ID-based Restrictive Partially Blind Signatures and Applications

Xiaofeng Chen[1], Fangguo Zhang[1], and Shengli Liu[2]

[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] Department of Computer Science,
Shanghai Jiao Tong University, Shanghai 200030, P.R.China
liu-sl@cs.sjtu.edu.cn

Abstract. Restrictive blind signatures allow a recipient to receive a blind signature on a message not known to the signer but the choice of 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 receiver. Restrictive partially blind signatures incorporate the advantages of these two blind signatures. The existing restrictive partially blind signature scheme was constructed under certificate-based (CA-based) public key systems. In this paper we follow Brand's construction to propose the first identity-based (ID-based) restrictive blind signature scheme from bilinear pairings. Furthermore, we first propose an ID-based restrictive partially blind signature scheme, which is provably secure in the random oracle model. As an application, we use the proposed signature scheme to build an untraceable off-line electronic cash system followed Brand's construction.

Key words: ID-based systems, Blind signatures, Bilinear pairings.

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 schemes where anonymity is of great concern. About the formal definition and security of blind signature schemes, refer to [14, 16–18].

Restrictive blind signatures, firstly introduced by Brands [5, 6], which allow a recipient to receive a blind signature on a message not known 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.

The concept of partially blind signatures was first introduced by Abe and Fujisaki [1] and allows 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. Partially blind signatures play an important role in designing efficient electronic cash systems. For example, the bank does not require different public keys for different coins 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. However, their scheme was constructed under the CA-based public key systems. There seems no such schemes under the ID-based public key systems to the best of our knowledge.

The concept of ID-based public key systems, proposed by Shamir in 1984 [19], allows a user to use his identity as the public key. It can simplify key management procedure compared to CA-based systems, so it can be an alternative for CA-based public key systems in some occasions, especially when efficient key management and moderate security are required. Many ID-based schemes have been proposed after the initial work of Shamir, but most of them are impractical due to low efficiency. Recently, the bilinear pairings have been found various applications in cryptography, more precisely, they can be used to construct ID-based cryptographic schemes [3, 4, 13, 20].

Recently, Chow *et al* first presented an ID-based partially blind signature scheme [12]. In this paper, we utilize their scheme to propose an ID-based restrictive partially blind signature scheme from bilinear pairings. Our contribution is two folds:
1. We first propose an ID-based restrictive blind signature scheme using the ID-based knowledge proof for the equality of two discrete logarithms from bilinear pairings.
2. We first introduce the notion of ID-based restrictive partially blind signatures and propose a concrete signature scheme from bilinear pairings. Furthermore, we give a formal proof of security for the proposed scheme in the random oracle model.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. The definitions associated with ID-based restrictive partially blind signatures are introduced in Section 3. Two building blocks of ID-based restrictive partially blind signatures are given in Section 4. The proposed restrictive partially blind signature scheme and its security analysis are given in Section 5. Finally, conclusions will be made in Section 6.

2 Preliminaries

In this section, we will briefly describe the basic definition and properties of bilinear pairings and gap Diffie-Hellman group. We also introduce ID-based public key setting and a knowledge proof for the equality of two discrete logarithms from bilinear pairings.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a, b be elements of Z_q^*. We assume that

the discrete logarithm problem (DLP) in both G_1 and G_2 are hard. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists P and $Q \in G_1$ such that $e(P, Q) \neq 1$;
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

2.2 Gap Diffie-Hellman Group

Let G be a cyclic multiplicative group generated by g, whose order is a prime q, assume that the inversion and multiplication in G can be computed efficiently. We first introduce the following problems in G.

1. Discrete Logarithm Problem (DLP): Given two elements g and h, to find an integer $n \in Z_q^*$, such that $h = g^n$ whenever such an integer exists.
2. Computation Diffie-Hellman Problem (CDHP): Given g, g^a, g^b for $a, b \in Z_q^*$, to compute g^{ab}.
3. Decision Diffie-Hellman Problem (DDHP): Given g, g^a, g^b, g^c for $a, b, c \in Z_q^*$, to decide whether $c \equiv ab \bmod q$.

We call G a gap Diffie-Hellman group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP with non-negligible probability. Such groups can be found in supersingular elliptic curve or hyperelliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [3, 9, 13].

Throughout the rest of this paper we define G_1 be a gap Diffie-Hellman group of prime order q, G_2 be a cyclic multiplicative group of the same order q and a bilinear pairing $e : G_1 \times G_1 \to G_2$. Define four cryptographic secure hash functions $H : \{0,1\}^* \to G_1$, $H_1 : {G_2}^4 \to Z_q$, $H_2 : \{0,1\}^* \times G_1 \to Z_q$ and $H_3 : {G_1}^2 \times {G_2}^4 \to Z_q$.

2.3 ID-based Setting from Bilinear Pairings

The ID-based public key systems allow some public information of the user such as name, address and email *etc.*, rather than an arbitrary string to be used his public key. The private key of the user is calculated by PKG and sent to the user via a secure channel.

ID-based public key setting from bilinear pairings can be implemented as follows:

- **Setup:** PKG chooses a random number $s \in Z_q^*$ and set $P_{pub} = sP$. The center publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H\}$, and keep s as the *master-key*, which is known only himself.
- **Extract:** A user submits his/her identity information ID to PKG. PKG computes the user's public key as $Q_{ID} = H(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key.

2.4 ID-based Knowledge Proof for the Equality of Two Discrete Logarithm from Bilinear Pairings

A prover with possession of a secret number $\beta \in Z_q$ wants to show that $\log_g u = \log_h v$ while without exposing β, where $u = g^\beta$, $v = h^\beta$. Chaum and Pedersen [11] first proposed an interactive

protocol to solve this problem. Motivated by this idea, Baek and Zheng [7, 8] construct a new ID-based knowledge proof for the equality of two discrete logarithms from bilinear pairings.

Define $g = e(P, Q_{ID})$, $u = e(P_{pub}, Q_{ID})$, $h = e(L, Q_{ID})$ and $v = e(L, S_{ID})$, where P and L are independent points of G_1. The following protocol presents a knowledge proof of that $\log_g u = \log_h v$. An interesting property of this proof is that even the prover does not know the discrete logarithm $\log_g u = \log_h v$ (just be convinced that it equals to the master-key s of the PKG), which is different from the previous protocols. With the notation of [4], $< g, h, u, v >$ is called a Diffie-Hellman tuple.

- The prover randomly chooses an element Q in G_1 and computes $a = e(P, Q)$, $b = e(L, Q)$. The prover sends (a, b) to the verifier.
- The verifier randomly chooses an integer $c \in Z_q$ and sends c to the prover.
- The prover computes $S = Q + cS_{ID}$ and sends S to the verifier.
- The verifier checks whether $e(P, S) = au^c$ and $e(L, S) = bv^c$. If both the equations hold, returns "*accept*"; else, returns "*reject*".

3 Definitions

Abe and Okamoto first present 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 $\mathtt{info}$. In real applications, $\mathtt{info}$ may be decided by the negotiation between the signer and user. For the sake of simplicity, we omit this negotiation throughout this paper. In the following, we follow the definitions of [2, 14, 5, 12] to give a formal definition of ID-based restrictive partially blind signatures.

Definition 1. *(ID-based Restrictive Partially Blind Signatures) An ID-based 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 *and an identity information* ID*, outputs the private key* $sk = S_{ID}$.
- **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* $\mathtt{info}$ *is agreed common information between* U *and* S*. The public input tape of* U *contains* ID *and* $\mathtt{info}$*. The public input tape of* S *contains* $\mathtt{info}$*. 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* $\mathtt{info}$ *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* $(\mathtt{info}, m, \sigma)$.
- **Signature Verification** $\mathcal{SV}$**:** *On input* $(ID, \mathtt{info}, m, \sigma)$ *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 $\mathtt{info}$ on its proper tapes, and U outputs $(\mathtt{info}, m, \sigma)$ that satisfies*

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

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 $(\mathtt{info}, m, \sigma)$ is valid with regard to ID 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. *$sk = S_{ID} \leftarrow \mathcal{KG}(\mathsf{Params}, ID)$.*
2. *$(m_0, m_1, \mathtt{info}_0, \mathtt{info}_1) \leftarrow S^*(1^k, ID, sk)$.*
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 $\mathtt{info}_0$ and $\mathtt{info}_1$ on the public input tapes of U_0 and U_1, respectively. Also put ID 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 $(\mathtt{info}_0, m_b, \sigma_b)$ and $(\mathtt{info}_0, m_{1-b}, \sigma_{1-b})$, respectively, on their private tapes. If $\mathtt{info}_0 \neq \mathtt{info}_1$, then give $\perp$ to S^*. If $\mathtt{info}_0 = \mathtt{info}_1$, 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) Suppose the adversary $\mathcal{A}$ can perform a polynomial bounded number of the following types of queries (including the hash queries and signing queries) in an adaptively manner during the signature issuing protocol.*

1. *$sk = S_{ID} \leftarrow \mathcal{KG}(\mathsf{Params}, ID)$.*

2. *For each* $\texttt{info}$, $\mathcal{A}$ *chooses a message* m *and an identity* ID, *the challenger* $\mathcal{C}$ *issues a signature* σ *and send it to* $\mathcal{A}$.
3. $\mathcal{A}$ *outputs a tuple* $(ID, \texttt{info}, m, \sigma)$, *where* $(ID, m, \texttt{info})$ *is never queried before. We say the adversary* $\mathcal{A}$ *wins the game if* σ *is a valid signature for* m *and* $\texttt{info}$.

An ID-based partially blind signature scheme is existential unforgeable against adaptively chosen message and ID attacks if no probabilistic polynomial-time adversary can win the above game with a non-negligible advantage.

4 Building Blocks

In this section, we describe two building blocks of ID-based restrictive partially blind signatures. Firstly, we propose an ID-based restrictive blind signature scheme from bilinear pairings. We then introduce the ID-based partially blind signature scheme proposed by Chow *et al.*

4.1 ID-based Restrictive Blind Signature Scheme

Brand's restrictive blind signature scheme is mainly based on Chaum-Pedersen's knowledge proof of common exponent [11]. Maitland and Boyd [15] presented the following general construction based on Brand's original scheme. In this paper, we first propose ID-based restrictive blind signature scheme by using the ID-based knowledge proof for the equality of two discrete logarithms from bilinear pairings.

- PKG chooses a random number $s \in Z_q^*$ as the *master-key* and set $P_{pub} = sP$. The system parameters are $params = \{G_1, G_2, e, q, P, P_{pub}, H, H_1\}$.
- The signer submits his/her identity information ID to PKG. PKG computes $Q_{ID} = H(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key. For the sake of simplicity, define $g = e(P, Q_{ID}), y = e(P_{pub}, Q_{ID})$.
- Suppose the signed message is $M \in G_1$.[1] The signer generates a random number $Q \in_R G_1$, and sends $z = e(M, S_{ID}), a = e(P, Q)$, and $b = e(M, Q)$ to the receiver.
- The receiver generates random numbers $\alpha, \beta, u, v \in_R Z_q$ and computes

$$M' = \alpha M + \beta P, A = e(M', Q_{ID}), z' = z^{\alpha} y^{\beta}, a' = a^u g^v, b' = a^{u\beta} b^{u\alpha} A^v.$$

  The receiver then computes $c' = H_1(A, z', a', b')$ and sends $c = c'/u \mod q$ to the signer.
- The signer responds with $S = Q + cS_{ID}$.
- The receiver accepts if and only if $e(P, S) = ay^c, e(M, S) = bz^c$. If the receiver accepts, computes $S' = uS + vQ_{ID}$.

(z', c', S') is a valid signature on M' if the following equation holds:

$$c' = H_1(e(M', Q_{ID}), z', e(P, S')y^{-c'}, e(M', S')z'^{-c'}).$$

[1] In real applications, if the signed message m is not an element of G_1, we can use a cryptographic secure hash function to map m into an element M of G_1.

This is because

$$\begin{aligned} A &= e(M', Q_{ID}) \\ e(P, S') &= e(P, uS + vQ_{ID}) = e(P, S)^u e(P, Q_{ID})^v \\ &= (ay^c)^u g^v = a^u g^v y^{cu} \\ &= a' y^{c'} \\ e(M', S') &= e(M', uS + vQ_{ID}) = e(M', S)^u e(M', Q_{ID})^v \\ &= e(\alpha M + \beta P, S)^u A^v = (bz^c)^{u\alpha} (ay^c)^{u\beta} A^v \\ &= a^{u\beta} b^{u\alpha} (z^\alpha y^\beta)^{c'} A^v \\ &= b' z'^{c'} \end{aligned}$$

Thus, the receiver obtains a signature on the message M' where $M' = \alpha M + \beta P$ and (α, β) are values chosen by the receiver. In addition, in the particular case where $\beta = 0$, the above signature scheme achieves the restrictiveness [15]. For designing an electronic cash system, the system parameters consist of another two random generators P_1 and P_2. A user chooses a random number u as his identification information and computes $M = uP_1 + P_2$. 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 P_1 and P_2. This restricts M' must be the form of αM. For more details, refer to [5].

4.2 ID-based Partially Blind Signature Scheme

Chow *et al* first presented the following ID-based partially blind signature scheme [12]. Suppose the signed message is m and the agreed common information is Δ.

- PKG chooses a random number $s \in Z_q^*$ as the *master-key* and set $P_{pub} = sP$. The system parameters are $params = \{G_1, G_2, e, q, P, P_{pub}, H, H_2\}$.
- The signer submits his/her identity information ID to PKG. PKG computes $Q_{ID} = H(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key.
- The signer randomly chooses $r \in_R Z_q^*$, and sends $U = rP, Y = rQ_{ID}$ to the receiver.
- The receiver generates random numbers $\alpha, \beta, \gamma \in_R Z_q^*$ and computes

  $$Y' = \alpha Y + \alpha\beta Q_{ID} - \gamma H(\Delta), U' = \alpha U + \gamma P_{pub}, h = \alpha^{-1} H_2(m, Y') + \beta.$$

  The receiver then sends h to the signer.
- The signer responds with $S = (r + h)S_{ID} + rH(\Delta)$.
- The receiver computes $S' = \alpha S$.

The resulting signature for the message m and the agreed information Δ is (Y', U', S') if $e(S', P) = e(Y' + H_2(m, Y')Q_{ID}, P_{pub})e(H(\Delta), U')$ holds.

For the correctness and security analysis of the scheme, refer to [12].

5 ID-based Restrictive Partially Blind Signatures

5.1 ID-based Restrictive Partially Blind Signature Scheme

- **System Parameters Generation $\mathcal{PG}$:** Given a security parameter k. The system parameters are $Params = \{G_1, G_2, e, q, P_{pub}, k, H, H_3\}$.

- **Key Generation $\mathcal{KG}$:** On input Params and the signer's identity information ID, outputs the private key $S_{ID} = sQ_{ID} = sH(ID)$ of the signer.
- **Signature Generation $\mathcal{SG}$:** Let the shared information $\textit{info} = \Delta$, and a message M from the receiver. Define $g = e(P, Q_{ID}), y = e(P_{pub}, Q_{ID})$. The signature issuing protocol is shown in Fig. 1.
  - The signer randomly chooses an element $Q \in_R G_1$, and computes $z = e(M, S_{ID})$, $a = e(P, Q)$, and $b = e(M, Q)$. He also randomly chooses a number $r \in_R Z_q^*$, and computes $U = rP$, and $Y = rQ_{ID}$. He then sends (z, a, b, U, Y) to the receiver.
  - The receiver generates random numbers $\alpha, \beta, u, v, \lambda, \mu, \gamma \in_R Z_q$, and computes $M' = \alpha M + \beta P$, $A = e(M', Q_{ID})$, $z' = z^{\alpha} y^{\beta}$, $a' = a^u g^v$, $b' = a^{u\beta} b^{u\alpha} A^v$, $Y' = \lambda Y + \lambda\mu Q_{ID} - \gamma H(\Delta)$, $U' = \lambda U + \gamma P_{pub}$, $c' = H_3(M', Y', U', A, z', a', b')$, $h_1 = c'/u$, and $h_2 = \lambda^{-1} c' + \mu$. He then sends h_1, h_2 to the signer.
  - The signer responds with $S_1 = Q + h_1 S_{ID}, S_2 = (r + h_2) S_{ID} + rH(\Delta)$.
  - If the equations $e(P, S_1) = a y^{h_1}$ and $e(M, S_1) = b z^{h_1}$ hold, the receiver computes $S_1' = uS_1 + vQ_{ID}$, and $S_2' = \lambda S_2$.

  The resulting signature for Δ and message M' is a tuple $(Y', U', z', c', S_1', S_2')$.
- **Signature Verification $\mathcal{SV}$:** Given the message M', the shared information Δ and the tuple $(Y', U', z', c', S_1', S_2')$, the verifier accepts the signature if the following equations hold:

$$c' = H_3(M', Y', U', e(M', Q_{ID}), z', e(P, S_1') y^{-c'}, e(M', S_1') z'^{-c'})$$

$$e(S_2', P) = e(Y' + c' Q_{ID}, P_{pub}) e(H(\Delta), U').$$

5.2 Security Analysis

Theorem 1. *The proposed scheme achieves the property of completeness.*

Proof. Note that

$$A = e(M', Q_{ID})$$

$$e(P, S_1') = e(P, S_1)^u e(P, Q_{ID})^v = (a y^h)^u g^v = a' y^{c'}$$

$$e(M', S_1') = e(M', S_1)^u e(M', Q_{ID})^v = e(\alpha M + \beta P, S_1)^u A^v = b' z'^{c'}$$

and

$$\begin{aligned} e(S_2', P) &= e(\lambda S_2, P) \\ &= e((\lambda r + \lambda h_2) S_{ID} + \lambda r H(\Delta), P) \\ &= e((\lambda r + c' + \lambda\mu) S_{ID}, P) e(H(\Delta), \lambda r P) \\ &= e((\lambda r + c' + \lambda\mu) Q_{ID}, P_{pub}) e(H(\Delta), U' - \gamma P_{pub}) \\ &= e((\lambda r + c' + \lambda\mu) Q_{ID} - \gamma H(\Delta), P_{pub}) e(H(\Delta), U') \\ &= e(Y' + c' Q_{ID}, P_{pub}) e(H(\Delta), U') \end{aligned}$$

Thus, the proposed scheme achieves the property of completeness.

Theorem 2. *The proposed scheme achieves the property of restrictiveness.*

Proof. Similar to [5, 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 $M' = \alpha M + \beta P$ with α and β randomly chosen by the recipient. In addition, in the particular case where $\beta = 0$, if there exists a representation (μ_1, μ_2) of M with respect to bases P_1 and P_2 such that $M = \mu_1 P_1 + \mu_2 P_2$ and if there exists a representation (μ_1', μ_2') of M' with respect to g_1 and g_2 such that $M' = \mu_1' P_1 + \mu_2' P_2$, then the relation $I_1(\mu_1, \mu_2) = \mu_1/\mu_2 = \mu_1'/\mu_2' = I_2(\mu_1', \mu_2')$ holds.

Theorem 3. *The proposed scheme is partially blind.*

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).

If in step 5, the shared information $\Delta_0 = \Delta_1$. Let $(Y', U', z', c', S_1', S_2', M')$ be one of the signatures subsequently given to S^*. Let $(Y, U, z, a, b, h_1, h_2, S_1, S_2, M)$ be data appearing in the view of S^* during one of the executions of the signature issuing protocol at step 4. It is sufficient to show that there exists a tuple of random blinding factors $(\alpha, \beta, u, v, \lambda, \mu, \gamma)$ that maps $(Y, U, z, a, b, h_1, h_2, S_1, S_2, M)$ to $(Y', U', z', c', S_1', S_2', M')$.

Let $S_2' = \lambda S_2$, $U' = \lambda U + \gamma P_{pub}$ and $Y' = \lambda Y + \lambda\mu Q_{ID} - \gamma H(\Delta)$. The unique blinding factors (λ, μ, γ) are always exist.[2]

Let $u = c'/h_1$, we know there exists a unique blinding factor v which satisfies the equation $S_1' = uS_1 + vQ_{ID}$. Determine a representation $M' = \alpha M + \beta P$, which is known to exist. Note that $z' = A^s$ and $z = e(M, Q_{ID})^s$ have been established by the interactive proof and the fact that the signature is valid. Therefore, $z' = e(M', Q_{ID})^s = z^\alpha y^\beta$. Since $e(P, S_1) = ay^{h_1}$ and $e(M, S_1) = bz^{h_1}$, we have $a' = e(P, S_1')y^{-c'} = a^u g^v$ and $b' = e(M', S_1')(z')^{-c'} = a^{u\beta} b^{u\alpha} A^v$.

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

Theorem 4. *The proposed scheme is secure against on the existential adaptively chosen message and ID attacks under the assumption of CDHP in G_1 is intractable and the random oracle model.*

Proof. The proof follows the security argument given by Chow *et al* [12].

5.3 Application for Electronic Cash System

We follow Brand's construction to describe an electronic cash system using the proposed ID-based restrictive partially blind signature scheme. 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 (P, P_1, P_2) be a random generator tuple of G_1. Suppose PKG chooses a random number $s \in Z_q^*$ as the *master-key* and sets $P_{pub} = sP$. $\mathcal{B}$ submits his identity information ID to PKG and PKG computes the private key S_{ID} for $\mathcal{B}$. Define three cryptographic secure hash functions $H : \{0,1\}^* \to G$, $H_0 : G_1^3 \times G_2^5 \to Z_q$ and $H_1 : G \times G \times ID_S \times Date/Time \to Z_q$. For the sake of simplicity, define $g = e(P, Q_{ID}), g_1 = e(P_1, Q_{ID}), g_2 = e(P_2, Q_{ID}), y = e(P_{pub}, Q_{ID})$.

[2] Though it is difficult to compute (λ, μ, γ), we only need to exploit the existence of them.

Opening an account. When $\mathcal{U}$ opens an account at $\mathcal{B}$, $\mathcal{B}$ requests $\mathcal{U}$ to identity himself. $\mathcal{U}$ then generates at random a number $u_1 \in_R Z_q$, and computes the unique account number $I = u_1 P_1$. If $M = u_1 P_1 + P_2 \neq O$, 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 Δ. To this end, the following withdrawal protocol between $\mathcal{U}$ and $\mathcal{B}$ is performed:

Step 1. $\mathcal{B}$ randomly chooses an element $Q \in_R G_1$, and computes $z = e(M, S_{ID})$, $a = e(P, Q)$, and $b = e(M, Q)$. He also randomly chooses a number $r \in_R Z_q^*$, and computes $U = rP$, and $Y = rQ_{ID}$. He then sends (z, a, b, U, Y) to $\mathcal{U}$.
Step 2. $\mathcal{U}$ generates random numbers $\alpha, x_1, x_2, u, v, \lambda, \mu, \gamma \in_R Z_q$, and computes $M' = \alpha M$, $A = e(M', Q_{ID})$, $B = g_1^{x_1} g_2^{x_2}$, $z' = z^{\alpha}$, $a' = a^u g^v$, $b' = b^{u\alpha} A^v$, $Y' = \lambda Y + \lambda\mu Q_{ID} - \gamma H(\Delta)$, $U' = \lambda U + \gamma P_{pub}$, $c' = H_0(M', Y', U', A, B, z', a', b')$, $h_1 = c'/u$, and $h_2 = \lambda^{-1} c' + \mu$. He then sends h_1, h_2 to $\mathcal{B}$.
Step 3. $\mathcal{B}$ responds with $S_1 = Q + h_1 S_{ID}, S_2 = (r + h_2) S_{ID} + rH(\Delta)$.
Step 4. If the equations $e(P, S_1) = ay^{h_1}$ and $e(M, S_1) = bz^{h_1}$ hold, $\mathcal{U}$ computes $S_1' = uS_1 + vQ_{ID}$, and $S_2' = \alpha S_2$.

We say $M', B, \Delta, (Y', U', z', c', S_1', S_2')$ 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 $M', B, \Delta, (Y', U', z', c', S_1', S_2')$ to $\mathcal{S}$.
Step 2. Let $A = e(M', Q_{ID})$, and if $A \neq O$, $\mathcal{S}$ then sends $\mathcal{U}$ a challenge $d = H_1(A, B, ID_{\mathcal{S}}, date/time)$, 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 $(Y', U', z', c', S_1', S_2')$ is a valid signature on (M', B, Δ), and $g_1^{r_1} g_2^{r_2} = A^d B$.

The deposit protocol. After some delay in time, $\mathcal{S}$ sends $\mathcal{B}$ the payment transcript, consisting of $M', B, \Delta, (Y', U', z', c', S_1', S_2'), (r_1, r_2)$ 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 M' has been stored before. If M' has not stored before, $\mathcal{B}$ stores $M', \Delta, date/time, (r_1, r_2)$ in its database; Else, $\mathcal{B}$ can detect double-depositing (the same challenge)or double-spending (the different challenge). The information of $(r_1 - r_1')/(r_2 - r_2')$ serves as a proof to trace the dishonest double-spender.

6 Conclusions

Restrictive partially blind signatures incorporate the advantages of restrictive blind signatures and partially blind signatures, which play an important role in electronic commerce. In this paper we first propose an ID-based restrictive partially blind signature scheme from bilinear pairings.

Furthermore, we give a formal proof of security for the proposed schemes in the random oracle model. As an application, we use the proposed signature scheme to build an untraceable off-line electronic cash system followed Brand's construction.

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. 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.
4. 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.
5. S. Brands, *Untraceable Off-line cash in wallet with observers*, Advances in Cryptology-Crypto 1993, LNCS 773, pp. 302-318, Springer-Verlag, 1993.
6. 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.
7. J. Baek and Y. Zheng, *Identity-based threshold decryption*, PKC 2004, LNCS 2947, pp. 248-261, Springer-Verlag, 2004.
8. J. Baek and Y. Zheng, *Identity-based threshold signature scheme from the bilinear pairings*, IAS'04 track of ITCC'04, pp. 124-128, IEEE Computer Society, 2004.
9. J. Cha and J. 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 and T.P. Pedersen, *Wallet databases with observers*, Advances in Cryptology-Crypto 1992, LNCS 740, pp. 89-105, Springer-Verlag, 1993.
12. S.M. Chow, C.K. Hui, S.M. Yiu and K.P. Chow, *Two improved partially blind signature schemes from bilinear pairings*, ACISP 2005, LNCS 3574, pp. 316-328, Springer-Verlag, 2005. Full version can be found at: http://eprint.iacr.org/2004/108.
13. F. Hess, *Efficient identity based signature schemes based on pairingss*, SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 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. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp. 47-53, Springer-Verlag, 1984.
20. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, Advances in Cryptology-Asiacrypt 02, LNCS 2501, Queenstown, New Zealand, pp.533-547, Springer-Verlag, 2002.

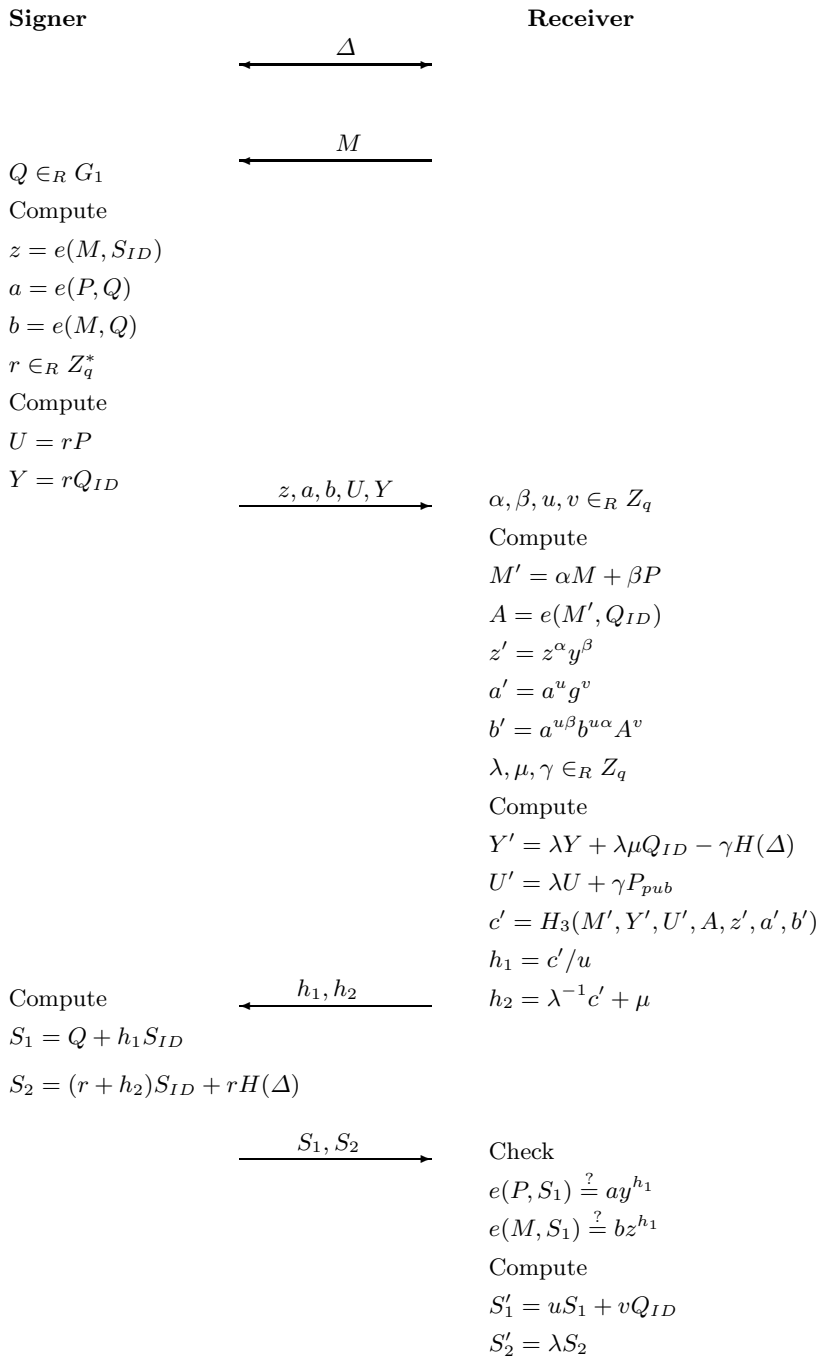

Fig. 1. ID-based Restrictive Partially Blind Signature Scheme