Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings*

Xiaofeng Chen[1], Fangguo Zhang[2], Yi Mu[3], and Willy Susilo[3]

[1] Department of Computer Science,
Sun Yat-sen University, Guangzhou 510275, P.R. China
isschxf@mail.sysu.edu.cn
[2] Department of Electronics and Communication Engineering,
Sun Yat-sen University, Guangzhou 510275, P.R. China
isszhfg@mail.sysu.edu.cn
[3] School of Information Technology and Computer Science,
University of Wollongong, Australia
{ymu, wsusilo}@uow.edu.au

Abstract. Restrictive blind signatures allow a recipient to receive a blind signature on a message unknown to the signer but the choice of the message is restricted and must conform to certain rules. Partially blind signatures allow a signer to explicitly include necessary information (expiration date, collateral conditions, or whatever) in the resulting signatures under some agreement with the receiver. Restrictive partially blind signatures incorporate the advantages of these two blind signatures. In this paper we first propose a new restrictive partially blind signature scheme from bilinear pairings. Since the proposed scheme does not use Chaum-Pedersen's knowledge proof protocol, it is much more efficient than the original restrictive partially blind signature scheme. We then present a formal proof of security in the random oracle model. Moreover, we use the proposed signature scheme to build an untraceable off-line electronic cash system followed Brand's construction.

Keywords: Restrictive partially blind signatures, Bilinear pairings, Electronic cash.

1 Introduction

Blind signatures, introduced by Chaum [10], allow a recipient to obtain a signature on message m without revealing anything about the message to the signer. Blind signatures play an important role in a plenty of applications such as electronic voting, electronic cash where anonymity is of great concern.

A serious problem in electronic cash schemes is double-spending. On-line electronic cash scheme provides a possible solution against double-spending. However, it requires that the shop must contact the bank during each transaction.

* Supported by National Natural Science Foundation of China (No. 60503006 and 60403007) and ARC Discovery Grant DP0557493.

G. Di Crescenzo and A. Rubin (Eds.): FC 2006, LNCS 4107, pp. 251–265, 2006.

So the bank will soon become the bottleneck of the systems. Chaum [11] also proposed an off-line electronic cash scheme, which ensures the bank to trace the double-spenders after the fact. However, such a system is very inefficient due to the cut-and-choose protocol.

Restrictive blind signatures were first introduced by Brands [7,8], which allow a recipient to receive a blind signature on a message unknown to the signer but the choice of the message is restricted and must conform to certain rules. Furthermore, he proposed a highly efficient electronic cash system, where the bank ensures that the user is restricted to embed his identity in the resulting blind signature. Brand's electronic cash system has received wide attention for its distinguished characters. However, Brand's original restrictive blind signature scheme is mainly based on Chaum-Pedersen's interactive zero-knowledge proof of common exponent [12]. The communication cost is a little high and the length of the signature is a little too long.

Partially blind signatures, first introduced by Abe and Fujisaki [1], allow a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. This notion overcomes some disadvantages of fully blind signatures such as the signer has no control over the attributes except for those bound by the public key. Partial blind signatures play an important role in designing the efficient electronic cash system. For example, the bank does not require different public keys for different coin values. On the other hand, the size of the database that stored the previously spent coins to detect double-spending would not increase infinitely over time.

Maitland and Boyd [15] first incorporated these two blind signatures and proposed a provably secure restrictive partially blind signature scheme, which satisfies the partial blindness and restrictive blindness. Their scheme followed the construction proposed by Abe and Okamoto [2] and used Brand's restrictive blind signature scheme. Therefore, the scheme still uses Chaum-Pedersen's zero-knowledge proof of common exponent and this increases the communication cost and the length of the signature.

Our Contribution. In this paper we first propose a new restrictive blind signature scheme and a restrictive partially blind signature scheme from bilinear pairings, and the former can be regarded as a special case of the latter. Our blind signature schemes use the so-called gap Diffile-Hellman group [5,9,13], where Decisional Diffie-Hellman Problem (DDHP) can be solved in polynomial time but there is no polynomial time algorithm to solve Computational Diffie-Hellman Problem (CDHP) with non-negligible probability. So it is not required to use the inefficient zero-knowledge proof of common exponent to ensure the validity of a Diffie-Helllman tuple in our schemes. Compared to the original schemes, the advantages of our scheme are shorter length of the signature and lower communication complexity. Furthermore, we give a formal security proof for the proposed schemes in the random oracle model.

The rest of the paper is organized as follows: The definitions associated with restrictive partially blind signatures are introduced in Section 2. The proposed

restrictive blind signature scheme is given in Section 3. The proposed restrictive partially blind signature scheme is given in Section 4. Finally, conclusions will be made in Section 5.

2 Definitions

Juels, Luby and Ostrovsky [14] gave a formal definition of blind signatures. They proved the existence of secure blind signatures assuming the one-way trapdoor permutation family. Pointcheval and Stern [17] showed the security of a certain type of efficient blind signature in the random oracle model. Later, they [16,18] developed a generic approach that converts logarithmically secure schemes into polynomially secure ones at the cost of two more data transmissions between the signer and the receiver.

Abe and Okamoto first presented the formal definition of partially blind signatures. Restrictive partially blind signatures can be regarded as partially blind signatures which also satisfies the property of restrictiveness. In the context of partially blind signatures, the signer and user are assumed to agree on a piece of information, denoted by info. In real applications, info may be decided by the negotiation between the signer and user. For the sake of simplicity, we omit the negotiation throughout this paper. In the following, we follow the definitions of [2,14,7] to give a formal definition of restrictive partially blind signatures.

Definition 1. *(Restrictive Partially Blind Signatures) A restrictive partially blind signature scheme is a four-tuple* $(\mathcal{PG}, \mathcal{KG}, \mathcal{SG}, \mathcal{SV})$.

- **System Parameters Generation** $\mathcal{PG}$**:** *On input a security parameter* k*, outputs the common system parameters* Params.
- **Key Generation** $\mathcal{KG}$**:** *On input* Params*, outputs a public and private key pair* (pk, sk).
- **Signature Generation** $\mathcal{SG}$**:** *Let* U *and* S *be two probabilistic interactive Turing machines and each of them has a public input tape, a private random tape, a private work 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. Suppose* info *is agreed common information between* U *and* S*. The public input tape of* U *contains* pk *generated by* $\mathcal{G}(1^k)$*, and* info*. The public input tape of* S *contains* info*. The private input tape of* S *contains* sk*, and that for* U *contains a message* m *which he knows a representation with respect to some bases in* Params*. The lengths of* info *and* m *are polynomial to* k*.* U *and* S *engage in the signature issuing protocol and stop in polynomial-time. When they stop, the public output of* S *contains either completed or not-completed. If it is completed, the private output tape of* U *contains either* $\perp$ *or* $(\mathit{info}, m, \sigma)$.
- **Signature Verification** $\mathcal{SV}$**:** *On input* $(pk, \mathit{info}, m, \sigma)$ *and outputs either accept or reject.*

Definition 2. *(Completeness) If S and U follow the signature issuing protocol, the signature scheme is complete if, for every constant $c > 0$, there exists a bound k_0 such that S outputs completed and $\boldsymbol{info}$ on its proper tapes, and U outputs $(\boldsymbol{info}, m, \sigma)$ that satisfies*

$$\mathcal{SV}(\boldsymbol{info}, m, \sigma) = accept$$

with probability at least $1 - 1/k^c$ for $k > k_0$. The probability is taken over the coin flips of $\mathcal{KG}, S$ and U.

We say a message-signature tuple $(\boldsymbol{info}, m, \sigma)$ is valid with regard to pk if it leads to $\mathcal{SV}$ to accept.

Definition 3. *(Restrictiveness) Let m be a message such that the user U knows a representation $(a_1, \cdots, a_k)$ of m with respect to a generator-tuple $(g_1, \cdots, g_k)$ at the start of a blind signature issuing protocol. Let $(b_1, \cdots, b_k)$ be the representation U knows of the blinded number m' of m after the protocol finished. If there exist two function I_1 and I_2 such that*

$$I_1(a_1, \cdots, a_k) = I_2(b_1, \cdots, b_k)$$

regardless of m and the blinding transformation applied by U, then the protocol is called a restrictive blind signature protocol. The function I_1 and I_2 are called blinding-invariant functions of the protocol with respect to $(g_1, \cdots, g_k)$.

Definition 4. *(Partial Blindness) Let U_0 and U_1 be two honest users that follow the signature issuing protocol.*

1. $(pk, sk) \leftarrow \mathcal{KG}(\mathsf{Params})$.
2. $(m_0, m_1, \boldsymbol{info}_0, \boldsymbol{info}_1) \leftarrow S^*(1^k, pk, sk)$.
3. *Set up the input tapes of U_0 and U_1 as follows:*
   - *Select $b \in_R \{0, 1\}$ and put m_b and m_{1-b} on the private input tapes of U_0 and U_1, respectively.*
   - *Put $\boldsymbol{info}_0$ and $\boldsymbol{info}_1$ on the public input tapes of U_0 and U_1, respectively. Also put pk on their public input tapes.*
   - *Randomly select the contents of the private random tapes.*
4. *S^* engages in the signature issuing protocol with U_0 and U_1.*
5. *Let U_0 and U_1 output $(\boldsymbol{info}_0, m_b, \sigma_b)$ and $(\boldsymbol{info}_0, m_{1-b}, \sigma_{1-b})$, respectively, on their private tapes. If $\boldsymbol{info}_0 \neq \boldsymbol{info}_1$, then give $\perp$ to S^*. If $\boldsymbol{info}_0 = \boldsymbol{info}_1$, then provide S^* with the additional inputs (σ_b, σ_{1-b}) ordered according to the corresponding messages (m_b, m_{1-b}).*
6. *S^* outputs $b' \in \{0, 1\}$. We say that S^* wins 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 S^*, S^* outputs $b' = b$ with probability at most $1/2 + 1/k^c$ for $k > k_0$. The probability is taken over the flips of $\mathcal{KG}, U_0, U_1$, and S^*.

Definition 5. *(Unforgeability) Let S be an honest signer that follows the signature issuing protocol.*

1. $(pk, sk) \leftarrow \mathcal{KG}(\mathsf{Params})$.
2. *Put sk and* **info** *on proper tapes of S.*
3. *U^* engages in the signature issuing protocol with S in a concurrent and interleaving way. For each* **info**, *let $l_{\mathbf{info}}$ be the number of executions of the signature issuing protocol where S outputs completed and* **info** *on its output tapes. (For* **info** *that has never appeared on the private output tapes of S, define $l_{\mathbf{info}} = 0$.)*
4. *U^* outputs a single piece of common information,* **info**, *and $l_{\mathbf{info}}+1$ signatures $(m_1, \sigma_1), \cdots, (m_{l_{\mathbf{info}}+1}, \sigma_{l_{\mathbf{info}}+1})$.*

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

$$\mathcal{SV}(pk, \mathbf{info}, m_j, \sigma_j) = accept$$

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

3 Restrictive Blind Signatures from Pairings

In Brand's restrictive blind signature scheme, the Chaum-Pedersen's protocol must be used to provide a proof that $\log_g y = \log_m z$, *i.e.*, $< g, y, m, z >$ is a valid Diffie-Hellman tuple. We argue the knowledge proof can be avoided in the gap Diffie-Hellman (blind) signature scheme [6,3]. However, if we directly use the gap Diffie-Hellman blind signature scheme as a building block to design our restrictive blind signature scheme from pairings, there exists a cheating attack.[1] In this section, we first propose a variant of gap Diffie-Hellman blind signature scheme, the security of which is based on a variant of CDHP, named RCDHP, which is equivalent to CDHP. We then propose a restrictive blind signature scheme which is derived from the variant of gap Diffie-Hellman blind signature scheme and Brand's original blind signature scheme.

3.1 A Variant of Gap Diffie-Hellman Blind Signature Scheme

We firstly introduce a variant of CDHP in G which we call Reversion Computational Diffie-Hellman Problem (RCDHP).[2]

RCDHP: Given g, g^a and g^b, to compute g^c which satisfies $a \equiv bc \bmod q$.

[1] It is trivial to see that the user can get the signature $\tilde{\sigma} = \tilde{m}^x$ for any message $\tilde{m}$ with the signature $z = m^x$ for a message m. This will destroy the property of restrictiveness of the signature scheme. We argue that this attack can be avoidable if the form of z and $\tilde{\sigma}$ is different. For details, refer to section 3.2.

[2] We distinguish it with Inversion Computational Diffie-Hellman Problem: Given g and g^a, to compute $g^{a^{-1}}$.

Theorem 1. RCDHP *is equivalent to* CDHP *in* G.

Proof. Given (g, g^a, g^b), suppose we can solve RCDHP in G, then we can obtain $g^{b^{-1}}$ from g and g^b. Note $a = (ab)b^{-1} \bmod q$, we can compute g^{ab} from g^a and $g^{b^{-1}}$, *i.e.*, we can solve CDHP in G.

Given (g, g^a, g^b), let $h = g^b$, so $g = h^{b^{-1}}$. Suppose we can solve CDHP in G, so with h and $h^{b^{-1}}$ we can obtain $h^{b^{-2}}$, *i.e.*, $g^{b^{-1}}$. Then we can obtain $g^{ab^{-1}}$ from g^a and $g^{b^{-1}}$, *i.e.*, we solve RCDHP in G. □

In the following, we present a variant of Boneh *et al*'s signature scheme, the security of which is based on the assumption that RCDHP in G is intractable. The system parameters are the same as above.

Given the signed message m and the signer's secret key x, the signature on m is $\sigma = H(m)^{x^{-1}}$. Anyone can verify that $< g, y, \sigma, H(m) >$ is a valid Diffie-Hellman tuple.

Similarly, we can present the corresponding blind signature scheme based on the above variant of Boneh *et al*'s signature scheme.

- The user picks a random number $r \in_R Z_q^*$, and sends $\tilde{m} = H(m) \cdot y^r$ to the signer.
- The signer computes $\tilde{\sigma} = \tilde{m}^{x^{-1}}$ and sends it to the user.
- The user computes $\sigma = \tilde{\sigma} \cdot g^{-r}$.

If $< g, y, \sigma, H(m) >$ is a valid Diffie-Hellman tuple, then σ is a valid signature on message m.

3.2 The Proposed Restrictive Blind Signature Scheme

- **System Parameters Generation:** Given a security parameter k, let G_1 be a gap Diffie-Hellman group generated by g, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$. $H : G_1 \times G_1 \to G_1$ is a cryptographic hash function. The system parameters are $Params = \{G_1, G_2, e, q, g, k, H\}$.
- **Key Generation:** Let $(x, y = g^x)$ be the private and public key pair of the signer.
- **Signature Generation:** Let m be a message from the receiver.
  - The signer generates a random number $r \in_R Z_q$ and sends $z = m^{rx}$, $b = m^r$, and $a = y^r$ to the receiver.
  - The receiver checks whether $e(z, g) = e(b, y) = e(m, a)$. If not, he terminates the protocol. Else, he generates random numbers $\alpha, \lambda, u \in_R Z_q$ and computes

$$m' = m^\alpha, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}, a' = a^\lambda, \tilde{m} = H(m', z', b', a')y^u.$$

    The receiver then sends $\tilde{m}$ to the signer.
  - The signer responds with $\tilde{\sigma} = \tilde{m}^{x^{-1}}$ and the receiver computes $\sigma = \tilde{\sigma} g^{-u}$.

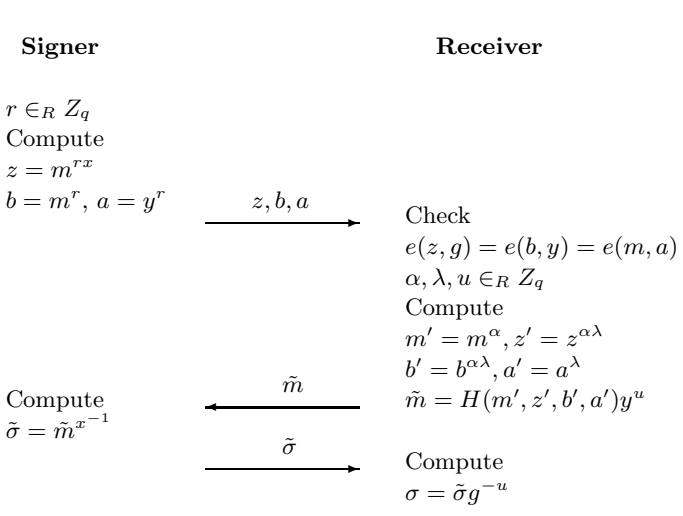

Fig. 1. Restrictive Blind Signature Scheme from Pairings

Thus, the receiver obtains a signature on the message m' where $m' = m^\alpha$ and α is chosen by the receiver.

– **Signature Verification:** (z', b', a', σ) is a valid signature on m' if the following equations hold:

$$e(\sigma, y) = e(H(m', z', b', a'), g);\ e(z', g) = e(b', y) = e(m', a').$$

3.3 Security Analysis of the Proposed Scheme

Theorem 2. *The proposed restrictive blind signature scheme achieves the properties of Correctness, Blindness, Restrictiveness.*

Proof. We show that our scheme satisfies all the security properties.

– *Correctness*: Firstly, note that $\sigma = \tilde{\sigma} g^{-u} = H(m', z', b', a')^{x^{-1}}$, we have $e(\sigma, y) = e(H(m', z', b', a'), g)$. Secondly, since $z' = z^{\alpha\lambda} = m^{rx\alpha\lambda}$, $b' = m^{r\alpha\lambda}$, and $a' = y^{r\lambda}$, so $e(z', g) = e(b', y) = e(m', a')$.

– *Blindness*: Let $(\tilde{m}, m, z, b, a, \tilde{\sigma})$ be any of the review of the protocol as seen by the signer. Therefore, $\tilde{\sigma} = \tilde{m}^{x^{-1}}$ and $e(z, g) = e(b, y) = e(m, a)$. Let (z', b', a', σ) be a valid signature on message m' obtained by the receiver. Choose the unique blinding factor $F = \tilde{\sigma}/\sigma$ and determine three representations $m' = m^\alpha, a' = a^\lambda, F = g^u$.[3] Note that $\sigma = H(m', z', b', a')^{x^{-1}}$ and $e(z', g) = e(b', y) = e(m', a')$ have been established by the fact that the blind signature is valid, therefore we have

$$\tilde{m} = \tilde{\sigma}^x = (\sigma F)^x = H(m', z', b', a')y^u, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}.$$

[3] Though it is difficult to compute (α, λ, u), we only need to exploit the existence of them.

– *Restrictiveness*: Similar to [7,15], the restrictiveness nature of the scheme can be captured by the following assumption: The recipient obtains a signature on a message that can only be the form $m' = m^{\alpha}$ with α randomly chosen by the receiver. In addition, if there exists a representation (μ_1, μ_2) of m with respect to bases g_1 and g_2 such that $m = g_1^{\mu_1} g_2^{\mu_2}$ and if there exists a representation (μ_1', μ_2') of m' with respect to g_1 and g_2 such that $m' = g_1^{\mu_1'} g_2^{\mu_2'}$, then the relation $I_1(\mu_1, \mu_2) = \mu_1/\mu_2 = \mu_1'/\mu_2' = I_2(\mu_1', \mu_2')$ holds. In the applications of an electronic cash system, a user chooses a random number u as his identification information and computes $m = g_1^u g_2$. He then with the bank performs the signature issuing protocol to obtain a coin. When spending the coin at a shop, the user must provide a proof that he knows a representation of m' with respect to base g_1 and g_2. This restricts m' must be the form of m^{α}. For more details, refer to [7]. □

4 Restrictive Partially Blind Signatures from Pairings

In this section, we firstly propose a concrete restrictive partially blind signature scheme from pairings based on [19,20]. The proposed restrictive blind signature scheme in section 3 can be regarded as a special case of it when $H_0(c)$ equals to 0. We then discuss the security and efficiency of the scheme under the assumption of ideal randomness of hash functions H and H_0. Finally, we describe an electronic cash system using the proposed signature scheme.

4.1 The Proposed Restrictive Partially Blind Signature Scheme

– **System Parameters Generation $\mathcal{PG}$:** Given a security parameter k. Let G_1 be a gap Diffie-Hellman group generated by g, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H : G_1 \times G_1 \times \{0,1\}^* \to G_1$, $H_0 : \{0,1\}^* \to Z_q$. The system parameters are $Params = \{G_1, G_2, e, q, g, k, H, H_0\}$.
– **Key Generation $\mathcal{KG}$:** On input $Params$, outputs the private and public key pair $(x, y = g^x)$ of the signer.
– **Signature Generation $\mathcal{SG}$:** Let the shared information $\boldsymbol{info} = c$, and the signed message be $m' = m^{\alpha}$, where α is a value chosen by the receiver.
  • The signer generates a random number $r \in_R Z_q$ and sends $z = m^{rx}$, $b = m^r$, and $a = y^r$ to the receiver.
  • The receiver checks whether $e(z, g) = e(b, y) = e(m, a)$. If not, he terminates the protocol. Else, he generates random numbers $\alpha, \lambda, u \in_R Z_q$ and computes

$$m' = m^{\alpha}, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}, a' = a^{\lambda}, \tilde{m} = H(m', z', b', a', c)(g^{H_0(c)} y)^u.$$

    The receiver then sends $\tilde{m}$ to the signer.
  • The signer responds with $\tilde{\sigma} = \tilde{m}^{\frac{1}{H_0(c)+x}}$ and the receiver computes $\sigma = \tilde{\sigma} g^{-u}$.

The resulting signature for the shared information c and message m' is (z', b', a', σ).

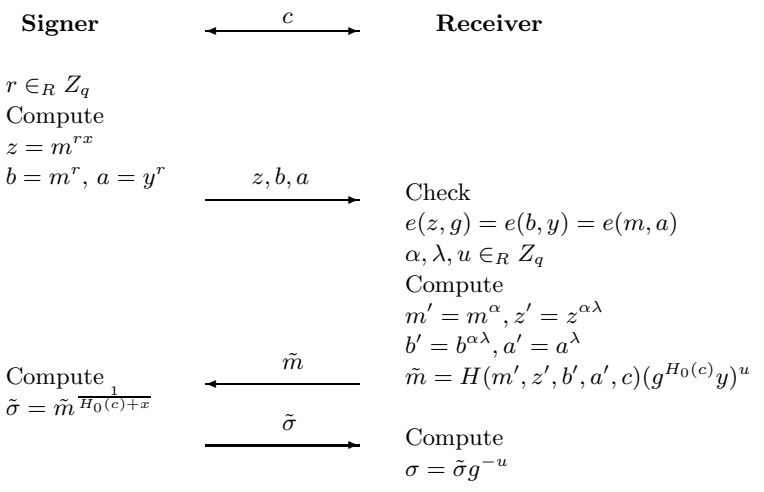

Fig. 2. Restrictive Partially Blind Signature Scheme from Pairings

– **Signature Verification $\mathcal{SV}$:** (z', b', a', σ) is a valid signature on c and m' if the following equations hold:

$$e(\sigma, g^{H_0(c)}y) = e(H(m', z', b', a', c), g);\ e(z', g) = e(b', y) = e(m', a').$$

4.2 Security Analysis of the Proposed Scheme

Theorem 3. *The proposed scheme achieves the property of completeness.*

Proof

$$\begin{aligned} e(\sigma, g^{H_0(c)}y) &= e(\tilde{\sigma}g^{-u}, g^{H_0(c)}y) = e(\tilde{m}^{\frac{1}{H_0(c)+x}}g^{-u}, g^{H_0(c)}y) \\ &= e(H(m', z', b', a', c)^{\frac{1}{H_0(c)+x}}, g^{H_0(c)}y) \\ &= e(H(m', z', b', a', c), g) \\ e(z', g) &= e(m^{rx\alpha\lambda}, g) = e(b', y) = e(m^\alpha, g^{rx\lambda}) = e(m', a') \end{aligned}$$

Theorem 4. *The proposed scheme achieves the property of restrictiveness.*

Proof. It is same to Theorem 2. □

Theorem 5. *The proposed scheme achieves partial blindness.*

Proof. Suppose S^* is given $\perp$ in step 5 of the game in definition 4, S^* determines b with a probability $1/2$ (the same probability as randomly guessing b).

Suppose that in step 5, the shared information $c_0 = c_1$. Let (z', b', a', σ, m') be one of the signatures subsequently given to S^*. Let $(z, b, a, \tilde{m}, \tilde{\sigma}, m, c)$ be data appearing in the view of S^* during one of the executions of the signature issuing protocol at step 4. Therefore, $\tilde{\sigma} = \tilde{m}^{\frac{1}{H_0(c)+x}}$ and $e(z, g) = e(b, y) = e(m, a)$.

It is sufficient to show that there exists a tuple of random blinding factors (α, λ, u) that maps $(z, b, a, \tilde{m}, \tilde{\sigma}, m)$ to (z', b', a', σ, m'). Suppose $m' = m^\alpha, a' = a^\lambda$, and $F = \tilde{\sigma}/\sigma = g^u$.[4] Note that $\sigma = H(m', z', b', a', c)^{\frac{1}{H_0(c)+x}}$ and $e(z', g) = e(b', y) = e(m', a')$ have been established by the fact the signature is valid. Therefore, we have

$$\tilde{m} = \tilde{\sigma}^{H_0(c)+x} = (\sigma F)^{H_0(c)+x} = H(m', z', b', a', c)(g^{H_0(c)}y)^u, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}.$$

Thus, the blinding factors which lead to the same relation defined in the signature issuing protocol always exist. Therefore, even an infinitely powerful S^* succeeds in determining b with probability $1/2$. □

Theorem 6. *The proposed scheme is unforgeable if $l_{info} < poly(\log k)$ for all $info$.*

Proof. The proof follows the security argument given by Abe and Okamoto [2]. We first deal with the common-part forgery where an attacker forges a signature with regard to common information c that has never appeared in the game of the definition 5, *i.e.*, $l_c = 0$. We then treat one-more forgery where $l_c \neq 0$.

Suppose a successful common-part forger $\mathcal{U}^*$ who plays the game of the definition 5 and produces a valid message-signature tuple $(z', b', a', \sigma, c, m')$ such that $l_c = 0$ with a non-negligible probability ϵ, we can construct a machine $\mathcal{M}$ to solve the q-Strong Diffie-Hellman Problem for $q = 0$ [4]: given (g, y), output a pair $(c, g^{\frac{1}{c+x}})$ where $c \in Z_q^*$.

Let q_H and q_{H_0} be the maximum number of queries asked from $\mathcal{U}^*$ to $\mathcal{H}$ and $\mathcal{H}_0$, respectively. Similarly, let q_S be the maximum number of invocation of the signer $\mathcal{S}$. All those parameters are limited by a polynomial in the security parameter k. For simplicity, we assume that all queries are different. Let $(x, y = g^x)$ be the private and public key pair of the signer. Machine $\mathcal{M}$ simulates the game in definition 5 as follows:

1. Choose randomly $v_i, w_j, \omega \in Z_q$ for $i = 1, 2, \cdots, q_H + q_S$, $j = 1, 2, \cdots, q_{H_0} + q_S$.
2. Select $I \in_U \{1, 2, \cdots, q_H + q_S\}$ and $J \in_U \{1, 2, \cdots, q_{H_0} + q_S\}$. Run $\mathcal{U}^*$ with (g, y, q) simulating $\mathcal{H}, \mathcal{H}_0$ and $\mathcal{S}$ as follows.
   - For i-th query to $\mathcal{H}$, respond

$$H(m_i, z_i, b_i, a_i, c_i) = \begin{cases} g^\omega, & \text{if } i = I \\ (y \cdot g^{w_i})^{v_i}, & \text{if } i \neq I \end{cases}$$

   - For j-th query to $\mathcal{H}_0$, respond $H_0(c_j) = w_j$.

[4] Similarly, we only need to exploit the existence of (α, λ, u).

– For requests to $\mathcal{S}$, first negotiate the common information. Let c_k be the result of negotiation, then respond

$$\sigma_k = \begin{cases} \text{“Fail”}, & \text{if } c_k = c_I \\ g^{v_k}, & \text{if } c_k \neq c_I \end{cases}$$

3. If $\mathcal{U}^*$ eventually outputs a valid signature σ with regard to c_J and m_I, output them.

The probability that $\mathcal{U}^*$ is successful without querying $\mathcal{H}, \mathcal{H}_0$ in a proper way is negligible because of the randomness of those hash functions.

Now we use $\mathcal{M}$ to solve the q-Strong Diffie-Hellman Problem for q=0. Note that $\sigma = g^{\omega \frac{1}{H_0(c_J)+x}}$, therefore we can output a valid pair $(H_0(c_J), \sigma^{\omega^{-1}})$.

We then consider the case where the forgery is attempted against the common information such that $l_c \neq 0$. Here we only need to consider a single c in the game of the definition 5. For the case where c is not all the same in the game of the definition 5, we can follow the solution [2] to turn the game into the fixed-info version.

Since there is a unique c in the game of the definition 5, we only need to prove the security of fully blind version of our scheme. For any public information c, the signer sets up the system parameters $params = \{G_1, G_2, e, q, g, k, H, H_0\}$. Let $(X = H_0(c) + x, Y = g^{H_0(c)+x})$ be the private and public key pair of the signer, here $x \in_R Z_q^*$. Let m' be the signed message. The blind signature issuing protocol of this fully blind signature scheme is shown as follows:

– The signer generates a random number $r \in_R Z_q$ and sends $z = m'^{rX}$, $b = m'^r$, and $a = Y^r$ to the receiver.
– The receiver checks whether $e(z, g) = e(b, Y) = e(m, a)$. If not, he terminates the protocol. Else, he generates random numbers $\alpha, \lambda, u \in_R Z_q$ and computes

$$m' = m^\alpha, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}, a' = a^\lambda, \tilde{m} = H(m', z', b', a')Y^u.$$

The receiver then sends $\tilde{m}$ to the signer.
– The signer responds with $\tilde{\sigma} = \tilde{m}^{\frac{1}{X}}$ and the receiver computes $\sigma = \tilde{\sigma} g^{-u}$.

(z', b', a', σ) is a valid signature on m' if the following equations hold:

$$e(\sigma, Y) = e(H(m', z', b', a'), g);\ e(z', g) = e(b', Y) = e(m', a').$$

We call above fully blind signature scheme FuBS, which is actually the restrictive blind signature scheme proposed in section 3. It is easy to see that if a message-signature pair (m, c, S) can be forged for the proposed partially blind signature scheme, then a blind signature on the message $m' = m||c$ for the corresponding FuBS can be forged.

Next, we show that FuBS is secure against one-more forgery under chosen message attack using the similar technique in [3]. In the following we firstly introduce a variations of chosen-target CDHP, named “Chosen target RCDHP”.

Definition 6. *Let G_1 be a gap Diffie-Hellman group of prime order q and g is a generator of G_1. Let x be a random element of Z_q^* and $y = g^x$. Let $H_0 : \{0,1\}^* \rightarrow G_1$ be a cryptographic hash function. The adversary $\mathcal{A}$ is given input (q, g, y, H_0) and has access to the target oracle T_{G_1} that returns a random element z_i in G_1 and the helper oracle* RCDH-$x(\cdot)$*, i.e., compute $(\cdot)^{x^{-1}}$. Let q_T and q_H be the number of queries $\mathcal{A}$ made to the target oracle and the helper oracle, respectively. The advantage of the adversary attacking the chosen-target RCDHP $\mathsf{Adv}_{G_1}^{ct-rcdh}(\mathcal{A})$ is defined as the probability of $\mathcal{A}$ to output a set of l pairs $((v_1, j_1), (v_2, j_2), \ldots, (v_l, j_l))$, for all $1 \leq i \leq l$ $\exists$ $1 \leq j_i \leq q_T$ such that $v_i = z_{j_i}^{x^{-1}}$ where all v_i are distinct and $q_H < q_T$.*

The chosen-target RCDH assumption states that there is no polynomial-time adversary $\mathcal{A}$ with non-negligible $\mathsf{Adv}_{\mathbb{G}_1}^{ct-icdh}(\mathcal{A})$.

The following lemma shows that FuBS is secure under the assumption that the chosen-target RCDHP in G_1 is intractable.

Lemma 1. *If the chosen-target RCDH assumption is true in the group G_1 then FuBS is secure against one-more forgery under the chosen message attack.*

Proof. (sketch). If there is a probabilistic polynomial time one-more forger algorithm $\mathcal{F}$ with a non-negligible probability ϵ for FuBS under a chosen message attack, then we can use $\mathcal{F}$ to construct an algorithm $\mathcal{A}$ to solve the chosen-target RCDHP with a non-negligible probability.

Suppose that a probabilistic polynomial time forger algorithm $\mathcal{F}$ is given. Suppose that $\mathcal{A}$ is given a challenge as in Definition 6. Now $\mathcal{F}$ has access to a blind signing oracle $x(\cdot)$ and the random hash oracle $H_0(\cdot)$. First, $\mathcal{A}$ provides $(G_1, G_2, e, q, g, H_0, y)$ to $\mathcal{F}$ and $\mathcal{A}$ has to simulate the random hash oracle and the blind signing oracle for $\mathcal{F}$.

Each time $\mathcal{F}$ makes a new hash oracle query which differs from previous one, $\mathcal{A}$ will forward to its target oracle and returns the reply to $\mathcal{F}$. $\mathcal{A}$ stores the pair query-reply in the list of those pairs. If $\mathcal{F}$ makes a query to blind signing oracle, $\mathcal{A}$ will forward to its helper oracle RCDH-$x(\cdot)$ and returns the answer to $\mathcal{F}$.

Eventually $\mathcal{F}$ halts and outputs a list of message-signature pairs $((m_1, S_1), (m_2, S_2), \ldots, (m_l, S_l))$. $\mathcal{A}$ can find m_i in the list stored hash oracle query-reply for $i = 1, 2, \ldots, l$. Let j_i be the index of the found pair, then $\mathcal{A}$ can output its list as $((S_1, j_1), (S_2, j_2), \ldots, (S_l, j_l))$. Then this list is a solution to the problem in Definition 6. □

4.3 Efficiency

We compare our signature scheme to previous restrictive partially blind signature scheme. In the following table we denote by $|G_1|$ the bits of representing any element of G_1. Similarly, let $|p|$ and $|q|$ denote the bits of primes p and q such that $q|p-1$, respectively. Also, let P be the pairings operation, M exponentiation in G_1, E exponentiation in Z_p and R inversion in Z_q (we ignore other operations such as hash in both schemes).

Table 1. Comparison with Maitland-Boyd's signature scheme

Properties	*Scheme* [14]	*Our Proposed Scheme*
Length of signature	$\|p\|+4\|q\|$	$4\|G_1\|$
Communication	$4\|p\|+5\|q\|$	$5\|G_1\|$
Computation (*for signature generation*)	$20E+2R$	$9M+1R+3P$
Computation (*for signature verification*)	$6E$	$5P$

The computation complexity of our signature scheme requires more overhead than that of Maitland-Boyd's signature scheme since the pairing computation is the operation which by far takes the most running time. However, the advantages of our scheme are the short length of the signature and low communication complexity (remember that the order of G_1 is only q). Therefore, it is more suitable for low-bandwidth communication environments.

4.4 Application for Electronic Cash System

We follow Brand's construction to describe an electronic cash system using the proposed restrictive partially blind signature scheme from pairings. We denote the bank by $\mathcal{B}$, a generic account-holder by $\mathcal{U}$, and a generic shop by $\mathcal{S}$.

The setup of the system. Let G be a gap Diffie-Hellman group with the prime order q, (g, g_1, g_2) be a random generator tuple. The key pair of $\mathcal{B}$ is $(x, y = g^x)$. Define three cryptographic secure hash functions $H : G\times G\times G \rightarrow G$, $H_0 : \{0,1\}^* \rightarrow Z_q$ and $H_1 : G \times G \times ID_S \times Date/Time \rightarrow Z_q$.

Opening an account. When $\mathcal{U}$ opens an account at $\mathcal{B}$, $\mathcal{B}$ requests $\mathcal{U}$ to identify himself. $\mathcal{U}$ then generates at random a number $u_1 \in_R Z_q$, and computes the unique account number $I = g_1^{u_1}$. If $g_1^{u_1} g_2 \neq 1$, then $\mathcal{U}$ transmits I to $\mathcal{B}$, and keeps u_1 secret. $\mathcal{B}$ stores the identifying information of $\mathcal{U}$ in the account database, together with I. The information I enables $\mathcal{B}$ to uniquely identify $\mathcal{U}$ in case he double-spends.

The withdrawal protocol. When $\mathcal{U}$ wants to withdraw a coin, he first proves ownership of his account and negotiates a common information c. To this end, the following withdrawal protocol between $\mathcal{U}$ and $\mathcal{B}$ is performed:

Step 1. $\mathcal{B}$ generates a random number $r \in_R Z_q$ and sends $z = (Ig_2)^{rx}$, $b = (Ig_2)^r$, and $a = y^r$ to $\mathcal{U}$.
Step 2. $\mathcal{U}$ checks whether $e(z, g) = e(b, y) = e(Ig_2, a)$. If the equation does not hold, he terminates the protocol. Else, he generates random numbers $\alpha, \lambda, x_1, x_2$, $u \in_R Z_q$ and computes $A = (Ig_2)^\alpha, z' = z^{\alpha\lambda}, b' = b^{\alpha\lambda}, a' = a^\lambda, B = g_1^{x_1} g_2^{x_2}$ and $\tilde{m} = H(A, B, z', b', a', c)(g^{H_0(c)} y)^u$. He then sends $\tilde{m}$ to $\mathcal{B}$.
Step 3. $\mathcal{B}$ responds with $\tilde{\sigma} = \tilde{m}^{\frac{1}{H_0(c)+x}}$, and $\mathcal{U}$ computes $\sigma = \tilde{\sigma} g^{-u}$.

If $e(\sigma, g^{H_0(c)}y) = e(H(A, B, z', b', a', c), g)$, then $A, B, c, (z', b', a', \sigma)$ is a valid coin of which $\mathcal{U}$ knows a representation.

The payment protocol. When $\mathcal{U}$ wants to spend his coin at $\mathcal{S}$, the following protocol is performed:

Step 1. $\mathcal{U}$ sends $A, B, c, (z', b', a', \sigma)$ to $\mathcal{S}$.
Step 2. If $A \neq 1$, $\mathcal{S}$ then sends a challenge $d = H_1(A, B, ID_{\mathcal{S}}, date/time)$ to $\mathcal{U}$, where $ID_{\mathcal{S}}$ can be the account number of $\mathcal{S}$, $date/time$ is the number representing date and time of the transaction.
Step 3. $\mathcal{U}$ computes the responses $r_1 = d(u_1\alpha) + x_1$ and $r_2 = d\alpha + x_2$ and sends them to $\mathcal{S}$.

$\mathcal{S}$ accepts the coin if and only if the equations $e(\sigma, g^{H_0(c)}y) = e(H(A, B, z',\ b',\ a',\ c),\ g)$, $e(z', g) = e(b', y) = e(A, a')$, and $g_1^{r_1} g_2^{r_2} = A^d B$ hold.

The deposit protocol. After some delay in time, $\mathcal{S}$ sends $\mathcal{B}$ the payment transcript, consisting of $A, B, c, (z', b', a', \sigma), (r_1, r_2)$ and date/time of transaction. $\mathcal{B}$ first checks the validity of the coin. If the verifications hold, he then searches its deposit database to find out whether A has been stored before. If A has not stored before, $\mathcal{B}$ stores $A, c, date/time, (r_1, r_2)$ in its database; Else, $\mathcal{B}$ can detect double-depositing (the same challenge) or double-spending (the different challenge). The number $(r_1 - r_1')/(r_2 - r_2')$ serves as a proof of double-spending.

5 Conclusions

In this paper we first propose a new restrictive blind signature scheme and a restrictive partially blind signature scheme from bilinear pairings. The former can be regarded as a special case of the latter. Compared to other schemes, our schemes have the advantages of the shorter signature length and lower communication complexity. We also provide a formal security proof for the proposed schemes in the random oracle model.

Acknowledgement

We would like to express our gratitude to Jacques Traoré for pointing out a security flaw in the first version of this paper. Also, we would like to thank Marina Blanton for the suggestions to improve this paper. Finally, we are grateful to the anonymous referees of Financial Cryptography and Data Security 2006 for their invaluable suggestions.

References

1. M. Abe and E. Fujisaki, *How to date blind signatures*, Advances in Cryptology-Asiacrypt 1996, LNCS 1163, pp. 244-251, Springer-Verlag, 1996.
2. M. Abe and T. Okamoto, *Provably secure partially blind signature*, Advances in Cryptology-Crypto 2000, LNCS 1880, pp. 271-286, Springer-Verlag, 2000.

3. A. Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme*, PKC 2003, LNCS 2567, pp. 31-46, Springer-Verlag, 2003.
4. D. Boneh and X. Boyen, *Short signatures without random oracles*, Advances in Cryptology-Eurocrypt 2004, LNCS 3027, pp. 56-73, pringer-Verlag, 2004.
5. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairings*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
6. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairings*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.
7. S. Brands, *Untraceable off-line cash in wallet with observers*, Advances in Cryptology-Crypto 1993, LNCS 773, pp. 302-318, Springer-Verlag, 1993.
8. S. Brands, *An efficient off-line electronic cash system based on the representation problem*, Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), 1993.
9. J. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, PKC 2003, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.
10. D. Chaum, *Blind signature for untraceable payments*, Advances in Cryptology-Eurocrypt 82, Plenum Press, pp. 199-203, 1982.
11. D. Chaum, A. Fiat, and M. Naor, *Untraceable electronic cash*, Advances in Cryptology-Crypto 1988, LNCS 403, pp. 319-327, Springer-Verlag, 1990.
12. D. Chaum and T.P. Pedersen, *Wallet databases with observers*, Advances in Cryptology-Crypto 1992, LNCS 740, pp. 89-105, Springer-Verlag, 1992.
13. F. Hess, *Efficient identity based signature schemes based on pairingss*, SAC 2002, LNCS 2595, Springer-Verlag, pp. 310-324, 2002.
14. A. Juels, M. Luby, and R. Ostrovsky, *Security of blind signatures*, Advances in Cryptology-Crypto 1997, LNCS 1294, pp. 150-164, Springer-Verlag, 1997.
15. G. Maitland and C. Boyd, *A provably secure restrictive partially blind signature scheme*, PKC 2002, LNCS 2274, pp. 99-114. Springer-Verlag, 2002.
16. D. Pointcheval, *Strengthened security for blind signatures*, Advances in Cryptology-Eurocrypt 1998, LNCS 1403, pp. 391-403, Springer-Verlag, 1998.
17. D. Pointcheval and J. Stern, *Provably secure blind signature schemes*, Advances in Cryptology-Asiacrypt 1996, LNCS 1163, pp. 252-265, Springer-Verlag, 1996.
18. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptography, Vol.13, No.3, pp. 361-396, Springer-Verlag, 2000.
19. F. Zhang, R. Safavi-Naini, and W. Susilo, *Efficient verifiably encrypted signature and partially blind signature from bilinear pairings*, Indocrypt 2003, LNCS 2904, pp. 191-204, Springer-Verlag, 2003.
20. F. Zhang, R. Safavi-Naini and W. Susilo, *An efficient signature scheme from bilinear pairings and its applications*, PKC 2004, LNCS 2947, pp. 277-290, Springer-Verlag, 2004.