotes a concatenation of strings $a$ and $b$. $a \in_R G$ denotes that the element $a$ is randomly selected from the set $G$. $H(.)$ is a collision-resistant hash function defined as $H(.): \{0, 1\}^* \rightarrow Z_q$, where $Z_q$ is the additive group of integers modulo $q$.

*Proposed scheme:* Assume that the user $U$ wants to get a partially blind signature on a message $m \in M$. Also, assume that the signer $S$ and user $U$ have agreed on common information $info \in M$. Let $x_1, x_2 \in_R Z_q$ be the signer's secret keys and the corresponding public keys be $y_1 = g^{x_1}$ and $y_2 = g^{x_2}$, where $y_1, y_2 \in G$. The signer and user cooperatively execute the following steps.

1. $S$ chooses $w \in_R Z_q$, computes the commitment $r = g^w \in G$ and sends $r$ to the user $U$.
2. $U$ chooses $u, v \in_R Z_q$, computes the quantities $z = H(info)$, $r' = r\, g^u (y_1 y_2^z)^v \in G$, $c' = H(g||y_1||y_2||m||info||r')$ and $c = c' + v \in Z_q$. $U$ sends the challenge $c$ to $S$.
3. $S$ computes $z = H(info)$ and $s = w + c(x_1 + z x_2) \in Z_q$, and sends $s$ to $U$ as response.
4. $U$ computes $s' = s + u \in Z_q$. $U$ accepts $(m, info, c', s')$ as a valid signature if $c' = H(g||y_1||y_2||m||info||g^{s'}(y_1 y_2^z)^{-c'})$, otherwise rejects the response $s$.

*Blindness:* Let $(info, r, c, s)$ denote the signer's view and the user has the corresponding signature, *i.e.*, the tuple $(m, info, c', s')$. Also assume that the signer cannot distinguish the signatures by analyzing the information $info$. The property of blindness requires that the signer's view is independent of the user's signature. The lemma below proves the blindness of the proposed scheme.

**Lemma 1.** The tuple $(m, info, c', s')$ is a partially blind signature issued by a signer.

Among the four elements in this tuple, the signer has only the knowledge of the item *info*.

**Proof.** The signer and user have negotiated the common information *info* before they are engaged in the signing steps, and the signer has no knowledge of the message *m*, therefore the signer partially knows the context *(m, info)*. There exists a unique pair *(u, v)* for every valid signature, *i.e.*, $u = s' - s$ and $v = c - c'$. The existence of a unique pair *(u, v)* proves the property of blindness, since the user chooses them randomly from $Z_q$, the additive group of integers modulo *q*. □

Before discussing the security of the proposed scheme, the relevant vocabularies: novel adaptively parallel attack, ROS-problem, generic model and one-more forgery should be introduced. The following briefly describe them.

*A new novel adaptively parallel attack on Schnorr's signatures:* For easy reading, the novel adaptively parallel attack proposed in [8] is described briefly in the following. Assume that a signer has a secret key $x \in Z_q$ and the corresponding public key $y = g^x \in G$. A Schnorr signature on the message *m* is the triplet *(m, c, z)* and verified by checking $c = H(g^z y^{-c}, m)$. Let an adversary initiate simultaneously *l* sessions with the signer. Then the adversary will receive *l* commitments $g_1 = g^{r_1}, \ldots, g_l = g^{r_l}$, where $r_i \in_R Z_q$, $g_i \in G$ and $i = 1,\ldots, l$. In order to compute appropriate challenges, the adversary randomly selects $a_{k,1},\ldots, a_{k,l}$ from the group $Z_q$ and messages $m_1,\ldots, m_t$ from the message space *M*, computes the quantities

$$f_k = g_1^{a_{k,1}} \ldots g_l^{a_{k,l}} \in G \text{ and} \quad (1)$$

$$H(f_k, m_k) \text{ for } k = 1,\ldots,t. \quad (2)$$

Then the adversary finds solvable $(l + 1)$ equations out of the following *t* equations

(3) in the unknown variables (challenges) $c_1, \ldots, c_l$ over the group $Z_q$.

$$H(f_k, m_k) = \sum_{i=1}^{l} a_{k,i} c_i \quad \text{for } k = 1,\ldots, t. \tag{3}$$

Without loss of generality, the set of solvable $(l + 1)$ equations are as follows ("$s$" implies solved).

$$H(f_s, m_s) = \sum_{i=1}^{l} a_{s,i} c_i \quad \text{for } s = 1,\ldots, l, (l + 1). \tag{4}$$

After solving these $l$ variables, the adversary sends them as challenges to the signer. The signer sends the following responses back to the adversary.

$$z_i = r_i + c_i\, x \in Z_q \text{ for } i = 1,\ldots, l. \tag{5}$$

From the $l$ challenges, $l$ responses in (5), and $(l + 1)$ solved equations in (4), the adversary obtains the set of $(l + 1)$ signatures $(m_s, c'_s, z'_s)$ by the following equations.

$$c'_s = \sum_{i=1}^{l} a_{s,i} c_i = H(f_s, m_s), \tag{6}$$

$$z'_s = \sum_{i=1}^{l} a_{s,i} z_i \ , \ s = 1,\ldots, l, (l + 1). \tag{7}$$

*ROS-Problem*: The probability of obtaining $(l + 1)$ signatures from $l$ interactions with the signer depends on finding the $(l + 1)$ solvable equations (4) from the $t$ equations (3). Note that the hash function $H(.)$ has been modeled as a random oracle (ROM) proposed in [10-11] that given an input in $\{0, 1\}^*$ outputs a random number in $Z_q$. Thus the left-hand sides of equations (3) are random values. Then finding the $(l + 1)$ solvable equations (4) from the $t$ equations (3) is essential a ROS-problem stated in [7-8]. The ROS-problem is to find an over-determined solvable system of linear equations modulo $q$, *i.e.*, find a solvable subsystem of $(l + 1)$ equations from the following $t$ equations.

$$\sum_{i=1}^{l} a_{k,i} c_i = H(a_{k,1}, \ldots, a_{k,l}), \text{ where } k = 1,\ldots, t,\ l << t, \text{ and } a_{k,i} \in Z_q. \tag{8}$$

The ROS-problem is related to a NP-complete problem [7]. The expected number

of solvable *(l + 1)* distinct equations out of *t* equations in (8) is stated without proof by the following theorem, which is evaluated as Theorem 1 in [8].

**Theorem 2.** A. For arbitrary coefficients $a_{k,i} \in Z_q$, the average number of solvable subsystems of *(l + 1)* out of *t* equations (8) is at most $\binom{t}{l+1} / q$.

B. A constant selection of a set of *(l + 1)* equations out of *t* equations (8) is solvable with probability $q^{-1}(1 - q^{-1} + O(q^{-2}))$.

**Lemma 3.** The solvable subsystems of *(l + 1)* out of *t* equations (8) must be hard to find.

**Proof.** By Theorem 2.B, the lemma is proved. However, this lemma intends to describe a more concrete concept. Since there are at most $\binom{t}{l+1} / q$ solvable *(l + 1)* equations, then it seems feasible to forge Schnorr signature after some interactions with the signer. Using the example presented in [8], if finding a set of *(l + 1)* solvable equations is easy, then the novel adaptively attack is possible for $l = 4$, $t = 2^{50}$, and $q = 2^{200}$, *i.e.*, $(2^{50} / 120) \approx \binom{t}{l+1} / q$. This result contradicts the security of Schnorr signatures and proves the lemma. □

*Generic Model:* In equation (1), a new group element $f_k \in G$ is generated by $f_k = g_1^{a_{k,1}} \ldots g_l^{a_{k,l}}$. This is a generic step in the Generic Group model (GM). We introduce some vocabularies of GM, for further details please refer to [8, 12-15]. A generic step for group element consists of multivariate exponentiations (*mex*), *i.e.*, *mex:* $Z_q^d \times G^d \rightarrow G$, $(b_1,\ldots,b_d, g_1,\ldots, g_d) \mapsto \prod_{i=1}^{d} g_i^{b_i}$, where $d \geq 0$. Queries to the hash oracle and interactions with the signer are also generic steps. A generic algorithm is a sequence of *t* generic steps: Giving *t'* group elements $f_1,\ldots,f_{t'}$, computes the set of $t - t'$ group

elements $\{f_i \mid f_i = \prod_{j=1}^{i-1} f_j^{b_j}, i = (t' + 1),\ldots,t\}$, where non-group elements $b_1,\ldots,b_{i-1} \in Z_q$ depend arbitrarily on $i$ and the set of the previous collision of group elements. Thus a new group element is generated using the recorded data.

*One-more forgery:* For an integer $l$ polynomial in the security parameter, a practically blind signature scheme should be secure against the forgery of $(l, l + 1)$ even under the novel adaptively parallel attack mentioned above. The security of $(l, l + 1)$ forgery for blind signature was proposed in [4-5, 16]. The success of $(l, l + 1)$ forgery implies that after $l$ interactions with the signer, the adversary has obtained $(l + 1)$ signatures with non-negligible probability without knowing the signer's secret key. If the number $l$ is polynomial in the security parameter then the $(l, l + 1)$ forgery is called one-more forgery. In the electronic cash systems, the schemes of blind signature are essential ingredients of anonymous electronic cash. The success of $(l, l + 1)$ forgery implies that an adversary can spend more coins than he had withdrawn from the bank. The proposed scheme's security is discussed in the following.

*Security:* A generic adversary is an adversary in the model of ROM + GM. Under this model, the generic can interact with the signer, perform multivariate exponentiations, and query hash oracle. Assume that a generic adversary $A$ is given the public parameters: the group $G$ of prime order $q$, generator $g$ of $G$, signer's public keys $(y_1, y_2)$, and an oracle for $H(.)$. Also assume the adversary $A$ has performed $t$ generic steps including $l$ times of signer interactions, *i.e.*, the adversary $A$ can construct at least $l$ valid signatures. We want to prove that $A$ cannot have probability of success better than $\binom{t}{2} / q$, if $A$ conduct an adaptively parallel attack to produce $(l + 1)$ valid signatures, *i.e.*, the one-more signature forgery under the adaptively parallel attack.

Since the adversary *A* has conducted *t* generic steps including *l* interactions with the signer. Hence, the signer has generated the set of tuples $\{(w_i, s_i, g_i) | g_i = g^{w_i} \in G, w_i \in_R Z_q, s_i = w_i + c_i (x_1 + z_i x_2) \in Z_q, z_i = H(info_i), c_i$ is the $i_{th}$ challenge of the adversary $A , i = 1, 2,\ldots l\}$. Also assume the adversary *A* has produced some *t'* elements of *G* (including the received commitments) and queried *t"* times to the hash oracle, where $t = t' + t"$. Let $f = \{f_1 = g, f_2 = y_1, f_3 = y_2, f_4,\ldots,f_{t'} \in G\}$ be the set of *t'* elements generated by *A*, where $f_i = g^{a_{i,-2}} y_1^{a_{i,-1}} y_2^{a_{i,0}} \prod_{j=1}^{l} g_j^{a_{i,j}}$ for $i = 1, 2,\ldots, t'$. For example, the exponents of group element $f_1$ are $a_{1,-2} = 1, a_{1,-1} = a_{1,0} = \ldots = a_{1,l} = 0$. Obviously, the adversary chooses exponents $a_{i,j} \in Z_q$ depending arbitrarily on the previously computed non-group data and collided group elements such that $f_i$ is dependent on $f_{i-1}, f_{i-2},\ldots, f_1$.

In the following probabilistic analysis, the probability space consists of $H(.), y_1, y_2$, and the signer's random coins *w*.

**Lemma 4.** The probability of triple collisions among the group elements $f_1, f_2,\ldots, f_{t'}$ is at most $\binom{t'}{3} / q^2$.

**Proof.** Let us define the discrete random variables $X_{ijk}$ for $1 \le i < j < k \le t'$ as follow: $X_{ijk} = 1$ if collision occurs, *i.e.*, $f_i = f_j = f_k$, but otherwise $X_{ijk} = 0$. The probability that $f_i = f_j = f_k$ is $1 / q^2$, thus the expectation of the discrete random variable $E[X_{ijk}] = 1 \times (1 / q^2) + 0 \times (1 - 1 / q^2) = 1 / q^2$. The expected number of triplets is just the sum of the expectations, that is, $\sum_{i=3}^{t'} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} E[X_{ijk}] = \binom{t'}{3} / q^2$. Since the trivial collisions, *i.e.*, the event $(Collision = \{f_i = f_j = f_k \mid 1 \le i < j < k \le t'\}$ and *Collision* is independent of the signer's secret), contribute no information to solve the signer's secret data, we ignore the probability of trivial collisions. Thus, we have proved

Lemma 4. □

**Lemma 5.** If there occurs non-trivial triple collisions, then the signer's secret data, *i.e.*, $(x_1, x_2, w_1, \ldots, w_l)$, are solvable with overwhelming probability.

**Proof.** Assume the non-trivial collision triplet is $f_i = f_j = f_k \in G$, the relationship $log_g^{f_i} = log_g^{f_j} = log_g^{f_k}$ is true. Since $log_g^{f_i} = a_{i,-2} + a_{i,-1}\, x_1 + a_{i,0}\, x_2 + \sum_{e=1}^{l} a_{i,e} w_e$, $log_g^{f_j} = a_{j,-2} + a_{j,-1}\, x_1 + a_{j,0}\, x_2 + \sum_{e=1}^{l} a_{j,e} w_e$ and $log_g^{f_k} = a_{k,-2} + a_{k,-1}\, x_1 + a_{k,0}\, x_2 + \sum_{e=1}^{l} a_{k,e} w_e$, therefore, the following equations (9) and (10) are obtained.

$$a_{i,-2} + a_{i,-1}\, x_1 + a_{i,0}\, x_2 + \sum_{e=1}^{l} a_{i,e} w_e = a_{j,-2} + a_{j,-1}\, x_1 + a_{j,0}\, x_2 + \sum_{e=1}^{l} a_{j,e} w_e \bmod q \quad (9)$$

$$a_{j,-2} + a_{j,-1}\, x_1 + a_{j,0}\, x_2 + \sum_{e=1}^{l} a_{j,e} w_e = a_{k,-2} + a_{k,-1}\, x_1 + a_{k,0}\, x_2 + \sum_{e=1}^{l} a_{k,e} w_e \bmod q \quad (10)$$

From (9) and (10), the signer's secret keys $x_1$ and $x_2$ are expressed in (11) and (12).

$$x_1 = b_{1,0} + \sum_{e=1}^{l} b_{1,e} w_e \bmod q \quad (11)$$

$$x_2 = b_{2,0} + \sum_{e=1}^{l} b_{2,e} w_e \bmod q \quad (12)$$

Interacting with the signer $l$ times, the adversary $A$ has $l$ linear polynomials $s_i = w_i + c_i (x_1 + a_i x_2)$ in $Z_q[x_1, x_2, w_1, \ldots, w_l]$, *i.e.*, $x_1, x_2, w_1, \ldots, w_l$ are indeterminate variables over $Z_q$. For each polynomial, the variable $x_1$ and $x_2$ are replaced with $x_1 = b_{1,0} + \sum_{e=1}^{l} b_{1,e} w_e$ and $x_2 = b_{2,0} + \sum_{e=1}^{l} b_{2,e} w_e$. Thus, $A$ has $l$ linear polynomials in $Z_q[w_1, \ldots, w_l]$. Because the adversary chooses exponents $a_{i,j} \in Z_q$ depending arbitrarily on the previously computed non-group data, the $l$ linear polynomials in $Z_q[w_1, \ldots, w_l]$ are solvable with overwhelming probability $(1 - q^{-1})(1 - q^{-2}) \ldots (1 - q^{-l+1})$. □

**Lemma 6.** The probability of two pairs of pair collision among the group elements $f_1$,

$f_2,\ldots, f_{t'}$ are at most $(\binom{t'}{2} / q)^2$.

**Proof.** Let us define the discrete random variables $X_{ij}$ for $1 \le i < j \le t'$ as follow: $X_{ij} = 1$ if collision occurs, *i.e.*, $f_i = f_j$, but otherwise $X_{ij} = 0$. The probability that $f_i = f_j$ is $1 / q$, thus the expectation of the discrete random variable $E[X_{ij}] = 1 \times (1 / q) + 0 \times (1 - 1 / q) = 1 / q$. The probability of a pair collision is just the sum of the expectations, that is, $\sum_{i=2}^{t'} \sum_{j=1}^{i-1} E[X_{ij}] = \binom{t'}{2} / q$. Thus the probability of two pairs of pair collision is $(\binom{t'}{2} / q)^2$. Like the proof in Lemma 4, the event of trivial pair collision is ignored. Therefore, Lemma 6 is proved. □

**Lemma 7.** If there occurs two pairs of non-trivial pair collision, then the secret data, *i.e.*, $(x_1, x_2, w_1, \ldots, w_l)$, are solvable with overwhelming probability.

**Proof.** Assume the two pairs of non-trivial collision pair are $f_i = f_j$ and $f_m = f_n$, where $f_i$, $f_j$, $f_m$, $f_n \in G$. Thus the equations $\log_g^{f_i} = \log_g^{f_j}$ and $\log_g^{f_m} = \log_g^{f_n}$ are obtained. Similar to the proof in Lemma 5, the following equations (13) and (14) are derived.

$$a_{i,-2} + a_{i,-1} x_1 + a_{i,0} x_2 + \sum_{e=1}^{l} a_{i,e} w_e = a_{j,-2} + a_{j,-1} x_1 + a_{j,0} x_2 + \sum_{e=1}^{l} a_{j,e} w_e \bmod q \quad (13)$$

$$a_{m,-2} + a_{m,-1} x_1 + a_{m,0} x_2 + \sum_{e=1}^{l} a_{m,e} w_e = a_{n,-2} + a_{n,-1} x_1 + a_{n,0} x_2 + \sum_{e=1}^{l} a_{n,e} w_e \bmod q \quad (14)$$

From (13) and (14), the signer's secret keys $x_1$ and $x_2$ are expressed in (15) and (16).

$$x_1 = b_{1,0} + \sum_{e=1}^{l} b_{1,e} w_e \bmod q \quad (15)$$

$$x_2 = b_{2,0} + \sum_{e=1}^{l} b_{2,e} w_e \bmod q \quad (16)$$

Following the same procedure in Lemma 5, the proof of Lemma 7 is completed. □

**Lemma 8.** (The generic adaptively parallel attack) From the $l$ interactions with the signer, the adversary $A$ obtains $(l + 1)$ signatures with probability not better than $1/q$,

except he can solve ROS-problem or there exists group collisions or hash collisions.

**Proof.** The set of tuples $\{(w_j, g_j, c_j, s_j) | w_j \in_R Z_q, g_j = g^{w_j} \in G, j = 1,...,l\}$ describes the interactions between the signer and adversary. The signer sends $g_j$ to the adversary $A$ and responds $s_j = w_j + c_j (x_1 + z_j x_2)$ to $A$ when receiving the challenge $c_j$, where $z_j = H(info_j)$. Suppose that the adversary $A$ is able to constructs $(l + 1)$ different valid signatures $(m_i, info_i, c'_i, s'_i)$, $i = 1, ..., (l + 1)$. Then, $c'_i = H(g || y_1 || y_2 || m_i || info_i || g^{s'_i} (y_1 y_2^{z_i})^{-c'_i})$.

Since the adversary has generated $t'$ distinct group elements, he obtained a set of group elements $f = \{f_1 = g, f_2 = y_1, f_3 = y_2, f_4,...f_{t'} \in G\}$. In addition, he has queried $t''$ times to the hash oracle, *i.e.*,

$c_k = H(g || y_1 || y_2 || m_k || info_k || f_k)$ for $k = 1,...,t''$ and $f_k \in f$. (17)

Therefore, there is a mapping from $k \in \{1, 2,..., t''\}$ to each $i \in \{1, 2,...,(l + 1)\}$ such that $g^{s'_i} (y_1 y_2^{z_i})^{-c'_i} = f_i$ and $f_k = f_i$. Let us denote $f_k$ as $f_{ki}$ if $f_k = f_i$. Thus, the adversary $A$ has the following equations (18) and (19).

$$f_i = g^{s'_i} (y_1 y_2^{z_i})^{-c'_i} = g^{s'_i - c'_i x_1 - c'_i z_i x_2} \quad (18)$$

$$f_{ki} = g^{a_{ki,-2} + a_{ki,-1} x_1 + a_{ki,0} x_2 + \sum_{j=1}^{l} a_{ki,j} w_j} = g^{a_{ki,-2} + a_{ki,-1} x_1 + a_{ki,0} x_2 + \sum_{j=1}^{l} a_{ki,j} (s_j - c_j x_1 - c_j z_j x_2)} \quad (19)$$

From equations (18) and (19), we deduce equation (20) below.

$$s'_i = a_{ki,-2} + \sum_{j=1}^{l} a_{ki,j} s_j + (c'_i + a_{ki,-1} - \sum_{j=1}^{l} a_{ki,j} c_j) x_1 + (c'_i z_i + a_{ki,0} - \sum_{j=1}^{l} a_{ki,j} c_j z_j) x_2 \quad (20)$$

Since $x_1$ and $x_2$ are signer's secret key, the adversary can successfully compute $s'_i$ if he can set the coefficient of $x_1$ and $x_2$ to zero, *i.e.*, $(c'_i + a_{ki,-1} - \sum_{j=1}^{l} a_{ki,j} c_j) = (c'_i z_i + a_{ki,0} - \sum_{j=1}^{l} a_{ki,j} c_j z_j) = 0$. This implies the adversary can find two solvable $(l + 1)$ equations (21) and (22) out of $t''$ equations (17).

$$c'_i = -a_{ki,-1} + \sum_{j=1}^{l} a_{ki,j} c_j = H(g || y_1 || y_2 || m_{ki} || info_{ki} || f_{ki}) \text{ , } i = 1,..., (l+1) \quad (21)$$

$$c'_i = (-a_{ki,0} + \sum_{j=1}^{l} a_{ki,j} c_j z_j)(z_i)^{-1} = H(g || y_1 || y_2 || m_{ki} || info_{ki} || f_{ki}), \; i = 1,..., (l+1) \quad (22)$$

The suggestion of finding two solvable $(l + 1)$ equations (21) and (22) out of $t''$ equations (17) contradicts the intractability of the ROS- problem. Thus the probability that equations (21) and (22) hold true cannot exceed $1 / q$. Also the generic adaptive parallel attack has assumed that there is no collision of group elements and hash values, therefore, the adversary cannot have probability of success better than $1 / q$. □

**Lemma 9.** Due to collisions of hash value, the adversary $A$ obtains $(l + 1)$ signatures with probability not better than $(l \times t'' / q)$.

**Proof.** Assume that the tuple $(m_v, info_v, c_v, s_v)$ is a valid signature (the subscript $v$ implies "valid"). After interacting $l$ times with the signer, the adversary $A$ obtains at least $l$ valid signatures. Let $c_k = c_v$ be a hash collision. Then, $c_v = H(g || y_1 || y_2 || m_v || info_v || g^{s_v} (y_1 y_2^{z_v})^{-c_v}) = c_k = H(g || y_1 || y_2 || m_k || info_k || f_k)$, where $k, v \in \{1,..., t''\}$, $k \neq v$ and $g^{s_v} (y_1 y_2^{z_v})^{-c_v} \neq f_k$. If $f_k = g^{s_k} (y_1 y_2^{z_k})^{-c_k}$, then the tuple $(m_k, info_k, c_k, s_k)$ is also a valid signature. Thus the following equations (23) and (24) are obtained.

$$s_v = a_{v,-2} + \sum_{j=1}^{l} a_{v,j} s_j + (c_v + a_{v,-1} - \sum_{j=1}^{l} a_{v,j} c_j) x_1 +$$

$$(c_v z_v + a_{v,0} - \sum_{j=1}^{l} a_{v,j} c_j z_j) x_2 \quad (23)$$

$$s_k = a_{k,-2} + \sum_{j=1}^{l} a_{k,j} s_j + (c_k + a_{k,-1} - \sum_{j=1}^{l} a_{k,j} c_j) x_1 +$$

$$(c_k z_k + a_{k,0} - \sum_{j=1}^{l} a_{k,j} c_j z_j) x_2 \quad (24)$$

After interacting $l$ times with the signer, the $k_{th}$ group element $f_k$ is generated. Thus the coefficients $a_{k,b}$, $b = -1, 0, 1,\ldots, l$, are chosen such that $(a_{v,-1} - \sum_{j=1}^{l} a_{v,j} c_j) = (a_{k,-1}$

$-\sum_{j=1}^{l} a_{k,j} c_j$ ) and $(a_{v,0} - \sum_{j=1}^{l} a_{v,j} c_j z_j) = (a_{k,0} - \sum_{j=1}^{l} a_{k,j} c_j z_j)$. Therefore, $s_k = (s_v - a_{v,-2} + a_{k,-2}) \bmod q$, if there exists the hash collisions $c_v = c_k$ and $z_v = z_k$. Namely, the adversary could forge a signature, by giving valid signatures and hash collisions. Since a signer cannot distinguish signatures by analyzing the plain text *info*, the event $z_v = H(info_v) = z_k = H(info_k)$ occurs with high probability. Therefore, the probability of the hash collisions $c_v = c_k$ and $z_v = z_k$ is at most $(l \times t'' / q)$, since the adversary has queried hash oracle $t''$ times. □

**Theorem 10.** From the $l$ interactions with the signer, an adversary $A$ obtains $(l + 1)$ signatures with probability not better than $1/q + (\binom{t'}{2}/q)^2 + \binom{t'}{3}/q^2 + (l \times t'')/q < (l \times t)/q$.

**Proof.** The adversary can achieve his goal in the following cases:

1. Collisions of group elements,
2. Adaptively parallel attack, and
3. Collisions of hash values.

By lemma 4-7, the probability of the first case is at most $(\binom{t'}{2}/q)^2 + \binom{t'}{3}/q^2$. By lemma 6, the probability of the second case is at most $1/q$. In the third case, the probability does not exceed $l / q$. Therefore, combining three cases, the adversary $A$ obtains $(l + 1)$ signatures with probability not better than $1/q + (\binom{t'}{2}/q)^2 + \binom{t'}{3}/q^2 + (l \times t'')/q$. In the case $(t')^3 < q$, the probability expression is given by the compact form $(l \times t)/q$. □

*Performance:* Compare with the schemes in [3, 9], Table 1 shows that the proposed scheme is more efficient in both the computational cost and message size. The scheme in [9] has been incorporated the restrictive property, the comparison is made on the

non-restrictive version. In estimating the computational cost, we count only the modular exponentiations.

Table 1: The comparisons of the proposed scheme, schemes in [9] and [3]

| | Proposed scheme | Scheme [9] | Scheme [3] |
|---|---|---|---|
| Signer's computations | *1* | *3 (2.17)** | *3 (2.17)** |
| User's computations | *6 (2.5)** | *8 (4.68)** | *8 (4.68)** |
| Verifier's computations | *3 (1.25)** | *3 (2.34)** | *4 (2.34)** |
| Signature size | *2 \|M\| + 2 \|q\|* | *2 \|M\| + 4 \|q\|* | *2 \|M\| + 4 \|q\|* |

* The technique of efficient simultaneous multiple exponentiations [17] is used to evaluate the modular exponentiations.

*Conclusions:* The paper proposes a new provably secure scheme for partially blind signatures. Comparing with previous schemes, the proposed scheme has smaller signature size and less computational cost than that of the schemes in [3, 9]. We think that the improvement is due to the use of double secret keys. Using two secret keys combines the response message for plain information with response message of commitment. Thus the integration of response messages contributes to the efficiency of the proposed scheme in both the signature size and computational cost. The computational cost for signer, user and verifier are all reduced significantly. For the signer, the relief of computing is valuable, since the signer would be the bottleneck in the environment of electronic cash. Also, by Theorem 10, the proposed scheme is secure up to polynomial number of issued signatures.

**References**

1. D. Chaum, “Blind signatures for untraceable payments,” *Advances in Cryptology-CRYPTO’82*, pp. 199-203, 1983.
2. M. Abe and E. Fujisaki, “How to date blind signatures,” *Advances in Cryptology-ASIACRYPT’96*, LNCS 1163, pp. 244-251, 1996.
3. M. Abe and T. Okamoto, “Provably secure partially blind signatures,” *Advances in Cryptology-CRYPTO’00*, LNCS 1880, pp. 271-286, 2000.
4. D. Pointcheval and J. Stern, “ Provably secure blind signature schemes,” *Advances in Cryptology-ASIACRYPT’96*, LNCS 1163, pp. 252-265, 1996.
5. D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” *Journal of Cryptology*, Vol. 13, N0. 3, pp. 361-396, 2000.
6. D. Pointcheval, “Strengthened security for blind digital signatures,” *Advances in Cryptology-EUROCRYPT’98*, LNCS 1403, pp. 391-405, 1998.
7. J. Hastad, “Some optimal Inapproximability results,” *Proceedings of ACM Symposium on Theory of Computing 1997*, pp. 1-10, 1997.
8. C. P. Schnorr, “Security of blind discrete log signatures against interactive attacks,” *ICICS 2001*, LNCS 1880, pp. 1-12, 2001.
9. G. Maitland and C. Boyd, “A provably secure restrictive partially blind signature scheme,” *PKC 2002*, LNCS 2274, pp. 99-114, 2002.
10. A. Fiat and A. Shamir, “How to prove yourself: practical solutions of identification and signature problems,” *Advances in Cryptology-CRYPTO’86*, LNCS 263, pp. 186-194, 1987.
11. M. Bellare and P. Rogaway, “Random oracles are practical: a paradigm for designing efficient protocols”, *Proc. of the 1st ACM Conference on Computer and Communications Security CCS’93*, ACM press, pp. 62-73, 1993.
12. V. I. Nechaev, “Complexity of a determinate algorithm for the discrete logarithm,” *Math.* Notes 55, pp. 165-172, 1994.

13. V. Shoup, “Lower bounds for discrete logarithms and related problems,” *Advances in Cryptology-EUROCRYPT’97*, LNCS 1233, pp. 256-266, 1997.

14. C. P. Schnorr, “Small generic hardcore subsets for the discrete logarithm: short secret DL-Keys,” *Information and Processing Letters*, Vol. 79, pp. 93-98, 2001.

15. C. P. Schnorr and M. Jakobsson, “Security of signed ElGamal Encryption,” *Advances in Cryptology-ASIACRYPT 2000*, LNCS 1976, pp. 73-89, 2000.

16. A. Juels, M. Luby and R. Ostrovsky, “Security of blind digital signatures,” *Advances in Cryptology-CRYPTO’97*, LNCS 1294, pp. 150-164, 1997.

17. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, pp. 617-627, 1996.