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
The University of Hong Kong
Pokfulam, Hong Kong
{smchow, hui, smyiu, chow}@cs.hku.hk

Abstract. A blind signature scheme is a protocol for obtaining a digital signature from a signer, but the signer can neither learn the messages he/she sign nor the signatures the recipients obtain afterwards. Partially blind signature is a variant such that part of the message contains pre-agreed information (agreed by the signer and the signature requester) in unblinded form, while threshold blind signature distributes the signing power to a group of signers such that a signature can only be produced by interacting with a predetermined numbers of signers. In this paper, we propose a threshold partially blind signature scheme from bilinear pairings and an ID-based partially blind signature scheme, which are provably secure in the random oracle model. To the best of authors' knowledge, we give the first discussion on these two notions.

Key words: threshold partially blind signature, identity-based partially blind signature, bilinear pairings

1 Introduction

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 (e.g. [8]), unlinkable credentials (e.g. [7]), anonymous multiple choice electronic voting (e.g. [16]), oblivious keyword search (e.g. [21]), anonymous fingerprinting (e.g. [34]) or even in steganographic protocol (e.g. [18]).

The basic idea of most existing blind signature schemes is as follows. The requester (of the signature) randomly chooses some random factors and embeds them to the message to be signed. The random factors are kept in secret so the signer cannot recover the message. Using the blinded signature returned by the signer, the requester can remove the random factors introduced and get a valid signature. However, the property that requesters can ask the signer to blindly sign any message is undesirable in some situations. Consider using blind signature to design a e-cash scheme, expiry date information should be embedded in the e-cash issued, or there may be unlimited growth of the bank's database for double-spending checking. Besides, the possibility of including embedded information may provide a more convenient way for inscribing the face value of the e-cash to the blind signature. Hence it is more flexible if the

* This research is supported in part by the Areas of Excellence Scheme established under the University Grants Committee of the Hong Kong Special Administrative Region (HKSAR), China (Project No. AoE/E-01/99), two grants from the Research Grants Council of the HKSAR, China (Project No. HKU/7144/03E and HKU/7136/04E), and two grants from the Innovation and Technology Commission of the HKSAR, China (Project No. ITS/170/01 and UIM/145).

message to be signed is not "completely blind" and is able to embed some agreed information, which motivated the introduction of partially blind signature [1].

Recently, some pairing-based blind signature schemes were proposed, such as threshold blind signature in [31] and partially blind signature in [41]. Compared with previous blind signature schemes based on other difficult problems, their work have some nice properties like short signature size. In this paper, we propose two improved partially blind signature schemes from bilinear pairings.

1.1 Related Work

Blind signature schemes were classified into four main classes by [15], namely, hidden, weak blind, interactive blind and strong blind. In another criterion [14], hidden signature was further divided into message hidden signatures and parameter hidden signatures. Several hidden and weak blind signature schemes had been discussed in [14, 15] as well. Pointcheval and Stern presented the formal definition and the security notion for blind signature in [23]. Unfortunately, [26] showed an inherent weakness in their result and presented a novel parallel one-more signature forgery attack. A blind signature scheme using bilinear pairings was proposed in [3].

Some schemes were devised to solve the perfect crime resulting from the unconditional anonymity provided by the blind signature [32], such as fair blind signature in [30], indirect discourse proofs in [12] and "magic ink" signature in [35]. Partially blind signature was introduced in [1], together with a RSA-based scheme. This notion was formalized in [2], a discrete-logarithm based scheme that is provably secure was also proposed.

Another line of research efforts were done in combining the properties of other classes of cryptographic schemes into blind signatures. In proxy blind signature ([39] and [42]), the signer delegates his/her signing power to a proxy, who blindly signs a message on behalf of the original signer. In [10] and [11], forward-secure blind signature scheme were proposed to address key exposure problem, in which all previously generated signatures are still considered to be valid even the secret key is compromised. They give an extra level of security to normal blind signature. Unfortunately, [11] was shown to be insecure by [19]. Group oriented blind signatures have been studied as well. Blind threshold signature that enables any t out of n legitimate signers to give a blind signature, was considered in [17] and [31]. Blind threshold-ring signature providing signer-ambiguity was considered in [6]. Blind multisignature was proposed in [9] and group blind signature was proposed in [20].

As an alternative to conventional public key infrastructure (PKI), Shamir introduced identity-based (ID-based) signature schemes [29] and the design of ID-based schemes have attracted a lot of attention recently (e.g. [9, 35–37]). 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 was proposed by Zhang and Kim in [37] and ID-based blind signcryption was proposed in [36].

Apart from blind signature schemes, there are other primitives that provide anonymity by cryptographic means. An example is blind auditable membership proofs [25], in which the problem of achieving anonymity and audibility at the same time is addressed. In verifiably encrypted signature (for examples, [4] and [41]), 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.

1.2 Our Contribution

We propose two new partially blind signature schemes. The first one is a PKI-based partially blind signature scheme from bilinear pairings, which is more efficient for the signature requesters' side than the existing scheme [41]. Moreover, we discuss how to extend the scheme into a threshold partially blind signature scheme. The second proposed scheme is an ID-based partially blind signature scheme. To the best of authors' knowledge, our schemes are the first of their kind.

1.3 Organization

The rest of the paper is organized as follows. The next section contains some preliminaries about the framework of (ID-based) partially blind signature schemes, bilinear pairing as well as the Gap Diffie-Hellman group. Formal definitions of security describing the adversary's capabilities are presented in Section 3. In Section 4, a PKI-based partially blind signature scheme and an ID-based partially blind signature scheme are proposed. The security and efficiency analysis of our schemes are given in Section 5. Finally, Section 6 concludes our paper.

2 Preliminaries

2.1 Framework of Partially Blind Signature

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 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 input x, it outputs the signer's secret signing key sk and its corresponding public verification key 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 agreed information c will be produced too if it is not given.
  - `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, a negotiated 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 the partially blind signature, i.e. if $(\sigma, c) = \texttt{Issue}(m, r, sk)$, $\texttt{Verify}(pk, m, c, \sigma) = \top$ must hold. Security requirements will be described in Section 3.

2.2 Framework of ID-based Partially Blind Signature

The framework of ID-based partially blind signature schemes is similar to that of its PKI counterpart. The differences are described below.

– `Setup`: This algorithm is usually executed by the private key generator (PKG). On an unary string input 1^k where k is a security parameter, it produces the 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 too, which is kept secret.
– `KeyGen`: On an arbitrary string input ID, it computes the private signing key S_{ID} with the help of master secret s, and the corresponding public verification key Q_{ID}, with respect to *params*.

2.3 Bilinear Pairing and Gap Diffie-Hellman Groups

Bilinear pairing is an important cryptographic primitive (see [3, 4, 9, 10, 31, 35–41]). 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 $\mathbb{G}_1$ and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman (DDH) problem is to decide if $c = ab$.*

Definition 2. *Given a generator P of a group $\mathbb{G}_1$, (P, aP, bP, cP) is defined as a valid Diffie-Hellman tuple if $c = ab$.*

Definition 3. *Given a generator P of a group $\mathbb{G}_1$ and a 2-tuple (aP, bP), the Computational Diffie-Hellman (CDH) problem is to compute abP.*

Definition 4. *If $\mathbb{G}_1$ 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 $\mathbb{G}_1$ 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 DDH problem in polynomial time.

2.4 Notations

The definitions of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\hat{e}(\cdot,\cdot)$ will be used throughout the rest of the paper. Besides, we let $H(\cdot)$ and $H_0(\cdot)$ be two cryptographic hash functions where $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $H : \{0,1\}^* \rightarrow \mathbb{G}_1$.

3 Formal Security Model

3.1 Unforgeability of PKI-based Partially Blind Signature

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 $\mathcal{A}$. We adopt a similar notion as [2].

EUF-PB-CMA2 Game:

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

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of the following types of queries in an adaptive manner (i.e. each query may depend on the responses to the previous queries).

- Hash functions queries: $\mathcal{A}$ can ask for the value of the hash functions $H(\cdot)$ and $H_0(\cdot)$ in our schemes) for the requested input.
- `Issue`: $\mathcal{A}$ chooses a public key pk, a plaintext m and the 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 5. *An partially blind scheme is said to be existential unforgeable against adaptive chosen-message attacks property if no adversary has a non-negligible advantage in the EUF-PB-CMA2 game.*

3.2 Unforgeability of ID-based Partially Blind Signature

Signature non-repudiation of an ID-based partially blind signature scheme is formally defined in terms of the *existential unforgeability of ID-based partially blind signature under adaptive chosen-message-and-identity attack* (EUF-IDPB-CMIA2) game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. We extend the notion in [2] to the ID-based settings.

EUF-IDPB-CMIA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate 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 the following types of queries in an adaptive manner (i.e. each query may depend on the responses to the previous queries).

– Hash functions queries: $\mathcal{A}$ can ask for the value of the hash functions ($H(\cdot)$ and $H_0(\cdot)$ in our schemes) for the requested input.
– `KeyGen`: $\mathcal{A}$ chooses an identity ID. $\mathcal{C}$ computes $\texttt{Extract}(ID) = S_{ID}$ and sends the result to $\mathcal{A}$. The corresponding public verification key Q_{ID} can be calculated by using the hash function $H(\cdot)$.
– `Issue`: $\mathcal{A}$ chooses an identity ID, a plaintext m and the 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 6. *An ID-based partially blind scheme is said to be existential unforgeable against adaptive chosen-message-and-identity attacks if no adversary has a non-negligible advantage in the EUF-IDPB-CMIA2 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 the 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. For the scheme to be practical, the cardinality of the finite agreed information space should be small compared with the anticipated number of total `Issue` requests. This weakness is inherent to any partial blind signature schemes as it is the price for embedding agreed information to the message to be signed.

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 $\mathcal{A}$. Again, we adopt a similar notion as [2].

Unlinkability Game:

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

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 an identity ID and sends them to $\mathcal{C}$.

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 $\mathcal{C}$ unblinds both signatures, it presents the signature of m_b to $\mathcal{A}$.

Response: The adversary $\mathcal{A}$ returns the guess b' and wins 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 any adversary has zero advantage in the UL game.*

4 Our Proposed Schemes

4.1 PKI-based Partially Blind Signature

`Setup`: The system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, H(\cdot), H_0(\cdot)\}$.

`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 $\alpha \in_R \mathbb{Z}_q^*$ and $\beta \in_R \mathbb{Z}_q^*$, sends $h = \alpha^{-1}H_0(m, Y') + \beta$ to the signer and computes $Y' = \alpha Y + \alpha\beta H(c)$.
- `Sign` (Part 2): The signer computes $S = (r + h)sZ$ and sends it to the requester. Now the `Sign` algorithm has been finished.
- `Unblind`: The requester unblinds the received S 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 signature requester) can verify the validity of the partially blind signature by checking whether $\hat{e}(S', P) = \hat{e}(Y' + H_0(m, Y')H(c), P_{pub})$ is true. If so, the partially blind signature is accepted as valid.

4.2 Threshold Partially Blind Signature

To extend our proposed partially blind signature scheme into the threshold version, we need the help of the following techniques in threshold cryptography.

Polynomial Interpolation Secret Sharing [28]: Many threshold schemes are based on Shamir's secret sharing, which is derived from the concept of Lagrange polynomial interpolation.

For a (t, n) instantiation (i.e. any t out of n pieces of share can be used to reconstruct the secret, but no one can get the secret with the knowledge of only $t-1$ of them), a trusted dealer first selects t random coefficients $a_0, a_1, \cdots, a_{t-1}$ from $\mathbb{Z}_q$ where a_0 is the master secret to be shared. Then n different public points $x_{i_j} \in \mathbb{Z}_q^*$ are chosen (where $1 \le j \le n$), one for each participant. Let f be a polynomial of degree $t-1$ and $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$, the share to be distributed to the participant with public point x_{i_j} assigned is $f(x_{i_j})$.

When t participants decided to reconstruct the secret, they can do so by recovering the polynomial. With the knowledge of t points $(x_{i_j}, f(x_{i_j}) = s_{i_j})$ on the curve, the coefficients $(a_0, \cdots, a_t)$ of f are uniquely determined and can be computed by the Lagrange interpolation of these t points by using the below formula.

$$f(x) = \sum_{j=1}^{t} s_{i_j} \prod_{1 \le l \le t, l \ne j} \frac{x - x_{i_l}}{x_{i_j} - x_{i_l}}.$$

Thus the secret $a_0 = f(0)$ can be obtained by $\sum_{j=1}^{t} b_j s_{i_j}$ where $b_j = \prod_{1 \le l \le t, l \ne j} \frac{x_{i_l}}{x_{i_l} - x_{i_j}}$.

Joint Random Secret Sharing (JRSS) [22]: In this protocol, each player can collectively generate a random secret and each of them can receive a (t,n)-secret sharing of this random value. Basically, this can be achieved by asking each participant to share his/her own random secret with the remaining participants by a (t,n)-secret sharing, and the final random secret shared by all these players is the sum of the random value selected by each participant.

Multiplication of Two Shared Secrets [13]: Two values shared by the (t,n)-secret sharing can be multiplied without revealing any information about the shares (except the wanted result of their products). The principle behind is as follows. Suppose there are two polynomials of degree $t-1$ for the (t,n)-secret sharing of value r and s respectively, their multiplications gives another polynomial of degree $2t-2$, which can be used for a $(2t-1,n)$-secret sharing of the products of r and s. However, this "newly generated" polynomial is not randomly generated anymore. To avoid leaking any information about r and s, we need to "re-randomize" it by using joint random secret sharing of a zero-value (such that the polynomial is randomized but the value to be shared remains unchanged).

Now we describe the $(2t-1,n)$ threshold extension of our scheme. Firstly, the shares s_i of the secret key s is generated by a (t,n)-JRSS. For signing, any $2t-1$ of the n signers jointly execute a $(t, 2t-1)$-JRSS to generate the random value r, and compute the value of $Y = rZ$ where $Z = H(c)$. The shares r_i of r are distributed to the participating $2t-1$ signers. Each of them executes a $(2t-1, 2t-1)$-JRSS of a zero-value to get the shares c_i. After received the value of h from the requester, each signer increments his/her share r_i by $r_i' = r_i + h$, the value of $(r+h)s$ can be recovered by these $2t-1$ signers, by interpolating the value of $r_i' s_i + c_i$ from each of them. Hence these signers can compute the blinded signature $S = (r+h)sZ$ to be sent to the requester, by the point scalar multiplication of their shares with Z.

4.3 ID-based Partially Blind Signature

`Setup`: The PKG randomly chooses $s \in_R \mathbb{Z}_q^*$. The master secret key is s and the system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_0(\cdot)\}$.

`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 of identity ID on the negotiated 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 $Y' = \alpha Y + \alpha\beta Q_{ID} - \gamma H(c)$, $C' = \alpha C + \gamma P_{pub}$, $h = \alpha^{-1} H_0(m, Y') + \beta$ 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`: The requester unblinds the received S by $S' = \alpha S$.

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

`Verify`: Any verifier (including the signature requester) can verify the validity of the ID-based partially blind signature by verifying if $\hat{e}(S', P) = \hat{e}(Y' + H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$ holds. If so, the partially blind signature is accepted as valid.

5 Analysis of the Proposed Schemes

5.1 Correctness Analysis

For any valid signature produced by our PKI-based scheme:

$$\begin{aligned}
\hat{e}(S', P) &= \hat{e}(\alpha S, P) \\
&= \hat{e}((\alpha(r + h)sZ, P) \\
&= \hat{e}((\alpha r + \alpha h)Z, P_{pub}) \\
&= \hat{e}((\alpha r + H_0(m, Y') + \alpha\beta)Z, P_{pub}) \\
&= \hat{e}((\alpha r + \alpha\beta)Z + H_0(m, Y')Z, P_{pub}) \\
&= \hat{e}(\alpha Y + \alpha\beta H(c) + H_0(m, Y')H(c), P_{pub}) \\
&= \hat{e}(Y' + H_0(m, Y')H(c), P_{pub})
\end{aligned}$$

Similarly, for our PKI-based partially blind signature scheme:

$$\begin{aligned}
\hat{e}(S', P) &= \hat{e}(\alpha S, P) \\
&= \hat{e}((\alpha r + \alpha h)S_{ID} + \alpha r H(c), P) \\
&= \hat{e}((\alpha r + H_0(m, Y') + \alpha\beta)S_{ID}, P)\hat{e}(H(c), \alpha r P) \\
&= \hat{e}((\alpha r + H_0(m, Y') + \alpha\beta)Q_{ID}, P_{pub})\hat{e}(H(c), C' - \gamma P_{pub}) \\
&= \hat{e}((\alpha r + \alpha\beta)Q_{ID} + H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(-\gamma H(c), P_{pub})\hat{e}(H(c), C') \\
&= \hat{e}(\alpha Y + \alpha\beta Q_{ID} - \gamma H(c) + H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C') \\
&= \hat{e}(Y' + H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')
\end{aligned}$$

5.2 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 (MapToPoint, the hash operation in BLS short signature scheme [5]) and pairing operation (Pairing). Table 1 shows a summary of the efficiency of our proposed schemes and also the revised scheme in [41].

The signature requesters usually posses less computational power than the signature issuer. Comparing our proposed schemes with the scheme in [41] (PKI-based but not ID-based), our PKI-based scheme is more efficient on the requesters' side, while our ID-based scheme only requires three more point scalar multiplications and one more inversion in $\mathbb{Z}_q$.

5.3 Security Analysis

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 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_0 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 $\leq 120686 q_H q_I 2^k t/\epsilon(2^k - 1)$.*

Algorithms	Efficiency					
	G_1 Add	G_1 Mul	Z_q Mul	Z_q Div	MapToPoint	Pairing
Existing Partially Blind Signature [41]						
`Issue(Signer)`	0	1	0	1	0	0
`Issue(Requester)`	3	3	0	0	1	0
`Verify`	1	1	0	0	1	2
Proposed PKI-based Partially Blind Signature						
`Issue(Signer)`	0	2	1	0	1	0
`Issue(Requester)`	1	3	0	1	1	0
`Verify`	1	1	0	0	1	2
Proposed ID-based Partially Blind Signature						
`Issue(Signer)`	1	4	0	0	1	0
`Issue(Requester)`	3	6	0	1	1	0
`Verify`	1	1	0	0	1	3

Table 1. Efficiency of our Proposed Schemes

Proof. See Appendix A. □

Theorem 2 *Our partially PKI-based blind signature scheme satisfies the partial blindness property in information theoretic sense.*

Proof. See Appendix A. □

Theorem 3 *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 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_0 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 $\leq 120686 q_H q_I 2^k t/\epsilon(2^k - 1)$.*

Proof. The proof is similar to that of Theorem 1. See Appendix A. □

Theorem 4 *Our ID-based partially blind signature scheme satisfies the partial blindness property in information theoretic sense.*

Proof. The proof is similar to that of Theorem 2. See Appendix A. □

5.4 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 PKI-based scheme) are unknown to the requester, changing $H(c)$ to $H(c')$ involves solving the CDH problem, which is computationally infeasible.

6 Conclusion

In this paper, we propose two improved partially blind signature schemes. One is a PKI-based threshold partially blind signature scheme while another one is an ID-based partially blind signature scheme. To the best of authors' knowledge, our schemes are the first of their kind. The proposed schemes are provably secure in the random oracle model. Future research directions include finding a formal proof of security against the parallel one-more signature forgery attack.

Acknowledgement

The authors would like to thank Dr. Fangguo Zhang for pointing out the mistake of the preliminary version of this paper (by showing a changing agreed information attack on the scheme) and all the anonymous reviewers for their helpful comments.

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*, pages 244–251. 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*, pages 271–286. Springer, 2000.
3. 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*, pages 31–46. Springer, 2002.
4. 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*, pages 416–432. Springer, 2003.
5. 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*, pages 514–532. Springer, 2001.
6. Tony K. Chan, Karyin Fung, Joseph K. Liu, and Victor K. Wei. Blind Spontaneous Anonymous Group Signatures for Ad Hoc Groups. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *Security in Ad-hoc and Sensor Networks, First European Workshop, ESAS 2004, Heidelberg, Germany, August 6, 2004, Revised Selected Papers*, volume 3313 of *Lecture Notes in Computer Science*, pages 82–94. Springer, 2005.
7. 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*, pages 246–264. Springer, 1990.
8. 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*, pages 319–327. Springer, 1990.
9. 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*, pages 11–19, 2003.

10. Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, and K.P. Chow. Forward-Secure Multisignature and Blind Signature Schemes. *Applied Mathematics and Computation*, September 2004.
11. 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*, pages 11–21. Springer, 2003.
12. 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*, pages 286–300. Springer, 1996.
13. Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Robust Threshold DSS Signatures. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 354–371. Springer, 1996.
14. 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.
15. 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.
16. 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.
17. 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*, pages 318–327. Springer, 2002.
18. 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.
19. Lihua Liu and Zhengjun Cao. Universal Forgeability of a Forward-Secure Blind Signature Scheme Proposed by Duc et al. Cryptology ePrint Archive, Report 2004/262, 2004. Available at http://eprint.iacr.org.
20. 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.
21. Wakaha Ogata and Kaoru Kurosawa. Oblivious Keyword Search. Cryptology ePrint Archive, Report 2002/182, 2002. Available at http://eprint.iacr.org.
22. Torben P. Pedersen. Distributed Provers with Applications to Undeniable Signatures. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 221–242. Springer, 1991.
23. 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*, pages 252–265. Springer, 1996.
24. 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.
25. 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.

26. 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*, pages 1–12. Springer, 2001.
27. Claus Peter Schnorr. Enhancing the Security of Perfect Blind DL-Signatures. Manuscript, December 2003.
28. Adi Shamir. How to Share A Secret. *Communications of the ACM*, 22(11):612–613, 1979.
29. 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.
30. 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.
31. 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, pages 233–238, 2003.
32. Sebastiaan von Solms and David Naccache. On Blind Signatures and Perfect Crimes. *Journal of Computer and Security*, 11:581–583, 1992.
33. David Wagner. A Generalized Birthday Problem. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 288–303. Springer, 2002.
34. Yan Wang, Shuwang Lu, and Zhenhua Liu. A Simple Anonymous Fingerprinting Scheme Based on Blind Signature. In Sihan Qing, Dieter Gollmann, and Jianying Zhou, editors, *Information and Communications Security, 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, 2003, Proceedings*, volume 2836 of *Lecture Notes in Computer Science*, pages 260–268. Springer, 2003.
35. 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*, pages 249–259. Springer, 2003.
36. Tsz Hon Yuen and Victor K. Wei. Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. In A. J. Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, Febrary 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 305–322, San Francisco, CA, USA, February 2005. Springer. Also available at Cryptology ePrint Archive, Report 2004/121.
37. 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*, pages 312–323. Springer, 2003.
38. Fangguo Zhang, Rei Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.
39. 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.
40. Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. In Thomas Johansson and Subhamoy Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003, Fourth International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 191–204. Springer, 2003.
41. 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/∼wsusilo.
42. 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 A

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 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_0 requests: $\mathcal{C}$ will answer each H_0 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 $H_0(m, Y')$ and $H(c)$ in the way as mentioned above. (Y', S', m, c) will be used as the answer, where $Y' = y_j P - H_0(m, Y')H(c)$ 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 $\hat{e}(S', P) = \hat{e}(Y' + H_0(m, Y')H(c), aP)$ and returns $\top$ or $\bot$ accordingly.

It follows from the forking lemma [24] 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 (h, Y, S, m, c) and (h', Y', S', m, c) 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, suppose they are (h, Y, S, m, c) and (h', Y', S', m, c).
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 negotiated 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 [24] 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
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 2.

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

$$S' = \alpha S \tag{1}$$
$$h = (\alpha^{-1} H_0(m, Y') + \beta) \pmod q \tag{2}$$
$$Y' = \alpha Y + \alpha\beta H(c) \tag{3}$$

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 $\beta' \in \mathbb{Z}_q^*$ while the value is determined by the equation $\beta' = h - (\alpha')^{-1} H_0(m, Y')$.

Since (Y', S', m, c) is a valid signature, we have $\hat{e}(S', P) = \hat{e}(Y' + H_0(m, Y')H(c), P_{pub})$, i.e. $\hat{e}(S', P) = \hat{e}(Y', P_{pub})\hat{e}(H_0(m, Y')H(c), P_{pub})$, this result will be useful shortly afterward. Besides, notice that 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.

Now we consider whether Eq (3) holds for α' and β' we have found:

$$\begin{aligned}
&\hat{e}(\alpha' Y + \alpha'\beta' H(c), P_{pub}) \\
&= \hat{e}(\alpha' Y + \alpha'(h - (\alpha')^{-1} H_0(m, Y'))H(c), P_{pub}) \\
&= \hat{e}(\alpha' r H(c) + \alpha' h H(c), P_{pub})\hat{e}(H_0(m, Y')H(c), P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r + h)H(c), P_{pub})\hat{e}(H_0(m, Y')H(c), P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r + h)H(c), P_{pub})\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha'(r + h)sH(c), P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha' S, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(S', P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(Y', P_{pub})
\end{aligned}$$

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. □

Proof of Theorem 3

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

Public key and private key request: $\mathcal{C}$ 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_0 requests: $\mathcal{C}$ will answer H_0 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 $H_0(m, Y')$ and $H(c)$ in the way as mentioned above. (Y', C', S', m, c) will be used as the answer, where $Y' = y_jP - H_0(m, Y')H_0(c)H(ID_j)$, $C' = z_jP$ 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_0 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 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 $\mathcal{A}$ make a forged signature $((ID_i, m), c, h, Y, C, S)$, it follows from the forking lemma [24] 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 forgeries $((ID_i, m), c, h, Y, C, S)$ 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 and valid forgeries: $((ID_i, m), c, h, Y, C, S)$ and $((ID_i, m), c, h', Y', C', S')$.
2. $\mathcal{C}'$ derives the value of abP by $(h - h')^{-1}(S - S')$, as both of $(P, aP, Y + hbP, S - rH(c))$ 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 $(2^k - 1)/q_I2^k$.

Based on the bound from the forking lemma [24] 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 $\leq 120686q_Hq_I2^kt/\epsilon(2^k - 1)$. □

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 blindness property in [37].

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

$$S' = \alpha S \tag{4}$$

$$C' = \alpha C + \gamma P_{pub} \tag{5}$$

$$h = (\alpha^{-1} H_0(m, Y') + \beta) \pmod q \tag{6}$$

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

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 (4) 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 $\beta' = h - (\alpha')^{-1} H_0(m, Y')$ and $\gamma' P_{pub} = C' - \alpha C$.

Since (Y', C', S', m, c) is a valid signature, $\hat{e}(S', P) = \hat{e}(Y' + H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$ holds, which gives us an useful result $\hat{e}(S', P) = \hat{e}(Y', P_{pub})\hat{e}(H_0(m, Y')Q_{ID}, P_{pub})\hat{e}(H(c), C')$ that will be used below. Besides, notice that 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.

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

$$\begin{aligned}
&\hat{e}(\alpha' Y + \alpha'\beta' Q_{ID} - \gamma' H(c), P_{pub}) \\
&= \hat{e}(\alpha' Y + \alpha'(h - (\alpha')^{-1} H_0(m, Y'))Q_{ID} - \gamma' H(c), P_{pub}) \\
&= \hat{e}(\alpha' r Q_{ID} + \alpha' h Q_{ID} - \gamma' H(c), P_{pub})\hat{e}(H_0(m, Y')Q_{ID}, P_{pub})^{-1} \\
&= \hat{e}(\alpha'(r + h)Q_{ID}, P_{pub})\hat{e}(H_0(m, Y')Q_{ID}, P_{pub})^{-1}\hat{e}(-\gamma' H(c), P_{pub}) \\
&= \hat{e}(\alpha'(r + h)Q_{ID}, P_{pub})\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub})\hat{e}(H(c), C')\hat{e}(H(c), -\gamma' P_{pub}) \\
&= \hat{e}(\alpha'(r + h)S_{ID}, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub})\hat{e}(H(c), \alpha' C) \\
&= \hat{e}(\alpha'(r + h)S_{ID}, P)\hat{e}(\alpha' r H(c), P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(\alpha' S, P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(S', P)\hat{e}(S', P)^{-1}\hat{e}(Y', P_{pub}) \\
&= \hat{e}(Y', P_{pub})
\end{aligned}$$

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. □

Appendix B

We remark that the security of our schemes also depends on the intractability of the ROS (find an Overdetermined, Solvable system of linear equations modulo q with Random inhomogeneities) problem.

Definition 8. *Given an oracle random function $F : \mathbb{Z}_q{}^l \rightarrow \mathbb{Z}_q$, the ROS problem is to find coefficients $a_{k,i} \in \mathbb{Z}_q$ and a solvable system of $l+1$ distinct equations (1) in the unknown $c_1, c_2, \cdots, c_l$ over $\mathbb{Z}_q$:*

$$a_{k,1}c_1 + \cdots + a_{k,l}c_l = F(a_{k,1}, \cdots, a_{k,1}) \text{ for } k = 1, 2, \cdots, t. \tag{1}$$

Now we describe how an adversary $\mathcal{A}$ that is able to solve ROS problem efficiently can get $l+1$ valid ID-based partially blind signature associated with the *same* agreed information c by requesting only l signatures from the *same* signature issuer $\mathcal{S}$ of identity ID.

1. $\mathcal{S}$ sends commitments $C_1 = r_1P$, $C_2 = r_2P$, $\cdots$, $C_l = r_lP$ and $Y_1 = r_1Q_{ID}$, $Y_2 = r_2Q_{ID}$, $\cdots$, $Y_l = r_lQ_{ID}$ to $\mathcal{A}$.
2. $\mathcal{A}$ chooses randomly $a_{k,1}, a_{k,2}, \cdots a_{k,l}$ from $\mathbb{Z}_q$ and messages $m_1, m_2, \cdots, m_t$ and computes $f_k = \sum_{i=1}^{l} (a_{k,i}Y_i)$ and $H_0(m_k, f_k)$ for $k = 1, 2, \cdots, t$ where $l+1 \leq t < q_{H_0}$, the maximum number of queries of H_0 issued by $\mathcal{A}$.
3. $\mathcal{A}$ solves the ROS-problem: $l+1$ of equations (2) in the unknowns $c_1, c_2, \cdots, c_l$ over $\mathbb{Z}_q$:

$$\sum_{j=1}^{l} (a_{k,j}c_j) = H_0(m_k, f_k) \text{ for } k = 1, 2, \cdots, t. \tag{2}$$

4. $\mathcal{A}$ sends the solutions $c_1, c_2, \cdots, c_l$ as the challenge (value to be signed) to $\mathcal{S}$.
5. $\mathcal{S}$ sends back $S_i = (r_i + c_i)S_{ID} + r_iH(c)$ for $i = 1, 2, \cdots, l$.
6. For each solved equation (2), $\mathcal{A}$ gets a valid signature $(Y_k{}', C_k{}', S_k{}')$ on message m_k by setting $Y_k{}' = f_k$, $C_k{}' = \sum_{j=1}^{l} a_{k,j}C_j$ and $S_k{}' = \sum_{j=1}^{l} a_{k,j}S_j$.

Now we show these $l+1$ signatures are valid.

$$\begin{aligned}
\hat{e}(S_k{}', P) &= \hat{e}(\sum_{j=1}^{l} a_{k,j}S_j, P) \\
&= \hat{e}(\sum_{j=1}^{l} a_{k,j}[(r_j + c_j)S_{ID} + r_jH(c)], P) \\
&= \hat{e}(S_{ID}, P)^{\sum_{j=1}^{l} a_{k,j}r_j} \hat{e}(S_{ID}, P)^{\sum_{j=1}^{l} a_{k,j}c_j} \hat{e}(H(c), \sum_{j=1}^{l} a_{k,j}r_jP) \\
&= \hat{e}(\sum_{j=1}^{l} a_{k,j}r_jQ_{ID}, P_{pub})\hat{e}(Q_{ID}, P_{pub})^{H_0(m_k, f_k)}\hat{e}(H(c), \sum_{j=1}^{l} a_{k,j}r_jP) \\
&= \hat{e}(\sum_{j=1}^{l} a_{k,j}Y_j, P_{pub})\hat{e}(H_0(m_k, f_k)Q_{ID}, P_{pub})\hat{e}(H(c), \sum_{j=1}^{l} a_{k,j}C_j) \\
&= \hat{e}(Y_k{}' + H_0(m_k, Y_k{}'), P_{pub})\hat{e}(H(c), C_k{}')
\end{aligned}$$

A similar attack can be applied on our PKI-based partially blind signature if an adversary can solve ROS problem efficiently. However, ROS problem is "a plausible but novel complexity assumption" [26]. We refer interested reader to [27] and [33] for more discussions on the relationship between ROS problem and blind signature schemes.