Two Improved Partially Blind Signature Schemes from Bilinear Pairings

Sherman S.M. Chow*, Lucas C.K. Hui, S.M. Yiu, and K.P. Chow

Department of Computer Science and Information Systems
The University of Hong Kong
Hong Kong
{smchow, hui, smyiu, chow}@csis.hku.hk

Abstract. A blind signature scheme is a protocol for obtaining a signature from a signer, but the signer can neither learn the messages he/she sign nor the signatures the recipients obtain afterwards. Such schemes are very important technologies in privacy oriented e-commerce applications. Followed by the first scheme introduced by D. Chaum [9], a number of new schemes based on different difficult problems and with new properties are proposed. One of the examples is the partially blind signature scheme introduced by Abe and Fujisaki [1]. Unlinkability is one of the key properties of a secure blind signature scheme. In this paper, we present a security analysis of a partially blind signature scheme newly proposed at INDOCRYPT 2003 [36][1]. By identifying the reason why the randomness introduced during the blinding phase can be removed, we show that their schemes are indeed *linkable*. In addition, we also modify the ID-based blind signature scheme by Zhang and Kim [33] elegantly to spawn an unlinkable partially blind signature scheme and an ID-based unlinkable partially blind signature scheme. The schemes are provably secure in the random oracle model [3]. To the best of authors' knowledge, our scheme is the first ID-based partially blind signature scheme.

Key words: Partially blind signature, identity-based signature, cryptanalysis, anonymity

1 Introduction

1.1 Background

A blind signature scheme is a protocol for obtaining a signature from a signer, but the signer can neither learn the messages he/she sign nor the signatures the recipients obtain afterwards. Blind signatures scheme is one of the examples of cryptographic schemes that have been employed extensively in privacy oriented e-services such as untraceable electronic cash[11], anonymous multiple choice electronic voting [19], unlinkable credentials [10], oblivious keyword search [23] or even in steganographic protocol [21].

The basic idea of most existing blind signature schemes is as follows. The requester (of the signature) randomly chooses some random factors and embed them to the message to be signed. The random factors are kept in secure so the signer cannot recover the message. Using the signature returned by the signer, the requester can remove the random factors associated with the signature and hence get a valid signature for the message to be signed. The property that requesters can ask the signer to blindly sign any message is undesirable in some situations. For examples, expiry date information should be embedded in the e-cash issued in order to prevent the possible unlimited growth of the e-cash database kept in the

* corresponding author

[1] Zhang *et al.* have revised their scheme to avoid the attack in this paper. [37]

bank for double-spending checking. Hence the message to be signed cannot be "completely blind" and some agreed information should be included in the blind signature. To address this problem, partially blind signatures are introduced [1].

Recently, a partially blind signature from bilinear pairings (ZSS scheme) is proposed [36]. Comparing with previous partially blind signature schemes based on other difficult problems, their work is better in both time complexities and space complexities, and achieves efficient batch verification. In this paper, we review the security of this scheme and propose two *unlinkable* schemes.

1.2 Related Work

Blind signature schemes are classified into four main classes by [18], namely, the hidden, the weak blind, the interactive blind and the strong blind. Examples of hidden and weak blind signature are given in [18] too. In another criterion [17], hidden signature is further divided into message hidden signatures and parameter hidden signatures. Several hidden and weak blind signature schemes have been discussed in [17] as well. Pointcheval and Stern presented the formal definition and security notion for blind signature in [24]. Unfortunately, [27] showed an inherent weakness in their result and presented a novel parallel one-more signature forgery attack.

Another line of research efforts are done in combining the properties of other classes of cryptographic schemes into blind signatures, such as proxy signatures, forward secure signatures and group oriented signatures. In proxy blind signature schemes ([38] and [35]) the signer delegates his/her signing power to a proxy, who blindly signs a message on behalf of the original signer. In [14], a forward-secure blind signature scheme is proposed to address key exposure problem, in which all previously generated signatures are still considered to be valid even the secret key is compromised. Group oriented blind signatures have been studied as well. Threshold blind signature that enables any t out of n legitimate signers to give a blind signature, is considered in [20] and [30]. Blind multisignature is proposed in [12] and group blind signature is proposed in [22].

As an alternative to conventional public key infrastructure (PKI), Shamir introduced identity-based (ID-based) signature schemes [28] and the design of ID-based schemes have attracted a lot of attention recently (e.g. [7, 8, 12, 32, 33]). The distinguishing property of ID-based cryptography is that a user's public key can be any string, such as an email address, that can identify the user. This removes the need for users to look up the signer's public key before the verification of signature. Utilizing bilinear pairings, an ID-based blind signature scheme is proposed by Zhang and Kim in [33]. A blind signature scheme using bilinear pairings for conventional public key infrastructure is proposed in [4].

Some schemes are devised to solve the perfect crime resulting from the unconditional anonymity provided by the blind signature [31], such as fair blind signature in [29], indirect discourse proofs in [16] and "magic ink" signature in [32]. For partially blind signatures, a number of schemes based on different difficult problems are proposed. For examples, RSA-based scheme by Abe and Fujisaki [1], discrete logarithm based scheme by Abe and Okamoto [2] and quadratic residues based scheme by Fan and Lei [15].

Apart from blind signature schemes, there are other primitives that provide anonymity by cryptographic means. An example is "blind auditable membership proofs" [26], in which the problem of achieving anonymity and audibility at the same time is addressed. In verifiably encrypted signature (for examples, [5] and [36]), the signature is encrypted so that any

recipient cannot get the signature, yet the recipient is convinced that its decryption gives a valid signature on a given message and there exists a trusted third party that is able to decrypt the encrypted signature.

1.3 Our Contribution

Our contribution is two-fold. First, we present a security analysis of an existing partially blind signature scheme [36]. By identifying the reason why the randomness introduced during the blinding phase can be removed, we show that their schemes are indeed *linkable*. Second, we propose two new blind signature schemes that achieve unlinkability. One is a partially blind signature scheme in conventional PKI while another one is an ID-based partially blind signature scheme. To the best of authors' knowledge, our scheme is the first ID-based partially blind signature scheme.

1.4 Organization

The rest of the paper is organized as follows. The next section contains some preliminaries about the formal definitions of a partially blind signature scheme, an ID-based partially blind signature scheme, bilinear pairing as well as the Gap Diffie-Hellman group. Formal definitions of security describing the adversary's capabilities are presented in Section 3. We review the ZSS scheme and analyze its security in Section 4. In Section 5, an ID-based partially blind signature scheme and a partially blind signature scheme in conventional public key infrastructure are proposed. The security and efficiency analysis of our schemes are given in Section 6. Finally, Section 7 concludes our paper.

2 Preliminaries

2.1 Framework of Partially Blind Signature Schemes

A partially blind signature scheme consists of four algorithms: `Setup`, `KeyGen`, `Issue`, and `Verify`. `Issue` is an interactive protocol between the signer and the requester which consists of four sub-algorithms: `Agree`, `Blind`, `Sign` and `Unblind`.

- `Setup`: On an unary string input 1^k where k is a security parameter, it produces the common public parameters $params$, which include a description of a finite signature space, a description of a finite message space together with a description of a finite agreed information space.
- `KeyGen`: On a random string x input, it outputs the signer's secret signing key sk and its corresponding public verification pk.
- `Issue`: Suppose the requester wants a message m to be signed, after the execution of four sub-algorithms, a signature σ will be produced. The negotiated information c will be produced too if it is not given as an input.
  - `Agree`: If the negotiated information c is not given as an input, the requester and the signer interacts and finally come up with the agreed information c.
  - `Blind`: On a random string r, a message m and agreed information c as the input, it outputs a string h to be signed by the signer, h is sent to the signer by this algorithm.

  - `Sign`: On a string h and the signer's private signing key sk as the input, it outputs a blind signature $\bar{\sigma}$ to be unblinded by the requester, $\bar{\sigma}$ is sent to the requester by this algorithm.
  - `Unblind`: On a signature $\bar{\sigma}$ and the previous used random string r, it outputs the unblinded signature σ.
- `Verify`: On an unblinded signature σ, a message m, an agreed information c and the signer's public verification key pk as the input, it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature signed by the signer with the corresponding private key pk on a message m and agreed information c.

These algorithms must satisfy the standard consistency constraint of partially blind signature, i.e. if $(\sigma, c) = \texttt{Issue}(m, r, sk)$, we must have $\texttt{Verify}(pk, m, c, \sigma) = \top$. Security requirements will be described in Section 3.

2.2 Framework of ID-Based Partially Blind Signature Schemes

The framework of ID-Based partially blind signature schemes is similar to that of partially blind signature schemes. The differences are described below.

- `Setup`: On an unary string input 1^k where k is a security parameter, it produces the common public parameters $params$, which include a description of a finite signature space, a description of a finite message space together with a description of a finite agreed information space. The master secret s is the output as well, which is kept secret by the Private Key Generator (PKG)
- `KeyGen`: On an arbitrary string input ID, it computes the private signing key S_{ID} and the corresponding public verification key Q_{ID}, with respect to $(params, s)$. This algorithm is to be used by PKG as well.
- `Verify`: On an unblinded signature σ, a message m, an agreed information c and the signer's identity ID as the input, it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature

Again, these algorithms must satisfy the standard consistency constraint of partially blind signature, i.e. if $(\sigma, c) = \texttt{Issue}(m, r, S_{ID})$, we must have $\texttt{Verify}(ID, m, c, \sigma) = \top$.

2.3 Bilinear Pairing and Gap Diffie-Hellman Groups

Bilinear pairing is an important cryptographic primitive (see [4, 5, 12, 13, 30, 33, 35, 36]). Here, we describe some of its key properties.

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q. The bilinear pairing is given as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, which satisfies the following properties:

1. *Bilinearity*: For all $P, Q, R \in \mathbb{G}_1$, $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$.
2. *Non-degeneracy*: There exists $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ $\forall P, Q \in \mathbb{G}_1$.

Definition 1. *Given a generator P of a group $\mathbb{G}$ and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman problem (DDH problem) is to decide whether $c = ab$.*

Definition 2. *Given a generator P of a group $\mathbb{G}$, (P, aP, bP, cP) is defined as a valid Diffie-Hellman tuple if $c = ab$.*

Definition 3. *Given a generator P of a group $\mathbb{G}$ and a 2-tuple (aP, bP), the Computational Diffie-Hellman problem (CDH problem) is to compute abP.*

Definition 4. *If $\mathbb{G}$ is a group such that DDH problem can be solved in polynomial time but no probabilistic algorithm can solve CDH problem with non-negligible advantage within polynomial time, then we call $\mathbb{G}$ a Gap Diffie-Hellman (GDH) group.*

We assume the existence of a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ that one can solve Decisional Diffie-Hellman Problem (DDH problem) in polynomial time.

3 Formal Security Model

Let $\mathbb{G}_1$ be a GDH group, $H(\cdot)$ and $H_1(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

3.1 Signature Non-Repudiation of ID-Based Partially Blind Signature

Signature non-repudiation of an ID-based partially blind signature is formally defined in terms of the *existential unforgeability of identity-based partially blind signature under adaptive chosen-message-and-identity attack* (EUF-IDPB-CMIA2) game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

EUF-IDPB-CMIA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate common public parameters *param* and also the master secret key s. $\mathcal{C}$ sends *param* to $\mathcal{A}$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

- Hash functions queries: $\mathcal{A}$ can ask for the value of the hash function $H(\cdot)$ and $H_1(\cdot)$ for the requested input.
- `KeyGen`: $\mathcal{A}$ chooses an identity ID. $\mathcal{C}$ computes $\texttt{Extract}(ID) = (S_{ID}, D_{ID})$ and sends the result to $\mathcal{A}$.
- `Issue`: $\mathcal{A}$ chooses an identity ID, a plaintext m and an negotiated information c. $\mathcal{C}$ issues the signature by computing $\sigma = \texttt{Issue}\ (m, c, S_{ID})$ and sends σ to $\mathcal{A}$.

Forgery: The adversary $\mathcal{A}$ outputs (σ, ID, m, c) where (ID, m, c) and ID were not used in any of the `Issue` and `Extract` queries, respectively, in the Attack phase. The adversary wins the game if the response of the `Verify` on (ID, m, c, σ) is not equal to $\perp$.

The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 5. *An ID-based partially blind scheme is said to have the existential unforgeability against adaptive chosen-message-and-identity attacks property (EUF-IDPB-CMIA2 secure) if no adversary has a non-negligible advantage in the EUF-IDPB-CMIA2 game.*

3.2 Signature Non-Repudiation of Partially Blind Signature in Conventional PKI

Signature non-repudiation of partially blind signature is formally defined in terms of the *existential unforgeability of partially blind signature under adaptive chosen-message attack* (EUF-PB-CMA2) game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

EUF-PB-CMA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate common public parameters *param*. $\mathcal{C}$ sends *param* to $\mathcal{A}$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

- Hash functions queries: $\mathcal{A}$ can ask for the value of the hash function $H(\cdot)$ and $H_1(\cdot)$ for the requested input.
- `Issue`: $\mathcal{A}$ chooses a public key pk, a plaintext m and an negotiated information c. $\mathcal{C}$ issues the signature by computing $\sigma =$ `Issue` (m, c, sk) and sends σ to $\mathcal{A}$.

Forgery: The adversary $\mathcal{A}$ outputs (σ, pk, m, c) where (pk, m, c) did not appear in any `Issue` query in the Attack phase. It wins the game if the response of the `Verify` on (pk, m, c, σ) is not equal to $\perp$.

The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 6. *An partially blind scheme is said to have the existential unforgeability against adaptive chosen-message attacks property (EUF-PB-CMA2 secure) if no adversary has a non-negligible advantage in the EUF-PB-CMA2 game.*

3.3 Partial Blindness

In the normal sense of blindness, the signer can learn no information on the message to be signed. If the signer can link the signature to the instance of the signing protocol, then the blindness is lost. In partially blind signature, a piece of information must be agreed by both the signer and the requester. If the signer embed an unique piece of agreed information c in each message to be signed, it is easy to see that the signer can link the signature to the instance of the signing protocol by using the agreed information as an index, and hence the blindness property will be lost.

So the normal sense of blindness is not applicable in our situation. The extended notion of partial blindness is defined in terms of the *Unlinkability Game* (UL) played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Unlinkability Game:

Setup: The adversary $\mathcal{A}$ takes a security parameter k and runs the `Setup` to generate common public parameters *param* (and also the master secret key s in ID-based case). $\mathcal{A}$ sends *param* to $\mathcal{C}$.

Preparation: The adversary $\mathcal{A}$ chooses two distinct messages m_0 and m_1, together with the agreed information c. For the ID-based case, the adversary $\mathcal{A}$ also chooses its own identity *ID* and sends it to the challenger $\mathcal{C}$.

Challenge: The challenger $\mathcal{C}$ chooses a random bit b secretly, and then ask the adversary $\mathcal{A}$ to partially sign on the message m_b with agreed information c and m_{1-b} with the same

piece of agreed information c. After the challenger $\mathcal{C}$ unblinds both signatures, it presents the signature of m_b to $\mathcal{A}$.

Response: The adversary $\mathcal{A}$ returns the guess b' and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |2P[b' = b] - 1|$ where $P[b' = b]$ denotes the probability that $b' = b$.

Definition 7. *An (ID-based) partially blind scheme is said to have the perfect partial blindness property if no adversary has zero advantage in the above game.*

Notice that for the scheme to be practical, we should require the cardinality of the finite agreed information space to be small compared with the anticipated number of total `Issue` requests.

4 Review and Analysis of the ZSS's scheme

4.1 The ZSS's scheme

Zhang, Safavi-Naini and Susilo (ZSS)'s scheme is basically a combination of their efficient signature scheme in [34] and a modification version of the blind signature proposed in [4]. The system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, \lambda, P, H(\cdot), H_0(\cdot)\}$ where $\mathbb{G}_1, \mathbb{G}_2, \hat{e}$ are defined as in previous section, $|q| \geq \lambda \geq 160$. $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic hash functions where $H_0 : \{0,1\}^* \rightarrow \{0,1\}^\lambda$ and $H : \{0,1\}^* \rightarrow \mathbb{G}_1$.

`KeyGen`: The signer randomly selects $x \in_R \mathbb{Z}_q^*$ and computes $P_{pub} = xP$ as his/her public verification key. The signing key is x and is kept in secret.

`Issue`: Suppose the requester now wants to get the signature of message m and the requester has already negotiated with the signer on the agreed information c to be attached to the message. The interaction between the requester and the signer is as follows:

- `Blind`: The requester randomly picks $r \in_R \mathbb{Z}_q^*$ and computes $U = r \cdot H_0(m||c)$, where $||$ denotes concatenation. U is sent to the signer.
- `Sign`: The signer computes $V = (H(c) + x)^{-1}U$ and returns V to the requester.
- `Unblind`: Upon the recipient of V, the requester unblinds it by $S = r^{-1}V$.

Finally (S, m, c) is the partially blind signature of message m and agreed information c.

`Verify`: Any verifier including the requester can verify the partially blind signature by checking whether $\hat{e}(H(c)P + P_{pub}, S) = \hat{e}(P, H_0(m||c))$ is true. If so, the partially blind signature is accepted as valid.

4.2 The Linkability of the ZSS's scheme

In [36], the authors argued that the scheme is unlinkable due to the randomness introduced during the blinding phase. However, we show that the randomness introduced can be removed actually by using the following algorithm `Link`, which is able to check whether a given signature is produced by a given instance of the protocol.

Information available from an instance of the protocol: $U = rH_0(m||c)$, $V = (H(c) + x)^{-1}U$.
Signature: $S = r^{-1}V$, m and c.

`Link`: Any party can accept the partially blind signature (S, m, c) as the one produced by the instance of the `Issue` protocol (U, V) if and only if

$$\hat{e}(S, U) = \hat{e}(V, H(m||c))$$

The completeness of the `Link` algorithm can be justified by the equation:

$$\hat{e}(S, U) = \hat{e}(r^{-1}V, r \cdot H_0(m||c)) = \hat{e}(V, H_0(m||c))$$

Obviously, for any valid blind signature (S, m, c), the signer can make a linkage between it and the previous invocation of the partially blind signature issuing protocol (c, U, V) without defeating the protocol. Therefore, the scheme does not achieve the unlinkability property.

The reason why their analysis of the unlinkability goes wrong is that they have not considered the fact that the randomness introduced during the blinding phase can be removed easily by the bilinearity of the pairing operations.

5 Our Proposed Schemes

In this section, we show how to extend the ID-based blind signature in [33] in an elegant way to spawn an unlinkable partially blind signature scheme and an ID-based unlinkable partially blind signature scheme. Define $\mathbb{G}_1, \mathbb{G}_2, \hat{e}$ as in the previous section where $\mathbb{G}_1$ is a GDH group. $H(\cdot)$ and $H_1(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

5.1 ID-Based Partially Blind Signature

`Setup`: The Private Key Generator (PKG) randomly chooses $s \in_R \mathbb{Z}_q^*$ and kept it as the master secret key. The system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_1(\cdot)\}$.

`KeyGen`: The signer with identity $ID \in \{0,1\}^*$ submits ID to PKG. PKG sets the signer's public key Q_{ID} to be $H(ID) \in \mathbb{G}_1$, computes the signer's private signing key S_{ID} by $S_{ID} = sQ_{ID}$ Then PKG sends the private signing key to the signer.

`Issue`: Suppose the requester now wants to get the signature of message m and the requester has already negotiated with the signer ID on the agreed information c to be attached to the message. The interaction between the requester and the signer is as follows:

- `Sign` (Part 1): The signer randomly chooses $r \in_R \mathbb{Z}_q^*$, computes $C = rP$, $Y = rQ_{ID}$ and sends (Y, C) to the requester. Notice that the `Sign` algorithm has not finished yet.
- `Blind`: The requester randomly picks α, β and $\gamma \in_R \mathbb{Z}_q^*$, computes $Y' = \alpha Y + \alpha\beta Q_{ID} - \gamma H(c)$, $C' = \alpha C + \gamma P_{pub}$, $h = \alpha^{-1} H_1(m, Y') + \beta$ and sends h to the signer.
- `Sign` (Part 2): The signer computes $S = (r + h)S_{ID} + rH(c)$ and sends it to the requester. Now the `Sign` algorithm has been finished.
- `Unblind`: Upon the recipient of S, the requester unblinds it by $S' = \alpha S$.

Finally (Y', C', S', m, c) is the partially blind signature of message m and agreed information c.

`Verify`: Any verifier including the requester can verify the partially blind signature by checking whether $\hat{e}(S', P) = \hat{e}(Y' + H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$ is true. If so, the partially blind signature is accepted as valid.

5.2 Partially Blind Signature in Conventional PKI

`Setup`: The system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, H(\cdot), H_1(\cdot)\}$.

`KeyGen`: The signer randomly selects $s \in_R \mathbb{Z}_q^*$ and computes $P_{pub} = sP$ as his/her public verification key. The signing key is s and is kept in secret.

`Issue`: Suppose the requester now wants to get the signature of message m and the requester has already negotiated with the signer with public key P_{pub} on the agreed information c to be attached to the message. The interaction between the requester and the signer is as follows:

- `Sign` (Part 1): The signer randomly chooses $r \in_R \mathbb{Z}_q^*$, computes $Z = H(c)$, $Y = rZ$ and sends Y to the requester. Notice that the `Sign` algorithm has not finished yet.
- `Blind`: The requester randomly picks $\alpha, \beta \in_R \mathbb{Z}_q^*$, computes $Y' = \alpha\ Y\ +\ \alpha\beta\ H(c)$, $h = \alpha^{-1}H_1(m,\ Y')\ +\ \beta$ and sends h to the signer.
- `Sign` (Part 2): The signer computes $S = (r+h)sZ$ and sends it to the requester. Now the `Sign` algorithm has been finished.
- `Unblind`: Upon the recipient of S, the requester unblinds it by $S' = \alpha S$.

Finally (Y', S', m, c) is the partially blind signature of message m and agreed information c.

`Verify`: Any verifier including the requester can verify the partially blind signature by checking whether $\hat{e}(S', P) = \hat{e}(Y' + H_1(m, Y')H(c), P_{pub})$ is true. If so, the partially blind signature is accepted as valid.

6 Analysis of the Proposed Schemes

6.1 Correctness Analysis

For any valid signature produced by our ID-based partially blind signature scheme:

$$\begin{aligned}
\hat{e}(S', P) &= \hat{e}(\alpha S, P) \\
&= \hat{e}((\alpha r + \alpha h)S_{ID} + \alpha r H(c), P) \\
&= \hat{e}((\alpha r + H_1(m, Y') + \alpha\beta)S_{ID}, P)\hat{e}(H(c), \alpha r P) \\
&= \hat{e}((\alpha r + H_1(m, Y') + \alpha\beta)Q_{ID}, P_{pub})\hat{e}(H(c), C' - \gamma P_{pub}) \\
&= \hat{e}((\alpha r + \alpha\beta)Q_{ID} + H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(-\gamma H(c), P_{pub})\hat{e}(H(c), C') \\
&= \hat{e}(\alpha Y + \alpha\beta Q_{ID} - \gamma H(c) + H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C') \\
&= \hat{e}(Y' + H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')
\end{aligned}$$

Similarly, for our partially blind signature scheme in conventional PKI:

$$\begin{aligned}
\hat{e}(S', P) &= \hat{e}(\alpha S, P) \\
&= \hat{e}((\alpha(r + h)sZ, P) \\
&= \hat{e}((\alpha r + \alpha h)Z, P_{pub}) \\
&= \hat{e}((\alpha r + H_1(m, Y') + \alpha\beta)Z, P_{pub}) \\
&= \hat{e}((\alpha r + \alpha\beta)Z + H_1(m, Y')Z, P_{pub}) \\
&= \hat{e}(\alpha Y + \alpha\beta H(c) + H_1(m, Y')H(c), P_{pub}) \\
&= \hat{e}(Y' + H_1(m, Y')H(c), P_{pub})
\end{aligned}$$

6.2 Efficiency Analysis

We consider the costly operations which include point addition on $\mathbb{G}_1$ ($\mathbb{G}_1$ Add), point scalar multiplication on $\mathbb{G}_1$ ($\mathbb{G}_1$ Mul), multiplication in $\mathbb{Z}_q$ ($\mathbb{Z}_q$ Mul), division in $\mathbb{Z}_q$ ($\mathbb{Z}_q$ Div), hashing into the group (Hash) and pairing operation (Pairing). We used the `MapToPoint` hash operation in BLS short signature scheme [6]. Table 1 shows a summary of the efficiency of our proposed schemes. All three algorithms in our scheme in conventional PKI are more efficient than that of ID-based version. Besides, for the signatures of the same agreed information, both of our schemes achieve efficient batch verification [33] as the linkable scheme in [36].

	Efficiency					
Algorithms	G_1 Add	G_1 Mul	Z_q Mul	Z_q Div	Hash	Pairing
ID-based Partially Blind Signature						
`Issue(Signer)`	1	4	0	0	1	0
`Issue(Requester)`	3	6	1	1	1	0
`Verify`	1	1	0	0	1	3
Partially Blind Signature in Conventional PKI						
`Issue(Signer)`	0	2	1	0	1	0
`Issue(Requester)`	1	3	1	1	1	0
`Verify`	1	1	0	0	1	2

Table 1. Efficiency of our proposed schemes

6.3 Existential Unforgeability of our ID-based Partially Blind Signature

Theorem 1 *In the random oracle model (the hash functions are modeled as random oracles), if there is an algorithm $\mathcal{A}$ for an adaptively chosen message and given ID attack to our scheme, with an advantage $\geq \epsilon = 10q_I(q_S+1)(q_S+q_H)/2^k$ within a time span t for a security parameter k; and asking at most q_I identity hashing queries, at most q_E key extraction queries, at most q_H H_1 queries, q_S `Issue` queries and q_V `Verify` queries. Then, there exists an algorithm $\mathcal{C}$ that can solve the CDH problem in expected time $\leq 120686q_Hq_I2^kt/\epsilon(2^k-1)$.*

Proof. See the appendix. □

6.4 Existential Unforgeability of our Partially Blind Signature in Conventional PKI

Theorem 2 *In the random oracle model (the hash functions are modeled as random oracles), if there is an algorithm $\mathcal{A}$ for an adaptively chosen message attack to our scheme, with an advantage $\geq \epsilon = 10q_I(q_S+1)(q_S+q_H)/2^k$ within a time span t for a security parameter k; and asking at most q_I H queries, at most q_H H_1 queries, q_S `Issue` queries and q_V `Verify` queries. Then, there exists an algorithm $\mathcal{C}$ that can solve the CDH problem in expected time $\leq 120686q_Hq_I2^kt/\epsilon(2^k-1)$.*

Proof. The proof is similar to that of Theorem 1. See the appendix. □

6.5 Partial Blindness

Theorem 3 *Our ID-based partially blind signature scheme satisfies the partial blindness property.*

Proof. See the appendix. □

Theorem 4 *Our partially blind signature scheme in conventional PKI satisfies the partial blindness property.*

Proof. The proof is similar to that of Theorem 3. See the appendix. □

6.6 Changing Agreed Information Attack

Changing agreed information attack is the attack in which the requester, after obtained the signature issued by the signer, can subsequently change the agreed information c to another one c' on his/her wish, yet the signature remains valid. In both of our schemes, since r (in ID-based scheme) and s (in conventional scheme) are unknown to the requester, changing $H(c)$ to $H(c')$ involves solving the CDH problem, which is computationally infeasible.

7 Conclusion

In this paper, we presented an attack that revokes the unlinkability of Zhang, Safavi-Naini and Susilo's partially blind signature and pointed out why the security proof provided in [36] is incorrect. Then, we propose two modified schemes which have the property of unlinkability. One is a partially blind signature scheme in conventional PKI while another one is the first ID-based partially blind signature scheme ever exists. The proposed schemes are provably secure in the random oracle model. Future research directions include investigating the novel parallel one-more signature forgery attack and finding a formal proof against this attack on our modified schemes.

Acknowledgement

The authors would like to thank Dr. F. Zhang for pointing out the mistake of an earlier version of this paper by showing a changing agreed information attack on the scheme.

References

1. Masayuki Abe and Eiichiro Fujisaki. How to Date Blind Signatures. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT 1996, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, volume 1163 of *Lecture Notes in Computer Science*. Springer, 1996.
2. Masayuki Abe and Tatsuaki Okamoto. Provably Secure Partially Blind Signatures. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*. Springer, 2000.
3. Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *The First ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
4. Alexandra Boldyreva. Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-Group Signature Scheme. In Yvo Desmedt, editor, *Public Key Cryptography - PKC 2003, Sixth International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings*, volume 2567 of *Lecture Notes in Computer Science*. Springer, 2002.
5. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*. Springer, 2003.
6. Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*. Springer, 2001.
7. Xavier Boyen. Multipurpose Identity-Based Signcryption : A Swiss Army Knife for Identity-Based Cryptography. In Dan Boneh, editor, *23rd International Conference on Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 382–398. Springer Verlag, 2003.
8. Jae Choon Cha and Jung Hee Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups . In Yvo Desmedt, editor, *Public Key Cryptography - PKC 2003, Sixth International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings*, volume 2567 of *Lecture Notes in Computer Science*. Springer, 2002.
9. David Chaum. Blind Signature System. In David Chaum, editor, *Advances in Cryptology, Proceedings of Crypto 1983*, pages 153–153, New York, 1984. Plenum Press.
10. David Chaum. Showing Credentials without Identification Transferring Signatures between Unconditionally Unlinkable Pseudonyms. In Jennifer Seberry and Josef Pieprzyk, editors, *Advances in Cryptology - AUSCRYPT '90, International Conference on Cryptology, Sydney, Australia, January 8-11, 1990, Proceedings*, volume 453 of *Lecture Notes in Computer Science*. Springer, 1990.
11. David Chaum, Amos Fiat, and Moni Naor. Untraceable Electronic Cash. In Shafi Goldwasser, editor, *Advances in Cryptology - CRYPTO 1988, Eighth Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*. Springer, 1990.
12. Xiaofeng Chen, Fangguo Zhang, and Kwangjo Kim. ID-based Multi-Proxy Signature and Blind Multisignature from Bilinear Pairings. In *KIISC conference 2003, Korea, August 17, 2003*, 2003.
13. Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2003.
14. Dang Nguyen Duc, Jung Hee Cheon, and Kwangjo Kim. A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption. In Robert H. Deng, Sihan Qing, Feng Bao, and Jianying Zhou, editors, *Information and Communications Security, Fifth International Conference, ICICS 2003, Huhehaote City, Inner-Mongolia, October 10-13, 2003, Proceedings*, volume 2836 of *Lecture Notes in Computer Science*. Springer, 2003.
15. Chun-I Fan and Chin-Laung Lei. Low-Computation Partially Blind Signatures for Electronic Cash. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, 1998.
16. Yair Frankel, Yiannis Tsiounis, and Moti Yung. "Indirect Discourse Proof": Achieving Efficient Fair Off-Line E-cash. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security,*

Kyongju, Korea, November 3-7, 1996, Proceedings, volume 1163 of *Lecture Notes in Computer Science*. Springer, 1996.
17. Patrick Horster, Markus Michels, and Holger Petersen. Hidden Signature Schemes Based on the Discrete Logarithm Problem and Related Concepts. Technical Report TR-94-40-R, Theoretical Computer Science and Information Security, Department of Computer Science, University of Technology Chemnitz-Zwickau, Germany, April 1995. Technical Report.
18. Patrick Horster and Holger Petersen. Classification of Blind Signature Schemes and Examples of Hidden and Weak Blind Signatures. Technical Report TR-94-1-E, Theoretical Computer Science and Information Security, Department of Computer Science, University of Technology Chemnitz-Zwickau, Germany, April 1994. Technical Report.
19. Wen-Shenq Juang and Chin-Laung Lei. A Secure and Practical Electronic Voting Scheme for Real World Environments. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, 1997.
20. Jinho Kim, Kwangjo Kim, and Chulsoo Lee. An Efficient and Provably Secure Threshold Blind Signature. In Kwangjo Kim, editor, *Information Security and Cryptology - ICISC 2001, Fourth International Conference, Seoul, Korea, December 6-7, 2001, Proceedings*, volume 2288 of *Lecture Notes in Computer Science*. Springer, 2002.
21. József Lenti, István Loványi, and Ákos Nagy. Blind Signature Based Steganographic Protocol. In *Proceedings of IEEE International Workshop on Intelligent Signal Processing, Budapest, Hungary 24-25 May 2001*, 2001.
22. Anna Lysyanskaya and Zulfikar Ramzan. Group Blind Digital Signatures: A Scalable Solution to Electronic Cash. In Rafael Hirschfeld, editor, *Financial Cryptography, Second International Conference, FC 1998, Anguilla, British West Indies, February 23-25, 1998, Proceedings*, volume 1465 of *Lecture Notes in Computer Science*, pages 184–197. Springer, 1998.
23. Wakaha Ogata and Kaoru Kurosawa. Oblivious Keyword Search. Cryptology ePrint Archive, Report 2002/182, 2002. Available at http://eprint.iacr.org.
24. David Pointcheval and Jacques Stern. Provably Secure Blind Signature Schemes. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT 1996, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, volume 1163 of *Lecture Notes in Computer Science*. Springer, 1996.
25. David Pointcheval and Jacques Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology: The Journal of the International Association for Cryptologic Research*, 13(3):361–396, 2000.
26. Tomas Sander, Amnon Ta-Shma, and Moti Yung. Blind, Auditable Membership Proofs. In Yair Frankel, editor, *Financial Cryptography, Fourth International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings*, volume 1962 of *Lecture Notes in Computer Science*, pages 53–71. Springer, 2001.
27. Claus-Peter Schnorr. Security of Blind Discrete Log Signatures against Interactive Attacks. In Sihan Qing, Tatsuaki Okamoto, and Jianying Zhou, editors, *Information and Communications Security, Third International Conference, ICICS 2001, Xian, China, November 13-16, 2001*, volume 2229 of *Lecture Notes in Computer Science*. Springer, 2001.
28. Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO 1984, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 19–22 August 1985.
29. Markus A. Stadler, Jean-Marc Piveteau, and Jan L. Camenisch. Fair Blind Signatures. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology - EUROCRYPT 1995, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, volume 921 of *Lecture Notes in Computer Science*, pages 209–219, Berlin, 1995. Springer-Verlag.
30. Duc Liem Vo, Fangguo Zhang, and Kwangjo Kim. A New Threshold Blind Signature Scheme from Pairings. In *Symposium on Cryptography and Information Security, SCIS2003, Jan.26-29, 2003, Itaya, Japan*, volume 1/2, 2003.
31. Sebastiaan von Solms and David Naccache. On Blind Signatures and Perfect Crimes. *Journal of Computer and Security*, 11:581–583, 1992.
32. Yan Xie, Fangguo Zhang, Xiaofeng Chen, and Kwangjo Kim. ID-based Distributed 'Magic Ink' Signature. In Robert H. Deng, Sihan Qing, Feng Bao, and Jianying Zhou, editors, *Information and Communications Security, Fifth International Conference, ICICS 2003, Huhehaote City, Inner-Mongolia, October 10-13, 2003*, volume 2836 of *Lecture Notes in Computer Science*. Springer, 2003.

33. Fangguo Zhang and Kwangjo Kim. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings. In Reihaneh Safavi-Naini and Jennifer Seberry, editors, *Information Security and Privacy, Eighth Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003, Proceedings*, volume 2727 of *Lecture Notes in Computer Science*. Springer, 2003.
34. Fangguo Zhang, Rei Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In *Public Key Cryptography - PKC 2004, Seventh International Workshop on Theory and Practice in Public Key Cryptography, Singapore 1-4 March, 2004, Proceedings*, Lecture Notes in Computer Science. Springer, 2004. to appear.
35. Fangguo Zhang, Reihaneh Safavi-Naini, and Chih-Yin Lin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/104, 2003. Available at http://eprint.iacr.org.
36. Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. In *Progress in Cryptology - INDOCRYPT 2003, Fourth International Conference on Cryptology in India, New Delhi, India, December 8-10, 2002*, volume 2904 of *Lecture Notes in Computer Science*. Springer, 2003.
37. Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings – revised version, 2004. Available at http://www.uow.edu.au/fangguo.
38. Tan Zuo-Wen, Liu Zhuo-Jun, and Tang Chun-Ming. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP and its Applications. Technical Report 21, Mathematics-Mechanization Research Center (MMRC), Institute of Systems Sciences, Chinese Academy of Sciences, Beijing, China, December 2002. Preprint.

Appendix

Proof of Theorem 1
We assume that the challenger $\mathcal{C}$ receives a random instance (P, aP, bP) of the CDH problem and has to compute abP. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the EUF-IDPB-CMA2 game. We will describe how $\mathcal{C}$ simulates the role of the challenger below, with the following assumptions:

1. $\mathcal{A}$ will ask for $H(ID)$ before ID is used in any `Issue`, `Verify` and `Extract` queries.
2. $\mathcal{A}$ will not ask for `Extract`(ID) again if the query `Extract`(ID) has been already issued before.

Public key and private key of the signer: $\mathcal{C}$ gives $\mathcal{A}$ the system parameters $P_{pub} = aP$. Note that a is unknown to $\mathcal{C}$. This value simulates the master key value for the PKG in the game.

H_1 requests: $\mathcal{C}$ will answer H_1 requests randomly, but to maintain the consistency and to avoid collision, $\mathcal{C}$ keeps a list L_1 to store the answers used. The same answer from the list L_1 will be given if the request has been asked before. Otherwise, a new value that does not appear in the list will be generated as the answer to $\mathcal{A}$, this new value and the corresponding request will then be stored in the list L_1 for later queries of the same request.

H requests and `Extract` requests: Similarly, when $\mathcal{A}$ asks queries on the hash values of identities, $\mathcal{C}$ checks another list L_2, If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a value c_i from $\mathbb{F}_q^*$ will be randomly generated and c_iP will be used as the answer, the query and the answer will then be stored in the list. Note that the associated private key is c_iaP which $\mathcal{C}$ knows how to compute.

The only exception is that $\mathcal{C}$ has to randomly choose one of the H queries from $\mathcal{A}$, say the i-th query, and answers $H(ID_i) = bP$ for this query. Since bP is a value in a random instance of the CDH problem, it does not affect the randomness of the hash function H. Since both a and b are unknown to $\mathcal{C}$, an `Extact` request on this identity will make $\mathcal{C}$ fails.

`Issue` requests: For an `Issue` request on (ID_j, m, c), $\mathcal{C}$ first randomly generates two values y_j and z_j, then simulates the value of $H_1(m, Y')$ and $H(c)$ in the way as mentioned above. (Y', C', S', m, c) will be used as the answer, where $Y' = y_jP - H_1(m, Y')H_1(c)H(ID_j)$, $C' = z_jP$ and $S' = y_j(aP) + z_jH(c)$.

`Verify` requests: For `Verify` request on (ID_j, m, c), $\mathcal{C}$ first checks the lists L_1, L_2 and rejects the signature if at least one of the tuple (m, Y') and (c) is not found in the corresponding list. Assume the answer of the H_1 query of (m, Y') is h_m and that of (c) is H_c, $\mathcal{C}$ just checks whether $\hat{e}(S', P) = \hat{e}(Y' + h_mH(ID_j), aP)\hat{e}(H_c, C')$ and returns $\top$ or $\perp$ accordingly.

We follow the same idea used in [7] to coalesce the signing identity ID_i and message m into a "generalized" forged message (ID_i, m) so as to hide the ID-based aspect of the EUF-IDPB-CMA2 attacks, and simulate the setting of an identity-less adaptive-CMA existential forgery for which the forking lemma is proven. Assume the adversary $\mathcal{A}$ can forge a valid signature $((ID_i, m), c, h, Y, C, S)$, it follows from the forking lemma [25] that if $\mathcal{A}$ is a sufficiently efficient forger in the above interaction, then we can construct a Las Vegas machine $\mathcal{A}'$ that outputs two signed messages $((ID_i, m), c, h, Y, C, S)$ and $((ID_i, m), c, h', Y', C', S')$ with $h \neq h'$.

Finally, to solve the CDH problem given the machine $\mathcal{A}'$, we construct a machine $\mathcal{C}$' as follows.

1. $\mathcal{C}'$ runs $\mathcal{A}'$ to obtain two distinct forgeries $((ID_i, m), c, h, Y, S)$ and $((ID_i, m), c, h', Y', S')$.
2. $\mathcal{C}'$ derives the value of abP by $(h - h')^{-1}(S - S')$, as both of $(P, aP, Y + hbP, S - rH(c))$ and $(P, aP, Y' + h'bP, S' - rH(c))$ are valid Diffie-Hellman tuples.

Now we consider the probability for $\mathcal{C}$ to successfully solve the given CDH problem. Since H is a random oracle, given that $\mathcal{A}$ have forged a valid signature of ID_i, the probability that $\mathcal{A}$ knows the value of $H(ID_i)$ without making any H query of ID_i is $(2^k - 1)/2^k$. Moreover, since the index i of ID_i is independently and randomly chosen, the probability of $\mathcal{A}$ to forge the signature of ID_i is at least $1/q_I$. Take both probabilities into account, $\mathcal{C}$'s probability of success is $(2^k - 1)/q_I 2^k$.

Based on the bound from the forking lemma [25] and the above probability of success, if $\mathcal{A}$ succeeds in time $\leq t$ with probability $\geq \epsilon = 10q_I(q_S + 1)(q_S + q_H)/2^k$, then $\mathcal{C}$ can solve the CDH problem in expected time $\leq 120686 q_H q_I 2^k t/\epsilon(2^k - 1)$. □

Proof of Theorem 2
We assume that the challenger $\mathcal{C}$ receives a random instance (P, aP, bP) of the CDH problem and has to compute the value of abP. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the EUF-PB-CMA2 game. $\mathcal{C}$ simulates the role of challenger as described below.

Public key and private key of the signer: $\mathcal{C}$ gives $\mathcal{A}$ the system parameters with its public key $P_{pub} = aP$. Note that a is unknown to $\mathcal{C}$. This value simulates the private key value in the game.

H_1 requests: $\mathcal{C}$ will answer each H_1 requests randomly. Similar to the proof in Theorem 1, $\mathcal{C}$ keeps a list L_1 of the answers with the corresponding queries to maintain the consistency and to avoid collision.

H requests: Similarly, $\mathcal{A}$ keeps a list L_2 for answering H request. The only exception is that $\mathcal{C}$ has to randomly choose one of the H queries from $\mathcal{A}$, say the i-th query, and answers $H(c_i) = bP$ for this query. Since bP is a value in a random instance of the CDH problem, it does not affect the randomness of the hash function H.

`Issue` requests: For an `Issue` request on (m, c), $\mathcal{C}$ first randomly generates a value y_j, then simulates the value of $H_1(m, Y')$ and $H(c)$ in the way as mentioned above. (Y', S', m, c) will be used as the answer, where $Y' = y_j P - H_1(m, Y')H(c)$ and $S' = y_j(aP)$.

`Verify` requests: For `Verify` request on (P_{pub}, m, c), $\mathcal{C}$ first checks the list L_1 and rejects the signature if at least one of the tuple (m, Y') and (c) is missing. Then $\mathcal{C}$ just checks whether $\hat{e}(S', P) = \hat{e}(Y' + H_1(m, Y')H(c), aP)$ and returns $\top$ or $\bot$ accordingly.

It follows from the forking lemma [25] that if $\mathcal{A}$ is a sufficiently efficient forger in the above interaction, then we can construct a Las Vegas machine $\mathcal{A}'$ that outputs two signed messages (m, c, h, Y, S) and (m, c, h', Y', S') with $h \neq h'$.

Finally, to solve the CDHP given the machine $\mathcal{A}'$, we construct a machine $\mathcal{C}'$ as follows.

1. $\mathcal{C}'$ runs $\mathcal{A}'$ to obtain two distinct forgeries (m, c, h, Y, C, S) and (m, c, h', Y', C', S').
2. $\mathcal{C}'$ derives the value of abP by $(h - h')^{-1}(S - S')$, as both of $(P, aP, Y + hbP, S)$ and $(P, aP, Y' + h'bP, S')$ are valid Diffie-Hellman tuples.

Now we consider the probability for $\mathcal{C}$ to successfully solve the given CDH problem. Since H is a random oracle, given that $\mathcal{A}$ have forged a valid signature of a certain message with agreed information c_i attached, the probability that $\mathcal{A}$ knows the value of $H(c)$ without

making any H query of c is $(2^k-1)/2^k$. Moreover, since the index i of c_i is independently and randomly chosen, the probability of $\mathcal{A}$ to forge the signature of a certain message with agreed information c_i attached is at least $1/q_I$. Take both probabilities into account, $\mathcal{C}$'s probability of success is $(2^k-1)/q_I 2^k$.

Based on the bound from the forking lemma [25] and the above probability of success, if $\mathcal{A}$ succeeds in time $\leq t$ with probability $\geq \epsilon = 10q_I(q_S+1)(q_S+q_H)/2^k$, then $\mathcal{C}$ can solve the CDH problem in expected time $\leq 120686 q_H q_I 2^k t/\epsilon(2^k-1)$. □

Proof of Theorem 3

Considering the `Issue` algorithm of our scheme, we can prove that the signer can learn no information on the message to be signed similar to the proof of blindness property in [33].

Given a signature (Y', C', S', m, c) and any view (Y, C, S, h), consider the following equations:

$$S' = \alpha S \tag{1}$$

$$C' = \alpha C + \gamma P_{pub} \tag{2}$$

$$h = (\alpha^{-1} H_1(m, Y') + \beta) \pmod q \tag{3}$$

$$Y' = \alpha Y + \alpha\beta Q_{ID} - \gamma H(c) \tag{4}$$

For any valid signature and any view, we know that we must be able to find an unique $\alpha' \in \mathbb{Z}_q^*$ such that Eq (1) holds. Moreover, we can get an unique $\beta' \in \mathbb{Z}_q^*$ and an unique $\gamma' \in \mathbb{Z}_q^*$ while the values are determined by the equations $\beta' = h - (\alpha')^{-1} H_1(m, Y')$ and $\gamma' P_{pub} = C' - \alpha C$.

Since (Y', C', S', m, c) is a valid signature, $\hat{e}(S', P) = \hat{e}(Y' + H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$ holds, i.e. $\hat{e}(S', P) = \hat{e}(Y', P_{pub})\hat{e}(H_1(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$, this result will be used below.

Now we consider whether Eq (4) holds for α' and β' we have found:

$$\begin{aligned}
&\hat{e}(\alpha' Y + \alpha'\beta' Q_{ID} - \gamma' H(c), P_{pub}) \\
&= \hat{e}(\alpha' Y + \alpha'(h - (\alpha')^{-1} H_1(m, Y'))Q_{ID} - \gamma' H(c), P_{pub}) \\
&= \hat{e}(\alpha' r Q_{ID} + \alpha' h Q_{ID} - \gamma' H(c), P_{pub})\hat{e}(H_1(m, Y')Q_{ID}, P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r+h)Q_{ID}, P_{pub})\hat{e}(H_1(m, Y')Q_{ID}, P_{pub})^{-1}\hat{e}(-\gamma H(c), P_{pub}) \\
&= \hat{e}(\alpha'(r+h)Q_{ID}, P_{pub})\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub})\hat{e}(H(c), C')\hat{e}(H(c), -\gamma P_{pub}) \\
&= \hat{e}(\alpha'(r+h)S_{ID}, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub})\hat{e}(H(c), \alpha C) \\
&= \hat{e}(\alpha'(r+h)S_{ID}, P)\hat{e}(\alpha' r H(c), P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha' S, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(S', P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(Y', P_{pub})
\end{aligned}$$

The above equation is valid since we can always find r such that $rQ_{ID} = Y$ and we must have $S = (r+h)S_{ID} + rH(c)$ for any valid view of the protocol signing on a certain message with agreed information c.

By the non-degeneracy of bilinear pairing, we know that

$$\hat{e}(Y', P_{pub}) = \hat{e}(\alpha' Y + \alpha'\beta' H(c), P_{pub}) \Leftrightarrow Y' = \alpha' Y + \alpha'\beta' H(c)$$

Hence the blind factors α, β and γ always exist which lead to the same relation defined in `Issue`, so any view of the `Issue` protocol is *unlinkable* to any valid signature.

Consider again the *Unlinkability Game*, the signature of m_b is associated with the instance of the signing protocol that produces the signature of m_b and that of m_{1-b} with equal probability since we can always find the corresponding blind factors α and β, we therefore claim that the advantage of $\mathcal{A}$ in the game is negligible. □

Proof of Theorem 4
Considering the `Issue` algorithm of our scheme, we can prove that the signer can learn no information on the message to be signed similar to the proof of theorem 3.

Given a valid signature (Y', S', m, c) and any view (Y, h, S), consider the following equations:

$$S' = \alpha S \tag{5}$$

$$h = (\alpha^{-1} H_1(m, Y') + \beta) \pmod q \tag{6}$$

$$Y' = \alpha Y + \alpha\beta H(c) \tag{7}$$

We know that we must be able to find an unique $\alpha' \in \mathbb{Z}_q^*$ such that Eq (5) holds. Moreover, we can get an unique $\beta' \in \mathbb{Z}_q^*$ while the value is determined by the equation $\beta' = h - (\alpha')^{-1} H_1(m, Y')$.

Since (Y', S', m, c) is a valid signature, we have $\hat{e}(S', P) = \hat{e}(Y' + H_1(m, Y')H(c), P_{pub})$, i.e. $\hat{e}(S', P) = \hat{e}(Y', P_{pub})\hat{e}(H_1(m, Y')H(c), P_{pub})$, this result will be useful shortly afterward.

Now we consider whether Eq (7) holds for α' and β' we have found:

$$\begin{aligned}
&\hat{e}(\alpha' Y + \alpha'\beta' H(c), P_{pub}) \\
&= \hat{e}(\alpha' Y + \alpha'(h - (\alpha')^{-1} H_1(m, Y'))H(c), P_{pub}) \\
&= \hat{e}(\alpha' r H(c) + \alpha' h H(c), P_{pub})\hat{e}(H_1(m, Y')H(c), P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r + h)H(c), P_{pub})\hat{e}(H_1(m, Y')H(c), P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r + h)H(c), P_{pub})\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha'(r + h)sH(c), P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha' S, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(S', P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(Y', P_{pub})
\end{aligned}$$

The above equation is valid since we can always find r such that $rH(c) = Y$ and we must have $S = (r + h)sH(c)$ for any valid view of the protocol signing on a certain message with agreed information c.

By the non-degeneracy of bilinear pairing, we know that

$$\hat{e}(Y', P_{pub}) = \hat{e}(\alpha' Y + \alpha'\beta' H(c), P_{pub}) \Leftrightarrow Y' = \alpha' Y + \alpha'\beta' H(c)$$

Hence the blind factors α, β always exist which lead to the same relation defined in `Issue`, so any view of the `Issue` protocol is *unlinkable* to any valid signature.

Consider again the *Unlinkability Game*, the signature of m_b is associated with the instance of the signing protocol that produces the signature of m_b and that of m_{1-b} with equal probability since we can always find the corresponding blind factors α and β, we therefore claim that the advantage of $\mathcal{A}$ in the game is 0. □