Efficient Partially Blind Signature Scheme with Provable Security*

Zheng Gong, Xiangxue Li, and Kefei Chen

Department of Computer Science and Engineering
Shanghai Jiaotong University, Shanghai, 200030, China
{neoyan, xxli, kfchen}@sjtu.edu.cn

Abstract. Partially blind signature was first introduced by Abe and Fujisaki. Subsequently, Abe and Okamoto proposed a provably secure construction for partially blind signature schemes with a formalized definition in their work. In this paper, based on discrete logarithm problem and the Schnorr's blind signature scheme, we propose a new efficient partially blind signature scheme. Follow the construction proposed by Abe and Okamoto, we prove its security in random oracle model. The computation and communication costs are both reduced in our scheme. It will make privacy-oriented applications which based on partially blind signatures more efficient and suitable for hardware-limited environment, such as smart phones and PDAs.

1 Introduction

Blind signature schemes, first introduced by Chaum in [1], allow a user to get a signature without giving the signer any information about the actual message. The signer also can't have a link between the users and the signatures. It's a useful property in privacy oriented e-services such as electronic cash and electronic voting system. However, it may not a good idea to blind everything in the e-cash system[2]. As to prevent a customer's double-spending, the bank has to keep a spent database which stores all spent e-cash to check whether a specified e-cash has been spent or not. Certainly, the spent database kept by the bank may grow unlimitedly. The other problem is to believe the face value of e-cash in the withdraw phase, the signer must assure that the message contains accurate information without seeing it.

Partially blind signature scheme proposed in [2] helps to solve the problems stated above. The scheme allows each of signatures contains an explicit information which both the signer and the user have agreed on. For example, the signer can attach the expiry date and denomination to his blind signatures as an attribute. Accordingly, The attribute of the signatures can be verified independently through those of the certified public key.

Based on different hard problem assumptions, many partially blind signature schemes have been given. The schemes proposed in [2,3,4] are based on RSA

* This work is partially supported by NSFC under the grants 90104005 and 60573030.

D.Z. Chen and D.T. Lee (Eds.): COCOON 2006, LNCS 4112, pp. 378–386, 2006.

algorithm, but the scheme in [2] does not have randomization property, which is important to withstand the chosen plaintext attack[5], and the scheme in [3] was also showed vulnerability on the chosen plaintext attack by [6]. The schemes proposed in [7,8,9] are based on discrete logarithm problem and [9] costs lower computation than [2,10]. The proposed partially blind signature schemes in [10,11] are based on the theories of quadratic residues, and the scheme [11] makes better performance than [10], but the signing protocol in [11] will give two valid signatures corresponding to the same message. The schemes proposed in [12,13] are based on bilinear pairings, but their verification of the signature require pairing operation, which is several times slower than modular exponentiation computation and not suitable for hardware-limited situations in client side, such as smart phones and PDAs.

Our Contribution. Considering both security and efficiency, based on discrete logarithm problem and the blind signature scheme in [14], we propose a new efficient partially blind signature scheme. Follow the construction that given in [7], we prove its security in random oracle model (ROM)[15]. Compared to the schemes in [4,7,9], the computation and communication costs for the user and the signer are both reduced in our scheme.

Organization. The rest of the paper is organized as follows. Section 2 describes the basic definitions associated with partially blind signatures. In section 3, we describe our efficient partially blind signature scheme, and then prove its security in section 4 and compare the performance of the proposed scheme with others related schemes in section 5. Section 6 concludes the paper.

2 Definitions

Abe and Okamoto introduced the notion of partially blind signatures in [7]. For the following provable security, We give the definitions proposed in [8] which provided a compact definitions based on [7]. In the phase of partially blind signatures, the signer and the user are assumed to have agreed on a piece of common information, denoted by **info**. An **info** may be sent from the user to the signer. The paper [7] formalized this notion by providing a function Ag. Function Ag is defined as a polynomial-time deterministic algorithm that completes the negotiation of **info** between the signer and the user correctly. In our scheme, this negotiation is considered to be done outside of the scheme.

Definition 1. ***(Partially Blind Signature Scheme)*** *A partially blind signature scheme is a four-tuple*$(\mathcal{G}, \mathcal{S}, \mathcal{U}, \mathcal{V})$.

- $\mathcal{G}$ *is a probabilistic polynomial-time algorithm, that takes security parameter* k *and outputs a public and secret key pair*(pk, sk).
- $\mathcal{S}$ *and* $\mathcal{U}$ *are pair of probabilistic interactive Turing machines each of which has a public input tape, a private input tape, a private random tape, a private word tape, a private output tape, a public output tape, and input and output communication tapes. The random tape and the input tapes are read-only,*

and the output tapes are write-only. The private work tape is read-write. The public input tape of $\mathcal{U}$ *contains* pk *generated by* $\mathcal{G}(1^k)$*, the description of* Ag*, and* $\mathbf{info}_u$*. The public input tape of* $\mathcal{S}$ *contains the description of* Ag *and* $\mathbf{info}_s$*. The private input type of* $\mathcal{S}$ *contains* sk*, and that for* $\mathcal{U}$ *contains a message* msg*. The lengths of* $\mathbf{info}_s$*,* $\mathbf{info}_u$*, and* $\mathbf{msg}$ *are polynomial in* k*.* $\mathcal{S}$ *and* $\mathcal{U}$ *engage in the signature issuing protocol and stop in polynomial-time. When they stop, the public output tape of* $\mathcal{S}$ *contains either completed or not-completed. If it is completed, then its private output tape contains common information* $\mathbf{info}$*. Similarly, the private output tape of* $\mathcal{U}$ *contains either* $\perp$ *or* $(\mathbf{info}, \mathbf{msg}, \mathbf{sig})$*.*

- $\mathcal{V}$ *is a polynomial-time algorithm.* $\mathcal{V}$ *takes* $(pk, \mathbf{info}, \mathbf{msg}, \mathbf{sig})$ *and outputs either accept or reject.*

Definition 2. ***(Partial Blindness)****Let* $\mathcal{U}_0$ *and* $\mathcal{U}_1$ *be two honest users that follow the signature issuing protocol. Let* $\mathcal{S}^*$ *play the following Game A in the presence of an independent umpire.*

1. $(pk, sk) \leftarrow \mathcal{G}(1^k)$.
2. $(\mathbf{msg}_0, \mathbf{msg}_1, \mathbf{info}_{u_0}, \mathbf{info}_{u_1}, Ag) \leftarrow \mathcal{S}^*(1^k, pk, sk)$.
3. *The umpire sets up the input tapes of* $\mathcal{U}_0$*,* $\mathcal{U}_1$ *as follows:*
   - *The umpire selects* $b \in_R \{0,1\}$ *and places* $\mathbf{msg}_b$ *and* $\mathbf{msg}_{1-b}$ *on the private input tapes of* $\mathcal{U}_0$ *and* $\mathcal{U}_1$*, respectively.* b *is not disclosed to* $\mathcal{S}^*$*.*
   - *Place* $\mathbf{info}_{u_0}$ *and* $\mathbf{info}_{u_1}$ *on the public input tapes of* $\mathcal{U}_0$ *and* $\mathcal{U}_1$ *respectively. Also place* pk *and* Ag *on their public input tapes.*
   - *Randomly select the contents of the private random tapes.*
4. $\mathcal{S}^*$ *engages in the signature issuing protocol with* $\mathcal{U}_0$ *and* $\mathcal{U}_1$ *in a parallel and arbitrarily interleaved fashion. If either signature issuing protocol fails to complete, the game is aborted.*
5. *Let* $\mathcal{U}_0$ *and* $\mathcal{U}_1$ *output* $(\mathbf{msg}_b, \mathbf{info}_0, \mathbf{sig}_b)$ *and* $(\mathbf{msg}_{1-b}, \mathbf{info}_1, \mathbf{sig}_{1-b})$*, respectively, on their private tapes. If* $\mathbf{info}_0 \neq \mathbf{info}_1$ *holds, then the umpire provides* $\mathcal{S}^*$ *with the no additional information. That is, the umpire gives* $\perp$ *to* $\mathcal{S}^*$*. If* $\mathbf{info}_0 = \mathbf{info}_1$ *holds, then the umpire provides* $\mathcal{S}^*$ *with the additional inputs* $\mathbf{sig}_b, \mathbf{sig}_{1-b}$ *ordered according to the corresponding messages* $\mathbf{msg}_0, \mathbf{msg}_1$*.*
6. $\mathcal{S}^*$ *outputs* $b' \in_R \{0,1\}$*. The signer S. wins the game if* $b' = b$*.*

A signature scheme is partially blind if, for every constant $c > 0$*, there exists a bound* k_0 *such that for all probabilistic polynomial-time algorithm* $\mathcal{S}^*$*,* $\mathcal{S}^*$ *outputs* $b' = b$ *with probability at most* $1/2 + 1/k^c$ *for* $k > k_0$*. The probability is taken over the coin flips of* $\mathcal{G}$*,* $\mathcal{U}_0$*,* $\mathcal{U}_1$*, and* $\mathcal{S}^*$*.*

Definition 3. ***(Unforgeability)****Let* $\mathcal{S}$ *be an honest signer that follow the signature issuing protocol. Let* $\mathcal{U}^*$ *play the following Game B in the presence of an independent umpire.*

1. $(pk, sk) \leftarrow \mathcal{G}(1^k)$.
2. $Ag \leftarrow \mathcal{U}^*(pk)$.

3. *The umpire places sk, Ag and a randomly taken* $\mathbf{info}_s$ *on the proper input tapes of* $\mathcal{S}$.
4. $\mathcal{U}^*$ *engages in the signature issuing protocol with* $\mathcal{S}$ *in a concurrent and interleaving way. For each* **info**, *let* $\ell_{\mathbf{info}}$ *be the number of executions of the signature issuing protocol where* $\mathcal{S}$ *outputs completed and* **info** *is on its output tapes. (For* **info** *that has never appeared on the private output tape of* $\mathcal{S}$, *define* $\ell_{\mathbf{info}} = 0$.*)*
5. $\mathcal{U}^*$ *outputs a single piece of common information,* **info**, *and* $\ell_{\mathbf{info}} + 1$ *signatures* $(\mathbf{msg}_1, \mathbf{sig}_1), \cdots, (\mathbf{msg}_{\ell_{\mathbf{info}}+1}, \mathbf{sig}_{\ell_{\mathbf{info}}+1})$.

A partially blind signature scheme is unforgeable if, for any probabilistic polynomial-time algorithm $\mathcal{U}^*$ *that plays the above game, the probability that the output of* $\mathcal{U}^*$ *satisfies*

$$\mathcal{V}(pk, \mathbf{info}, \mathbf{msg}_j, \mathbf{sig}_j) = accept$$

for all $j = 1, \cdots, \ell_{\mathbf{info}} + 1$ *is at most* $1/k^c$ *where* $k > k_0$ *for some bound* k_0 *and some constant* $c > 0$. *The probability is taken over the coin flips of* $\mathcal{G}$, $\mathcal{U}^*$, *and* $\mathcal{S}$.

Definition 4. ***(DLP (Discrete Logarithm Problem)):*** *For* $x, g \in_R \mathbb{Z}_p$, *given* $y = g^x (\mathrm{mod}\ p)$, *compute* $x = \log_g y$. *We assume that DLP is hard, which mean there is no polynomial time algorithm to solve it with non-negligible probability.*

3 The Proposed Partially Blind Signature Scheme

The proposed efficient partially blind signature scheme is based on the theories of DLP. Our scheme consists of five phases: **Initialization**, **Requesting**, **Signing**, **Extraction** and **Verifying**, as described below.

1. **Initialization.** Signer $\mathcal{S}$ selects two large prime numbers p and q(typical length: $|p| = 1024$, $|q| = 160$), which satisfied $q|p-1$. Then chooses a generator $g \in \mathbb{Z}_p, g^q \equiv 1 (\mathrm{mod}\ p)$. $\mathcal{S}$ picks up a random number $x \in \mathbb{Z}_q$, computes corresponding $y = g^x (\mathrm{mod}\ p)$. $a \parallel b$ denotes a concatenates b. $\mathcal{H}, \mathcal{F}, : \{0,1\}^* \mapsto \mathbb{Z}_q$ defined as two public hash functions. M is an arbitrary message space. The public key of $\mathcal{S}$ is the tuple (y, p, q, g), x is the private key.
2. **Requesting.** Assume that User $\mathcal{U}$ wants to get a partially blind signature on message $\mathbf{msg} \in M$, and then prepares a string $\mathbf{info} \in M$ that will be sent to $\mathcal{S}$ for his agreement, this negotiation is considered to be done outside of the scheme. Then $\mathcal{S}$ selects two random numbers $r, d \in_R \mathbb{Z}_q$, computes $z = \mathcal{F}(\mathbf{info})$, then submits $u = g^r z^d (\mathrm{mod}\ p)$ to $\mathcal{U}$.

   After receiving u, $\mathcal{U}$ also selects three random numbers $v, w, e \in_R \mathbb{Z}_q$, computes $z = \mathcal{F}(\mathbf{info})$ and $b = z^e (\mathrm{mod}\ p)$. Then computes $C' = \mathcal{H}(\mathbf{msg}||\mathbf{info}||t)$ while $t = ubg^v y^w (\mathrm{mod}\ p)$, sends $C = w - C'$ to $\mathcal{S}$.

3. **Signing.** After receiving C, $\mathcal{S}$ Signs C with the randomizing factor r and his private key x, computes $S = r + (C - z)x (\text{mod } q)$. Then $\mathcal{S}$ sends the other randomizing number d and S to $\mathcal{U}$.
4. **Extraction.** After receiving S and d, $\mathcal{U}$ computes $S' = S + v (\text{mod } q)$ and $N = d + e (\text{mod } q)$. Hence, the resulting signature on the message **msg** and the common information **info** is a tuple $(\mathbf{msg}, \mathbf{info}, S', C', N)$.
5. **Verifying.** For the signature $(\mathbf{msg}, \mathbf{info}, S', C', N)$, because

$$S' = S + v, S = r + (C - z)x$$

and

$$C = w - C', C' = \mathcal{H}(\mathbf{msg}||\mathbf{info}||t),$$

we can easily get

$$\begin{aligned} g^{S'} y^{z+C'} z^N &= z^{e+d} g^v g^{r+(C-z)x} y^{z+C'} (\text{mod } p) \\ &= ubg^v y^{C-z} y^{z+C'} (\text{mod } p) \\ &= ubg^v y^{C+C'} = ubg^v y^w = t (\text{mod } p). \end{aligned}$$

Hence, we have the equation

$$\mathcal{H}(\mathbf{msg}||\mathbf{info}||g^{S'} y^{z+C'} z^N (\text{mod } p)) = \mathcal{H}(\mathbf{msg}||\mathbf{info}||t) = C'.$$

The partially blind signature is accepted as valid if it satisfies the above equation.

4 Security

In this section, we discuss some security properties of our partially blind signature scheme based on assuming the intractability of the DLP.

4.1 Randomization

Theorem 1. *Given a response S produced by Signer $\mathcal{S}$, user $\mathcal{U}$ cannot remove the random factor r from S in polynomial time.*

Proof. In the scheme, $\mathcal{S}$ selects a large integers r and computes $u = g^r (\text{mod } p)$, and submits u to $\mathcal{U}$. Then $\mathcal{U}$ sends C to $\mathcal{S}$, and $\mathcal{S}$ returns $S = r + (C - z)x$. If $\mathcal{U}$ wants to remove r from the corresponding signature S, he must derive the unique pair (x, r) from (y, u). However, it is difficult for $\mathcal{U}$ to determine (x, r) because the derivation is DLP. Hence, in the proposed scheme, $\mathcal{U}$ cannot remove the random large integer r from the corresponding signature S of **msg**. □

4.2 Partial Blindness

Due to the **Definition 2**, for each instance numbered i of the proposed scheme, signer $\mathcal{S}^*$ can record C_i received from $\mathcal{U}$ who communicates with $\mathcal{S}^*$ during the instance i of the scheme. The tuple (S_i, C_i, r_i, d_i) is usually referred to as the view of $\mathcal{S}^*$ to the instance i of the scheme. Thus, we have the following theorem.

Theorem 2. *The proposed scheme is partially blind.*

Proof. Since the tuple $(\mathbf{msg}, \mathbf{info}, S', C', N)$ is produced, we have $S' = S_i + v, C' = w - C_i, N = d_i + e$ and $S_i = r_i + (C_i - z)x$. From the view of $\mathcal{S}^*$, Since v, w, e are three random numbers selected by $\mathcal{U}$ from $\mathbb{Z}_q$ and $\mathcal{S}^*$ cannot know v, w, e. The existence of a random triplet (v, w, e) that protects (S', C', N). Hence $\mathcal{S}^*$ can derive (v, w, e) from each view(S_i, C_i, r_i, N_i) such that $C_i = w - C'$,$C' = \mathcal{H}(\mathbf{msg}||\mathbf{info}||g^{S'}y^{z+C'}z^N(\text{mod } p))$ is satisfied where (S_i, C_i, r_i, N_i) regard as (S, C, r, N). When the instance $i \mapsto \{0, 1\}$, therefore, even an infinitely powerful $\mathcal{S}^*$ can succeed in determining i with probability $1/2$. □

From the proof of **Theorem 2**, we can know the importance of random factors v, w, e. $\mathcal{U}$ must reselect v, w, e in a new instance of the proposed scheme and protect factors v, e as a secret during the proceeding of the scheme. The random factors v, w, e must be destroyed after the signature $(\mathbf{msg}, \mathbf{info}, S', C', N)$ is created.

4.3 Unforgeability

From **Definition 3**, we analyze the successful forgery with following the same security argument given by Abe and Okamoto in [7]. Let us consider two types of forgery against the partially blind signature.

1. A user $\mathcal{U}^*$ can generate a valid partially blind signature while $\ell_{\mathbf{info}} = 0$.
2. Given a large number of valid partially blind signatures$(0 < \ell_{\mathbf{info}} < poly(\log\ n))$, $\mathcal{U}^*$ can extract a new valid signature.

Theorem 3. *The proposed scheme is unforgeable in the situation of type 1.*

Proof. We assume a successful forger $\mathcal{U}^*$ who plays Game B and produces a valid signature $(\mathbf{msg}, \mathbf{info}, S', C', N)$ with probability $\mu > 1/k^c$, such that $\ell_{\mathbf{info}} = 0$. By exploiting $\mathcal{U}^*$, we construct a machine $\mathcal{M}$ that forges the non-blind signature of the proposed scheme in a passive environment. $\mathcal{M}$ simulates random oracles $\mathcal{F}$ and $\mathcal{H}$.

Let q_F and q_H be the maximum number of queries that $\mathcal{U}^*$ asked from $\mathcal{F}$ and $\mathcal{H}$, respectively. Let q_S be the maximum number of queries of signer $\mathcal{S}$. Selects $i \in \{1, 2, \cdots, q_H + q_S\}$, $\mathcal{U}^*$ sends the tuple $(\mathbf{msg}_i, \mathbf{info}_i, t_i)$ to the oracle $\mathcal{H}$ for computing its hash value $\mathcal{H}(\mathbf{msg}_i||\mathbf{info}_i||t_i)$. Simultaneously, $\mathcal{U}^*$ asks $\mathcal{F}$ to get $z = \mathcal{F}(\mathbf{info})$. $\mathcal{F}$ returns $z_i = g^{\omega_i}(\text{mod } p)$, where $w_i \in_R \mathbb{Z}_q$. $\mathcal{M}$ knows ω_i from each pair of (z_i, ω_i) in $\mathcal{F}$. All of the parameters are limited by a polynomial in k. As the same proof construction in [7], we can easily know the success probability of $\mathcal{M}$ which is denoted by μ'.

$$\mu' = \frac{\mu}{(q_H + q_S)(q_F + q_S)}.$$

Then we use $\mathcal{M}$ to solve DLP. From the above construction. $\mathcal{M}$ can get a valid signature tuple (t_1, S_1', C_1', N_1) in polynomial running time after $1/\mu'$

trials, with probability at least $1 - e^{-1}$(here, e is base of natural logarithms). Because $\mathcal{U}^*$ only can get hash value from $\mathcal{H}$. Next, we use the standard replay technique [16,17]. That is, we repeat with the same random tape and a different choice of $\mathcal{H}$, we can get another valid signature (t_2, S_2', C_2', N_2) after $2/\mu'$ trials, with probability at least $(1 - e^{-1})/2$, and we have $t_1 = t_2$. From the equation $C' = \mathcal{H}(\mathbf{msg}||\mathbf{info}||g^{S'}y^{z+C'}z^N(\text{mod } p))$, we have

$$S_1' + (C_1' + z_1) \cdot x + \omega_1 \cdot N_1 = S_2' + (C_2' + z_2) \cdot x + \omega_2 \cdot N_2.$$

Since $\mathcal{H}$ was changed choice in the second time run, both $S_1' \neq S_2'$ and $C_1' \neq C_2'$ have a overwhelming probability in $1 - 2^{-k}$, $\mathcal{M}$ can get x from

$$x = \frac{(S_2' - S_1') + (\omega_2 \cdot N_2 - \omega_1 \cdot N_1)}{(C_1' - C_2') + (z_1 - z_2)} (\text{mod } q).$$

It means $\mathcal{M}$ can solve DLP in polynomial running time. □

Next we consider the forgery attempts in situation of type 2. We prove the security of our scheme where the common information is not all the same in Game B.

Theorem 4. *The proposed scheme is unforgeable in the situation of type 2.*

Proof. We assume a successful forger $\mathcal{U}_f^*$ who wins Game B with a probability η, which is a non-negligible in polynomial running time. Then we construct an machine $\mathcal{M}$ that simulates the signer in Game B. Let $\hat{S}$ denote the signer simulated by $\mathcal{M}$. $\mathcal{M}$ simulates two random oracles $\mathcal{F}$ and $\mathcal{H}$. $\mathcal{F}$ returns $z_i = g^{\omega_i}(\text{mod } p)$, where $\omega_i \in_R \mathbb{Z}_q$. We assume $\mathcal{M}$ don't know ω_i this time. $\mathcal{M}$ uses $\mathcal{U}_f^*$ as a black-box and breaks the intractability assumption of DLP to compute ω such that $z = g^{\omega}(\text{mod } p)$.

After $\ell_{\mathbf{info}}$ times execution with $\hat{S}$, $\mathcal{U}_f^*$ has got a set of successful challenge tuple $(\mathbf{msg}_1, \mathbf{info}_1, \mathbf{t}_1), (\mathbf{msg}_2, \mathbf{info}_2, \mathbf{t}_2), \cdots, (\mathbf{msg}_{\ell_{\mathbf{info}}}, \mathbf{info}_{\ell_{\mathbf{info}}}, \mathbf{t}_{\ell_{\mathbf{info}}})$. $\mathcal{U}_f^*$ sends the tuple $(\mathbf{msg}_i, \mathbf{info}_i, t_i)$ to the random oracle $\mathcal{H}$ for computing its hash value $\mathcal{H}(\mathbf{msg}_i||\mathbf{info}_i||t_i)$.

From the above construction, $\mathcal{U}_f^*$ can win Game B and forge a valid signature with a successful challenge tuple $(\mathbf{msg}_{\ell_{\mathbf{info}}+1}, \mathbf{info}_{\ell_{\mathbf{info}}+1}, \mathbf{t}_{\ell_{\mathbf{info}}+1})$ after $1/\eta$ trails, with probability at least $1 - e^{-1}$. First we consider the situation that there exists $i \in \{1, 2, \cdots, \ell_{\mathbf{info}}\}$, $\mathbf{msg}_i = \mathbf{msg}_{\ell_{\mathbf{info}}+1}$, $\mathbf{info}_i = \mathbf{info}_{\ell_{\mathbf{info}}+1}$ and $t_i = t_{\ell_{\mathbf{info}}+1}$. Because $\mathcal{U}^*$ only can get hash value from $\mathcal{H}$, We have

$$g^{S'_{\ell_{\mathbf{info}}+1}} y^{C'_{\ell_{\mathbf{info}}+1}} z^{N_{\ell_{\mathbf{info}}+1}} = g^{S_i'} y^{C_i'} z^{N_i}$$

such that

$$S'_{\ell_{\mathbf{info}}+1} + N_{\ell_{\mathbf{info}}+1} \cdot \omega = S_i' + N_i \cdot \omega.$$

Hence, we can compute ω from

$$\omega = \frac{S'_{\ell_{\mathbf{info}}+1} - S_i'}{N_{\ell_{\mathbf{info}}+1} - N_i} (\text{mod } q).$$

Then we consider the situation that there does not exist $i \in \{1, 2, \cdots, \ell_{\mathbf{info}}\}$, $\mathbf{msg}_i = \mathbf{msg}_{\ell_{\mathbf{info}}+1}$, $\mathbf{info}_i = \mathbf{info}_{\ell_{\mathbf{info}}+1}$ and $t_i = t_{\ell_{\mathbf{info}}+1}$. This derives to the same forgery attempts in the situation of type 1. □

From **Theorem 3** and **Theorem 4**, we have the following theorem.

Theorem 5. *The proposed scheme is unforgeable if* $\ell_{\mathbf{info}} < poly(\log\ n)$ *for all* **info**.

5 Performance Concerns

We will discuss the performance of the proposed scheme from the costs of communication and computation. Table 1 gives us a detail costs comparison amongst related partially blind signature schemes[4,7,9]. The techniques to perform the modular exponentiation computation are not used because they need additional storage, which is limited in some application environments.

Table 1. The Comparisons of the partially blind signature schemes

	Our Scheme	Abe00 [7]	Huang03 [9]	Cao05 [4]
Mathematical foundation	DLP	DLP	DLP/CRT	RSA
Signer's computation	$2T_e + 1T_m$	$3T_e + 2T_m$	$2T_e + 4T_m$	$2T_e + 2T_m + T_i$
User's computation	$3T_e + 3T_m$	$4T_e + 4T_m$	$4T_e + 2T_m$	$3T_e + 5T_m$
Verifier's computation	$3T_e + 2T_m$	$4T_e + 2T_m$	$5T_e + 3T_m$	$3T_e + 2T_m$
Signature size	$2\|m\| + 3\|q\|$	$2\|m\| + 4\|q\|$	$2\|m\| + 3\|n\|$	$2\|m\| + 2\|n\|$

*T_e: time for one exponentiation computation; T_m: time for one multiplication computation; T_i: time for one inverse computation; Typical length: $|q| = 160bit$, $|n| = 1024bit$.

With regard to estimate the computational costs, we count only modular exponentiation and multiplication. An inverse computation demands the same amount of computation as a modular exponentiation. We also do not calculate the computational costs on hash operations because it is much more faster than modular exponentiation computation, and each schemes takes nearly same times of hash operation. By Table 1, from the computational costs and signature sizes, our scheme all shows more efficient than the schemes in [4,7,9].

6 Conclusion

In this paper, we proposed an efficient partially blind signature scheme based on DLP and the Schnorr's blind signature scheme, and we proved its security in ROM. The computation and communication costs are both reduced in our scheme. It will makes privacy oriented applications which based on partially blind signatures more efficient and suitable for hardware-limited environment, such as smart phones and PDAs.

References

1. D.Chaum. Blind signature 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. H.Y. Chien, J.K. Jan, Y.M. Tseng. RSA-based partially blind signature with low computation. *In: Proceedings of the eighth international conference on parallel and distributed systems*, pp.385-389, 2001.
4. T.J. Cao et al. A randomized RSA-based partially blind signature scheme for electronic cash, *Computers & Security*. Vol:24, Issue:1, pp.44-49, 2005.
5. A. Shamir and C.P. Schnorr. Cryptanalysis of certain variants of Rabin's signature scheme. *Information proceeding Letters*, vol.19, pp.113-115, 1984.
6. M.S Kwon and Y.K Cho. Randomization enhanced blind signature schemes based on RSA. *IEICE A Fundam 2003*; E86-A(3); 730-3, 2003.
7. M.Abe and T.Okamoto. Provably secure partially blind signatures, *Advance in Cryptology-CRYPTO'00*, LNCS 1880, pp.271-286, 2000.
8. G.Maitland and C.Boyd. A provably secure restrictive partially blind signature scheme, *PKC 2002*, LNCS 2274, pp.99-114, 2002.
9. H.F. Huang and C.C Chang. A new design of efficient partially blind signature scheme, *Journal of Systems and Software*, Vol: 73, Issue: 3, pp.397-403, 2003.
10. C.I. Fan and C.L. Lei. Low-computation partially blind signatures for electronic cash. *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, E81-A(5)818-824, 1998.
11. C.I. Fan. Improved low-computation partially blind signatures . *Applied Mathematics and Computation*, Vol: 145, Issue:2-3, pp. 853-867, 2003.
12. Fangguo Zhang et al. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. *Cryptology - INDOCRYPT 2003*, LNCS 2904, pp. 191-204, 2003.
13. S.M. Sherman et al. Two Improved Partially Blind Signature Schemes from Bilinear Pairings. *ACISP 2005*, LNCS 3574, pp. 316-328, 2005.
14. C.P. Schnorr. Discrete log signatures against interactive attacks. *Information and Communications Security*, LNCS 2299, pp. 1-12, 2001.
15. M.Bellare and P.Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM CCS*, pp.62-73, 1993.
16. U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptography*. 1:77-94. 1988.
17. K. Ohta and T. Okamoto. On concrete security treatment of signatures derived from identification. In H. Krawczyk, editor, *Advances in Cryptology-Proceedings of CRYPTO'98*, LNCS 1462, pp.345-370. 1998.