One-Round ID-Based Blind Signature Scheme without ROS Assumption

Wei Gao[1], Xueli Wang[2], Guilin Wang[3], and Fei Li[4]

[1] College of Mathematics and Econometrics, Hunan University, Changsha 410082, China
sdgaowei@yahoo.com.cn
[2] School of Mathematics Science, South China Normal University, Guangzhou 510631, China
wangxuyuyan@yahoo.com.cn
[3] Institute for Infocomm Research,21 Heng Mui Keng Terrace, Singapore 119613
glwang@i2r.a-star.edu.sg
[4] School of Mathematics and Information Sciences, Guangzhou University, Guangzhou 510006, China
miss_lifei@yahoo.com.cn

Abstract. In this paper, we propose a new ID-based blind signature scheme based on bilinear pairings from scratch (i.e. without using existing ID-based signature schemes, and without using existing computational assumptions). First, the round complexity of our ID-based blind signature scheme is optimal. Namely, each interactive signature generation requires the requesting user and the signer to transmit only one message each. Second, the proposed scheme is provably secure against generic parallel attack without using the ROS assumption. Indeed, the security of the proposed scheme is based on a new formalized assumption called one-more bilinear Diffie-Hellman Inversion (1m-BDHI) assumption.

1 Introduction

In 1984, Shamir [26] introduced the concept of identity-based (simply ID-based) public key cryptosystems to simplify key management procedures in certificate-based public key setting. ID-based cryptosystems have a property that a user's public key can be easily derived from his identity by a publicly available function, while his private key can be calculated for him by a trusted authority, called Private Key Generator (PKG). They enable any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as the trusted PKG issues a private key to each user when he first joins the network. So they can be a good alternative for certificate-based public key infrastructure, especially when efficient key management and moderate security are required.

Bilinear pairings are the main tools to construct new ID-based cryptographic primitives. In 2000, Joux [20] used the Weil pairing to construct a one-round tripartite Diffie-Hellman key agreement protocol. After Joux's breakthrough, many

ID-based cryptographic schemes have been proposed using bilinear pairings [14]. In Crypto 2001, Boneh and Franklin [8] presented an ID-based encryption scheme based on bilinear pairings which is the first fully functioning, efficient and provably secure ID-based encryption scheme. In Asiacrypt 2001, Boneh, Lynn and Shacham [9] proposed a basic signature scheme using pairings which has the shortest length among signature schemes in classical cryptography.

Blind signature, first introduced by Chaum [12] in Crypto'82, is a variant of digital signature, which allows the user to get a signature without giving the signer any information about the actual message or the resulting signature. Formally, blindness means that the signer's view and the resulting signature are statistically independent, where the signer's view is the set of all values that can be gotten by the signer during the execution of the signature issuing protocol. This blindness property plays a central role in applications such as electronic voting and electronic cash systems.

Before the very recent generic results of Galindo et al. [18], three ID-based blind signature (IDBS) schemes [28,29,16] based on bilinear pairings have been proposed. However, for all these schemes, the security against one more signature forgery under the generic parallel attack [22] requires that the following ROS-problem is intractable[25,28,29,16]: find an overdetermined, solvable system of linear equations modulo q with random inhomogenities (right sides). Unfortunately, in Crypto 2002, Wagner [27] claimed that there is a subexponential time algorithm to break the ROS-problem. To be resistant against this attack, the size of q (security parameter) may need to be at least 1,600 bits long. In contrast, for common cryptographic primitives based on bilinear parings such as [9,8], the size of q is only about 160 bits. Since even the slightly larger security parameter will result in the dramatically larger amount of computation, all these existing schemes can not be efficiently implemented, and hence be of little interest in practice. In fact, until the very recent generic results of Galindo et al. [18], it remains *an open problem* to construct an ID-based blind signature scheme whose security does not depend on the ROS assumption.

On the other hand, all of the aforementioned ID-based blind signature schemes require three moves (essentially 2 rounds since these protocols have the signer go first which typically is a server). Of course, round complexity is the most important efficiency factor for an ID-based blind signature scheme, especially when it is applied in the applications such as E-voting, E-cash. And one-round is the optimal bound of round complexity. In fact, there are only four PKI-based blind signature schemes [12,7,21,15] with an optimal two-move signature generation protocol. However, there exists no ID-based signature scheme with two-move signature generation protocol. On one hand, since almost all ID-based signature schemes are constructed by using the proof of knowledge paradigm [5], it seems difficult to extend them into ID-based blind signature schemes with optimal round complexity [28,29,16,24]. On the other hand, the ID-based blind signature schemes constructed by Galindo et al.[18] need at least 4 moves (See Section 6 of our paper).

Our contribution. In this paper, we propose a new ID-based blind signature scheme based on bilinear pairings from scrach (new computational assumptions, new basic ID-based signature scheme, in addition to the new blind signature scheme). In more details, our contribution is as follows. (1) The round complexity is optimal. Namely, each interactive signature generation requires the requesting user and the signer to transmit only one message each. (2) The provable security against generic parallel attack doesn't depend on the difficulty of ROS-problem (See the following Definition 4). (3) To prove its security, we propose a new plausible computational assumption, namely, *one-more bilinear Diffie-Hellman Inversion assumption* (**1m-BDHI**, for short). This new assumption may be of independent interest, since other recently proposed computation assumptions in one-more flavor, such as one-more-RSA-inversion [3], one-more CDH [7], one-more discrete logarithm [4], have found many applications in provable security for blind signatures [3,7], transitive signatures [4], identification protocols [2] and so on. (4) The underlying ID-based signature scheme may be of independent interest, since it avoids using the proof of knowledge paradigm and has a loose algebraic structure which already allows the efficient extension to blind signatures. Additionally, we will show some advantages of our ID-based blind signature scheme over the generic construction due to Galindo et al. [18]. For example, we will show that the generic ID-based blind signature scheme of Galindo et al. does not completely solve the key management problem.

2 Preliminaries

In this section, we present the definitions of bilinear pairings and some relative assumptions.

Definition 1. *Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and let P be a generator of $\mathbb{G}_1$. The map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is said to be an bilinear paring if the following three conditions hold: (i) e is bilinear, i.e. $e(aP, bP) = e(P, P)^{ab}$ for all $a, b \in \mathbb{Z}_q$; (ii) e is non-degenerate, i.e. $e(P, P) \neq 1$; (iii) e is efficiently computable. Such a group $\mathbb{G}_1$ is called a bilinear group.*

Note that throughout this paper, without special descriptions, the groups $\mathbb{G}_1, \mathbb{G}_2$, the prime order q, the generator P of $\mathbb{G}_1$ and the bilinear pairing e are as defined in the above definition. Next, we review the following problems with respect to $(\mathbb{G}_1, \mathbb{G}_2, e, P, q)$:

- **Computational Diffie-Hellman (CDH) Problem**: Given random $P, aP, bP \in \mathbb{G}_1$, output $abP \in \mathbb{G}_1$, where $a, b \in_R \mathbb{Z}_q$.
- **Bilinear Diffie-Hellman (BDH) Problem** [8]: Given random $P, aP, bP, cP \in \mathbb{G}_1$, output $e(P, P)^{abc}$, where $a, b, c \in_R \mathbb{Z}_q$.
- **Generalized Tate Inversion (GTI) Problem** [20]: Given $h \in \mathbb{G}_2$, find a pair $(S, T) \in \mathbb{G}_1$ such that $e(S, T) = h$, where $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ denotes the Tate pairing.

– **Modified Generalized Bilinear Inversion (MGBI)**[1]: Given $h \in \mathbb{G}_2$ and the generator $P \in \mathbb{G}_1$, find a point $S \in \mathbb{G}_1$ such that $e(P, S) = h$, where e denotes the bilinear pairing.

Based on the above problems, we propose a new computational problem:

Definition 2 (Bilinear Diffie-Hellman Inversion (BDHI) Problem). *Given three random elements $aP, bP, cP \in \mathbb{G}_1$, compute two elements $S, T \in \mathbb{G}_1$ such that $e(S, T) = e(P, P)^{abc}$. Accordingly, the Bilinear Diffie-Hellman Inversion (BDHI) assumption states that: there is no PPT algorithm that can solve the BDHI problem with non-negligible probability.*

It is obvious that the BDH problem can be solved if the BDHI problem can be solved. And it is also obvious that the BDHI problem can solved if the CDH problem can be solved. So BDHI assumption is somewhere between CDH assumption and BDH assumption. That is, BDHI assumption is weaker than BDH assumption, but stronger than CDH assumption.

Furthermore, we propose another new computational assumption called one-more bilinear Diffie-Hellman Inversion (1m-BDHI) assumption. In fact, there exist many computational assumptions in the one-more flavor, such as One-more-RSA-inversion [3], one-more CDH [7], one more discrete logarithm [4]. These one-more assumptions can be used to prove security of many cryptographic schemes, such as the GQ identification scheme [2], blind signature schemes [4,7], transitive signatures [3].

Definition 3 (1m-BDHI Assumption). *Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear pairing, where $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and P be a generator of $\mathbb{G}_1$. Let x, y be random elements in $\mathbb{Z}_q$ and let $X = xP, Y = yP$. The adversary $\mathcal{A}$ is given $(e, \mathbb{G}_1, \mathbb{G}_2, q, P, X, Y)$ and has access to two oracles.*

– *The first one is a target oracle $\mathcal{TO}$ that, each time it is invoked (it takes no inputs), returns a random point from $\mathbb{G}_1$.*
– *The second one is the helper oracle $\mathcal{HO}$ which given $Z \in \mathbb{G}_1$, returns $S, T \in \mathbb{G}_1$ such that $e(S, T) = e(Y, Z)^x$. Additionally, this help oracle $\mathcal{HO}$ returns an auxiliary information piece R which can be used to check whether the equation $e(S, T) = e(Y, Z)^x$ holds. An example of the form of (R, S, T) used in this paper is given in the following remark.*

We say that $\mathcal{A}$ wins if its output is a sequence of points $S_1, T_1, \ldots, S_n, T_n \in \mathbb{G}_1$ satisfying $e(S_1, T_1) = e(Y, Z_1)^x, \ldots, e(S_n, T_n) = e(Y, Z_n)^x$, where all different $Z_1, \ldots, Z_n$ are obtained from $\mathcal{A}$'s target oracle and the number of queries made by $\mathcal{A}$ to its helper oracle $\mathcal{HO}$, is strictly less than n. The 1m-BDHI advantage of $\mathcal{A}$, denoted $Adv_{\mathcal{A}}^{1m-BDHI}(k)$, is the probability that $\mathcal{A}$ wins, taken over the coins used in the generation of $(e, \mathbb{G}_1, \mathbb{G}_T, q, P, X, Y)$, the coins of $\mathcal{A}$, and the coins used by the target oracle across its invocations. We say that the one-more BDHI problem is hard if the function $Adv_{\mathcal{A}}^{1m-BDHI}(k)$ is negligible for all polynomial-time adversaries $\mathcal{A}$.

Remark 1. In this paper, a valid answer (R, S, T) of the helper oracle $\mathcal{HO}$ should satisfy:

$$e(R,S) = e(xP, yP), e(R,Z) = e(P,T).$$

Indeed, suppose that $R = rP$. Then the above two equations imply the following equations respectively:

$$S = r^{-1}xyP, T = rZ.$$

So we have $e(S,T) = e(yP,Z)^x$.

Finally, we describe the ROS-problem.

Definition 4 (ROS-Problem [25]). *Given an oracle random function $F : \mathbb{Z}_q^l \to \mathbb{Z}_q$, find coefficients $a_{k,i} \in \mathbb{Z}_q$ and a solvable system of $l+1$ distinct equations (1) in the unknowns $c_1, c_2, \ldots, c_l$ over $\mathbb{Z}_q$:*

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

Accordingly, the ROS assumption states that: there is no PPT algorithm that can solve the ROS problem with non-negligible probability.

As Schnorr states, the intractability of the ROS-problem is "a palausible but novel complexity assumption". At Crypto 2002, D. Wagner [27] claimed that he can break ROS-problem with subexponential time. As argued in [28], to be resistant against this new attack, q may need to be at least 1600 bits long.

3 Frameworks of ID-based Blind Signatures

Definition 5. *An identity-based blind signature scheme $\mathcal{IDBS}$ can be described as a collection of the following four algorithms (or protocols):*

- Setup. *This algorithm is run by the trusted party called PKG on input a security parameter, and generates the public parameters params of the scheme and a master secret. PKG publishes params and keeps the master secret to itself.*
- Extract. *Given an identity ID, the master secret and params, this algorithm generates the private key D_{ID} of ID.*
- Issue. *The signer blindly issues a signature for the user by this protocol, which is often divided into three sub-protocols or algorithms* (Blind, BSign, Unblind)*:*
  - Blind. *Given the message m and a random string r, it outputs the blinded message m' and sends it the signer. In this process, the user sometimes needs the interactive help from the signer.*
  - BSign. *Given the blinded message m' and the signer's private signing key D_{ID} as the input, it outputs a blind signature σ' and sends it to the user. This procedure may be an interactive sub-protocol between the user and the signer.*
  - Unblind. *Given a signature σ' and the previous used random string r, it outputs the unblinded signature σ.*

– Verify. *Given a signature σ, a message m, an identity ID and params, this algorithm outputs 1 if σ is a valid signature on m for identity ID, or 0 otherwise.*

The security of an ID-based blind signature scheme consists of two requirements: the blindness property and the unforgeability of additional signatures. We say a blind signature scheme is secure if it satisfies these two requirements.

Definition 6 (Blindness). *Let $\mathcal{A}$ be a probabilistic polynomial-time adversary which plays the role of the signer, $\mathcal{U}_0$ and $\mathcal{U}_1$ be two honest users. $\mathcal{U}_0$ and $\mathcal{U}_1$ engage in the blind signature issuing protocol with $\mathcal{A}$ on messages m_b and m_{1-b}, and output signatures σ_b and σ_{1-b}, respectively, where $b \in \{0,1\}$ is a random bit chosen uniformly. $(m_0, m_1, \sigma_b, \sigma_{1-b})$ are sent to $\mathcal{A}$ and then $\mathcal{A}$ outputs $b' \in \{0,1\}$. For all such $\mathcal{A}$, $\mathcal{U}_0$ and $\mathcal{U}_1$, for any constant c, and for sufficiently large n,*

$$|Pr[b = b'] - 1/2| < n^{-c}.$$

To define unforgeability, let us introduce the following game among the adversary $\mathcal{A}$ which plays the role of the user, and the challenger $\mathcal{C}$ which plays the role of the honest signer.

– Setup. The challenger $\mathcal{C}$ takes a security parameter 1^k and runs the algorithm Setup to generate common public parameters *params* and also the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.
– Queries. The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in a concurrent and interleaving way as follows.
  • Hash function query. If the security is analyzed in the random oracle model [6], $\mathcal{C}$ computes the values of the hash functions for the requested input and sends the values to $\mathcal{A}$.
  • Extract query. $\mathcal{A}$ chooses an identity ID and sends it to $\mathcal{C}$. $\mathcal{C}$ computes $\mathsf{Extract}(ID) = D_{ID}$ and sends the result to $\mathcal{A}$.
  • Issue query. $\mathcal{A}$ chooses an identity ID, a plaintext m. To blindly obtain a signature on m with respect to ID, $\mathcal{A}$ engages in the blind signature issuing protocol with $\mathcal{C}$ in a concurrent and interleaving way.
– Forgery. $\mathcal{A}$ wins the game if $\mathcal{A}$ outputs n valid signatures $(m_1, \sigma_1), \ldots, (m_n, \sigma_n)$ with respect to the identity ID^* such that
  • $m_i \neq m_j$ for any pair (i, j), where $i \neq j$ $i, j \in \{1, \ldots, n\}$.
  • n is strictly larger than the number of the executions (with respect to the identity ID^*) of the protocol Issue between $\mathcal{C}$ and $\mathcal{A}$.
  • $\mathcal{A}$ has not made an extract query on the identity ID^*.

The advantage $Adv_{IDBS}^{unforge}$ of $\mathcal{A}$ is defined as the probability that it wins the above game, taken over the coin tosses made by $\mathcal{C}, \mathcal{A}$, Setup. In the above attack model, $\mathcal{A}$ is called *one-more forger under parallel chosen message and ID attacks.*

Definition 7 (Unforgeability). *An adversary $\mathcal{A}$ (t, q_E, q_S, ϵ)-breaks an ID-based blind signature scheme, if (1) $\mathcal{A}$ runs in time at most t, (2) $\mathcal{A}$ queries private keys for at most q_E identities and execute at most q_S times the blind signature issuing protocol, (3) $Adv_{IDBS}^{unforge}$ is at least ϵ. We say an ID-based blind signature scheme is (t, q_E, q_S, ϵ)-secure against one-more forgery under parallel chosen message and ID attacks if no adversary $\mathcal{A}$ (t, q_E, q_S, ϵ)-breaks the scheme.*

Remark 2. In the forgery step of the above attack game, if $(m_i, \sigma_i) \neq (m_j, \sigma_j)$ instead of $m_i \neq m_j$ holds for message-signature pairs output by the adversary, then we get the definition of the strong unforgeability of blind signature schemes. As mentioned in [10], for the main application of blind signatures, i.e., electronic cash, unforgeability (rather than strong unforgeability) suffices.

In fact, the above forger $\mathcal{A}$ against ID-based blind signatures is the natural analogy of the one-more forger under parallel attack [13] which is the most powerful attack for blind signatures. Unfortunately, before our schemes, there is no ID-based blind signature scheme based on bilinear pairings which can be proved secure in this model.

4 Construction

Our proposed scheme is described as follows:

- Setup. The Private Key Generator (PKG) generates parameters and master keys as follows:
  - generates groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q with bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$;
  - chooses an arbitrary generator $P \in \mathbb{G}_1$;
  - picks a random $s \in \mathbb{Z}_q$ and sets $P_{pub} = sP$;
  - chooses cryptographic hash functions $H_1, H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$. The PKG's public parameter is $params = (\mathbb{G}_1, \mathbb{G}_2, e, q, P, P_{pub}, H_1, H_2)$; its master secret is $s \in \mathbb{Z}_q$.
- Extract. The signer with identity ID receives the value $D_{ID} = sQ_{ID}$ from the PKG as its private key, where $Q_{ID} = H_1(ID) \in \mathbb{G}_1$.
- Issue.
  - Blind. The user randomly chooses a number $r_1 \in \mathbb{Z}_q$ as the blinding factor, computes $P'_m = r_1 H_2(m)$ and sends it to the signer.
  - BSign. The signer sends back (A', B', C'), where $A' = x_{ID} P'_m, B' = x_{ID}^{-1} D_{ID}, C' = x_{ID} P, x_{ID} \stackrel{R}{\leftarrow} \mathbb{Z}_q$.
  - Unblind. First, the user verifies the blind signature (A', B', C') by checking whehter
    $$e(A', P) = e(P'_m, C'), e(Q_{ID}, P_{pub}) = e(B', C').$$
    Next, the user selects a random number $r_2 \in \mathbb{Z}_q$ and computes the signature as (A, B, C), where $A = r_2 r_1^{-1} A', B = r_2^{-1} B', C = r_2 C'$.
- Verify. Let (A, B, C) be the signature on the message m and $P_m = H_2(m)$. The verifier checks that:

$$e(A,P) = e(P_m, C), e(Q_{ID}, P_{pub}) = e(B,C).$$

Correctness. If an entity with identity ID blindly issues a signature $\sigma = (A,B,C)$ on a message m to a user as described in the Issue protocol above, it is easy to see that σ will be accepted by a verifier:

$$\begin{aligned}
e(A,P) &= e(r_2 r_1^{-1} A', P) = (r_2 r_1^{-1} x_{ID} P'_m, P) \\
&= e(r_2 r_1^{-1} x_{ID} r_1 P_m, P) \\
&= e(r_2 x_{ID} P_m, P) = e(P_m, r_2 x_{ID} P) \\
&= e(P_m, r_2 C') \\
&= e(P_m, C), \\
e(B,C) &= e(r_2^{-1} B', r_2 C') \\
&= e(B', C') \\
&= e(x_{ID}^{-1} D_{ID}, x_{ID} P) \\
&= e(D_{ID}, P) = e(Q_{ID}, sP) \\
&= e(Q_{ID}, P_{pub}).
\end{aligned}$$

Similarly, we can see that the blind signature generated by the honest signer in Bsign must be accepted by the user in the step Unblind.

5 Security

First, we claim that our scheme has the *blindness property.* This is obvious since the signer receives only random elements in $\mathbb{G}_1$ which are independent of the outputs of the user.

Theorem 1 *The proposed ID-based blind signature scheme is blind.*

Proof. The blindness property will be proved according to Definition 6. We assume that when the signature $\sigma_b = (A_b, B_b, C_b)$ on the message m_b (resp. $\sigma_{1-b} = (A_{1-b}, B_{1-b}, C_{1-b})$ on m_{1-b}) is generated, the user $\mathcal{U}_0$ (resp. $\mathcal{U}_1$) sends P'_{m_b} (resp. $P'_{m_{1-b}}$) to the adversary $\mathcal{A}$ which then returns the blinded signature $\sigma'_b = (A'_b, B'_b, C'_b)$ (resp. $\sigma'_{1-b} = (A'_{1-b}, B'_{1-b}, C'_{1-b})$).

For σ_b, if we can prove that there exist two integers $r'_1, r'_2 \in \mathbb{Z}_q$ such that

$$P'_{m_{1-b}} = r'_1 H_2(m_b), A_b = r'_2 {r'}_1^{-1} A'_{1-b}, B_b = {r'}_2^{-1} B'_{1-b}, C_b = r'_2 C'_{1-b},$$

then it is obtained that for the adversary, σ_b may be linked to the process relative to the messages $(P'_{m_{1-b}}, A'_{1-b}, B'_{1-b}, C'_{1-b})$ and the user $\mathcal{U}_1$. In other words, the adversary $\mathcal{A}$ can not determine which of the two user generated the signature σ_b.

In fact, since (A_b, B_b, C_b) and $(A'_{1-b}, B'_{1-b}, C'_{1-b})$ are valid, we have

$$e(A_b, P) = e(P_{m_b}, C_b), e(Q_{ID}, P_{pub}) = e(B_b, C_b);$$

$$e(A'_{1-b}, P) = e(P'_{m_{1-b}}, C'_{1-b}), e(Q_{ID}, P_{pub}) = e(B'_{1-b}, C'_{1-b}).$$

Let $c_b, c'_{1-b} \in \mathbb{Z}_q$ be integers satisfying $C_b = c_b P$, $C'_{1-b} = c'_{1-b} P$ respectively. By the bilinear property of the pairing, then we have

$$A_b = c_b P_{m_b}, B_b = c_b^{-1} s Q_{ID};$$

$$A'_{1-b} = c'_{1-b} P'_{m_{1-b}}, B'_{1-b} = c'^{-1}_{1-b} s Q_{ID}.$$

Let r'_1, r'_2 be integers satisfying $C_b = r'_2 C'_{1-b}$ (i.e. $r'_2 = c_b c'^{-1}_{1-b} \mod q$) and $P'_{m_{1-b}} = r'_1 P_{m_b} (= r'_1 H_2(m_b))$ respectively , then they also satisfy

$$A_b = r'_2 r'^{-1}_1 A'_{1-b}, B_b = r'^{-1}_2 B'_{1-b}.$$

□

Next, we analyze the unforgeability of our scheme as follows. Here note that it is obvious that our blind signature scheme is not strongly unforgeable (see Remark 2 in Section 3). Instead, we will prove that its security satisfies the standard definition given in Section 3. As in [11], the proof is divided into two steps.

Consider the following variant of the attacking game for unforgeability in Section 3. First we fix an identity ID^*. In Setup Step, $\mathcal{C}$ gives to $\mathcal{A}$ system parameters together with ID^*, and in Step Forgery, $\mathcal{A}$ must output the given ID^* (together with n pairs (m_i, σ_i)) as its final result. If no polynomial time algorithm $\mathcal{A}$ has non-negligible advantage in this game, we say that the blind signature scheme is secure against *one-more forgery under parallel chosen message and given ID attacks*. The first step of our proof is to reduce the problem to this case.

Lemma 1 *For our scheme, if there is a one-more forger $\mathcal{A}_0$ under a parallel chosen message and ID attack with running time t_0 and advantage ϵ_0, then there is a one-more forger $\mathcal{A}_1$ under a parallel chosen message and given ID attack, which has running time $t_1 \leq t_0$ and advantage $\epsilon_1 \geq \epsilon_0(1 - \frac{1}{q})/q_{H_1}$, where q_{H_1} is the maximum number of queries to H_1 asked by $\mathcal{A}_0$. In addition, the numbers of queries to hash functions,* Extract*, and* Issue *asked by $\mathcal{A}_1$ are the same as those of $\mathcal{A}_0$.*

Proof. Without any loss of generality, we can assume that for any ID, $\mathcal{A}_0$ queries $H_1(ID)$ and Extract(ID) at most once. Let the fixed identity for $\mathcal{A}_1$ be ID^*. Our algorithm $\mathcal{A}_1$ is as follows:

- Choose $r \in \{1, \ldots, q_{H_1}\}$ randomly. Denote by ID_i the input of the i-th query to H_1 asked by $\mathcal{A}_0$. Let ID'_i be ID^* if $i = r$, and ID_i otherwise. Define $H'_1(ID_i)$, Extract$'(ID_i)$, Issue$'(ID_i, m)$ to be $H_1(ID'_i)$, Extract(ID'_i), Issue(ID'_i, m), respectively.
- Run $\mathcal{A}_0$ with the given system parameters. $\mathcal{A}_1$ responds to $\mathcal{A}_0$'s queries to H_1, H_2, Extract, and Issue by evaluating H'_1, H_2, Extract$'$, and Issue$'$, respectively. Let the output of $\mathcal{A}_0$ be n valid signatures $(m_1, \sigma_1), \ldots, (m_n, \sigma_n)$ with respect to ID_{out}, where n is strictly larger than the number of executions of the Issue' protocol.

– If $ID_{out} = ID^*$, then output n valid signatures $(m_1, \sigma_1), \ldots, (m_n, \sigma_n)$ together with the corresponding identity ID^*. Otherwise output *fail*.

Since the distributions produced by $H_1', \mathsf{Extract}'$, and Issue' are indistinguishable from those produced by $H_1, \mathsf{Extract}$, and Issue of our scheme, $\mathcal{A}_0$ learns nothing from query results, and hence

$$Pr[\mathcal{A}_0 \ succeeds] \geq \epsilon_0.$$

Since H_1 is a random oracle, if $\mathcal{A}_0$ has not made the the query $H_1'(ID_{out})$, the probability that the $\mathcal{A}_0$'s output is valid is negligible. Explicitly,

$$Pr[ID_{out} = ID_i \ for \ some \ i | \mathcal{A}_0 \ succeeds] \geq 1 - \tfrac{1}{q}.$$

Since r is independently and randomly chosen, we have

$$Pr[ID_{out} = ID_r = ID^* | ID_{out} = ID_i \ for \ some \ i] \geq \tfrac{1}{q_{H_1}}$$

Combining these,

$$Pr[\mathcal{A}_1 \ succeeds] \geq \epsilon_0 (1 - \tfrac{1}{q}) \tfrac{1}{q_{H_1}}$$

as desired. □

Lemma 2 *For our scheme, if there is a one-more forger $\mathcal{A}$ under a parallel chosen message and given ID attack with running time t_1 and advantage ϵ_1, then there is an adversary $\mathcal{B}$ attacking the one-more BDHI problem, which has running time $t_2 \leq t_1 + 4c_{\mathbb{G}_1}(q_{H_1} + q_{H_2} + q_S + q_E)$ and advantage $\epsilon_2 \geq \epsilon_1$, where $c_{\mathbb{G}_1}$ is a constant that depends on $\mathbb{G}_1$, and $q_{H_1}, q_{H_2}, q_E, q_S$ are the numbers of queries to the hash functions H_1, H_2, $\mathsf{Extract}$, and Issue asked by $\mathcal{A}_1$ respectively.*

Proof. Suppose that $\mathcal{A}$ is a one-more forger against our scheme under a parallel chosen message and given ID attack. We describe the algorithm $\mathcal{B}$ which will simulate the challenger for $\mathcal{A}$ in order to solve the one-more BDHI problem. The adversary $\mathcal{B}$ is given $(e, \mathbb{G}_1, \mathbb{G}_2, q, P, X, Y)$, the target oracle and the helper oracle. $\mathcal{B}$ simulates the challenger and interacts with forger $\mathcal{A}$ as follows.

– Setup. $\mathcal{B}$ first provides $\mathcal{A}$ with the public parameter $(e, \mathbb{G}_1, \mathbb{G}_2, q, P, P_{pub})$ and the fixed identity ID^*, where $P_{pub} = X$.
– H_1-$\mathsf{queries}$. To respond to these queries, $\mathcal{B}$ maintains a list of tuples $(ID_i, H_1(ID_i), r_i)$ as explained below. We refer to this list as H_1-list. The list is initially empty. When $\mathcal{A}$ queries the oracle H_1 at an identity ID_i, $\mathcal{B}$ responds as follows.
  - If the query ID_i appears on the H_1-list in a tuple $(ID_i, H_1(ID_i), r_i)$ (or $(ID_i, H_1(ID_i), *)$), then $\mathcal{B}$ responds with $H_1(ID_i)$.
  - If $ID_i = ID^*$, $\mathcal{B}$ sets $H_1(ID_i) = Y$ and sends it to $\mathcal{A}$. Additionally, $\mathcal{B}$ appends the tuple $(ID_i, H_1(ID_i), *)$ to the H_1-list.
  - If $ID_i \neq ID^*$, $\mathcal{B}$ randomly selects $r_i \in \mathbb{Z}_q$ and sends $H_1(ID_i) = r_i P$ to $\mathcal{A}$. Additionally, $\mathcal{B}$ appends the tuple $(ID_i, H_1(ID_i), r_i)$ to the H_1-list.

Since H_1 is a random oracle, $\mathcal{A}$ obtains no information on $H_1(ID)$ before he queries the H_1-oracle on ID. So, without loss of generality, we assume that $\mathcal{A}$ has already queried the H_1 oracle on an identity ID before he makes the issue query or extract query with respect to the ID.

- H_2-queries. When given the new query m_j, that is distinct from the previous hash queries, $\mathcal{B}$ obtains a point $Z_j \in \mathbb{G}$ as the hash value $H_2(m_j)$ from its target oracle $\mathcal{TO}$ and sends it to $\mathcal{A}$.
- Extract queries. Suppose that $\mathcal{A}$ makes an extract query on the identity $ID_i \neq ID^*$. Let $(ID_i, H_1(ID_i), r_i)$ be the tuple on the H_1-list containing ID_i. $\mathcal{B}$ answers this query by sends to $\mathcal{A}$ $D_{ID_i} = r_i X$. By assuming $X = xP$ for some unknown x, it is obvious that $D_{ID_i} = xH_1(ID_i) = r_i X$, since $H_1(ID_i) = r_i P$.
- Issue queries. Assume that $\mathcal{A}$ chooses the identity ID_i and the plaintext m_i and wants to blindly obtain the signature on m_i with respect to the identity ID_i. Note that the signer has only one move in the Issue protocol. Let P'_{m_i} be the blinded message that $\mathcal{A}$ sends to $\mathcal{B}$. $\mathcal{B}$ answer this query as follows.
  - If $ID_i \neq ID^*$, $\mathcal{B}$ computes the private key $D_{ID_i} = r_i X$, where (ID_i, $H_1(ID_i)$, r_i) is the corresponding tuple on the H_1-list. Then $\mathcal{B}$ uses the private key D_{ID_i} to compute the corresponding blinded signature as in BSign.
  - If $ID_i = ID^*$, $\mathcal{B}$ sends P'_{m_i} to its helper oracle $\mathcal{HO}$. Let (R_i, S_i, T_i) be the corresponding answer. $\mathcal{B}$ sets the blinded signature as (A'_i, B'_i, C'_i), where $A' = T_i, B'_i = S_i, C'_i = R_i$. It is obvious that this simulated signature is valid (see remark 1 in Section 2 and the algorithm Verifiy in Section 4).
- Outputs. At last, $\mathcal{A}$ outputs a list of message-signature pairs $((m_1, (A_1, B_1, C_1))$, $\ldots$, $(m_n, (A_n, B_n, C_n))$ with respect to the identity ID^*, where n is strictly larger than the number of executions of the protocol Issue with respect to the identity ID^*, and hence strictly larger than the number of queries made by $\mathcal{B}$ to its helper oracle $\mathcal{HO}$. $\mathcal{B}$ outputs $A_1, B_1, A_2, B_2, \ldots, A_n, B_n$. Here note that a valid signature (A_i, B_i, C_i) satisfies $e(A_i, B_i) = e(H_1(ID^*), H_2(m_i))^x = (Y, H_2(m_i))^x$ (see remark 1 in Section 2), and $H_2(m_i)$ is obtained from the target oracle. So the one-more BDHI problem is solved by $\mathcal{B}$.

It is easy to see that the view of $\mathcal{A}$ in the simulated experiment is indistinguishable from its view in the real experiment, and that $\mathcal{B}$ is successful only if $\mathcal{A}$ is successful. Thus, the probability ϵ_2 that $\mathcal{B}$ succeeds is at least the probability ϵ_1 that $\mathcal{A}$ succeeds. Algorithm $\mathcal{B}$'s running time is the same as $\mathcal{A}$'s running time plus the time it takes to respond to q_{H_1} H_1-hash queries, q_{H_2} H_2-hash queries, q_E extract queries and q_S signature issue queries. Each query requires at most four exponentiations (corresponding to issue queries for $ID_i \neq ID^*$) in $\mathbb{G}_1$ which we assume takes time $c_{\mathbb{G}_1}$. Hence, the total running time t_2 is at most $t_1 + 4c_{\mathbb{G}_1}(q_{H_1} + q_{H_2} + q_S + q_E)$ as required. This completes the proof of Theorem 1. □

Combing the above lemmas, we obtain the following theorem:

Theorem 2 *If the one-more BDHI assumption is true in the group $\mathbb{G}_1$, then the proposed ID-based blind signature scheme is secure against one-more forgery under parallel chosen message and ID attacks in the random oracle model.*

6 ID-based Blind Signatures: A Comparison

Table 1. Efficiency Comparison of ID-based Blind Signatures

	Signer	User	Verifier	Move	Size	Model
Ours	3M	4M+4e	4e	2	$3\|q\|$	ROM+1m-BDHI
ZK02 [28]	3M	3M+3e	1E+2e	3	$2\|q\|$	ROM+CDH+ROS(?)
ZK03 [29]	2M	4M+2e	1M+2e	3	$2\|q\|$	ROM+CDH+ROS(?)
HCW05 [16]	2M+1e	1M+3E+3e	1M+2e	3	$2\|q\|$	ROM+CDH+ROS(?)
Schnorr [22,25]	1E	3E	2E	4	$2\|q\| + Cert$	ROM+DLP+ROS(?)
Chaum82 [12]	1E	2E	2E	4	$\|n\| + Cert$	ROM+1m-RSA
Boldyreva03 [7]	1M	2M+4e	4e	4	$\|q\| + Cert$	ROM+1m-CDH
CKW04 [10]	25E	38E	2E	10	$\|p\| + 2\|q\| + Cert$	SM+CRS+SRSA+Seqn.
KZ05 [21]	5M+10E+6e	7M+15E+18e	1M+6e	6	$3\|q\| + Cert$	SM+CRS+DLDH+LRSW
Okamoto06 [23]	6M+3E	10M+5E+4e	3M+4e	6	$\|p\| + 2\|q\| + Cert$	SM+CRS+DCR+2SDH
Fischlin06 [15]	1E	NIZK	NIZK	4	NIZK+$Cert$	SM+CRS+GC

In this section, we give an efficiency comparison of ID-based blind signatures (ID-BS) (see Table 1). The purpose is to show the advantages of our scheme compared with existing solutions. Namely, as we claim before, the proposed scheme is the *first one-round* ID-base blind signature scheme, which is secure against generic parallel attack without relying on the intractability of ROS-problem.

As the main computational overheads, we only consider modular exponentiations (denote by E), scalar multiplications (denote by M), and bilinear mappings (denote by e). Since simultaneous exponentiations can be efficiently carried out by means of an exponent array, for simplicity we treat the cost for $a_1^{x_1}a_2^{x_2}$ or $a_1^{x_1}a_2^{x_2}a_3^{x_3}$ as just one single exponentiation. To count the computational costs of the signer, user and verifier in the above deduced ID-BS schemes, we assume the PKG use a similar underlying signature to issue certificates for signers. That is, the PKG uses Schnorr signature in the ID-based blind Schnorr signature, the RSA signature with a full domain hash in the ID-based Chaum and CKW blind signature schemes [12,10], and the BLS short signature in the ID-based Boldyreva, KZ, and Okamoto blind signature schemes [7,21,23]. For the generic scheme proposed by Fishlin [15], there are no concrete values since his scheme relies on general NIZK to prove the correctness of a ciphertext. About the security model, we mainly consider the following aspects: (1) whether a scheme is secure in the random oracle model (ROM) or standard model (SM); (2) whether a scheme needs common reference string (CRS); (3) whether a scheme relies on the intractability of ROS problem; and (4) what are the computational assumptions required.

First of all, we remark that the first four schemes (including our construction) in Table 1 are explicitly ID-BS schemes, while all other schemes are deduced from

the certificate-based generic construction [18], which is an extension of the result given in [5]. Here, note that due to the usage of certificates in Galindo et al.'s approach, the round complexity, the communication complexity and the signature size are also increased in all deduced ID-BS schemes. For example, though the standard blind signature schemes in [12,7,15] are round-optimal (i.e., they are one-round or 2-moves solutions), the correspond ID-based blind signatures become 4-move schemes. Compared with efficient ID-based blind signatures deduced from [12,7], our scheme is round-optimal (i.e. two moves rather than 4 moves) and has shorter signatures (without using a certificate to binding a random public key with each signer).

Secondly, we remark that the four schemes (ZK02,ZK03,HCW05,Schnorr) are not provably secure against one-more forgery. Furthermore, their security needs the ROS assumption which results in the loss of practical efficiency, since to guarantee the security one has to select q as large as 1600 bits. In contrast, the security of our scheme is based on the one-more BDHI assumption which is one-more version of the BDHI assumption. And the BDHI assumption is weaker than the well-known bilinear Diffie-Hellman assumption. In the existing literature [8], it is believed that the 160-bit q can ensure the difficulty of the BDH problem on the bilinear group $\mathbb{G}_1$ of order q. In the full paper of [3], the one-more-RSA-inversion problem and its analogues are fully discussed. It is trivial to extend the results of [3] to the case of one-more-BDHI problem. As argued in [3], although the one-more BDHI assumption is stronger than the relative BDHI assumption, it *seems feasible* to believe that the 160-bit q is enough to ensure the difficulty of the 1m-BDHI problem on the bilinear group $\mathbb{G}_1$ of order q. Of course, our scheme based on 160-bit q-order bilinear groups will be dramatically efficient than the previous analogues [28,29,16] based on 1600-bit q-order bilinear groups.

Thirdly, we remark that the last four schemes are all provably secure in the standard model but need common reference strings. At the same time, those schemes are not much efficient, since in the blind signature issuing protocols some kinds of ZK proofs are involved.

At last, we remark that the overload of the PKG of our scheme is much more light than that of the generic ID-based blind signatures due to Galindo et al. [18]. As we all know, one of the main motivations of ID-based cryptography is to solve the problem of the burdensome key management in PKI-based cryptography. However, for Galindo et al.'s generic construction, to ensure blindness, the PKG should guarantee that one identity can not get more than one private keys. So, like the CA (certificate authority) in PKI-based cryptography, PKG has to face the key management problem: he must cautiously store all the private keys issued to the identities. In contrast, what the PKG in our scheme need to do is to keep his master private key secret. In this sense, we say that Galindo et al. [18] may forget *one of the most important tasks (key management)* of ID-based cryptography, when they constructed the generic ID-based blind signature scheme.

Based on the above discussion, we conclude that the proposed scheme is the first one-round ID-based blind signature, which is provably secure against

generic parallel attack without relying on the ROS problem and any set-up assumptions, in the the random oracle model. Compared with ID-based blind scheme deduced from Galindo et al.'s generic approach, which can be secure in the stand model, our solution is much more efficient in all aspects of round complexity, computational complexity, signature size and the overload of PKG.

Additionally, as stated in [18], the ID-based framework (the algorithms of Setup and Private Key Extraction) due to Galindo et al. can not support ID-based encryption scheme. However, it is the ID-based encryption scheme due to Boneh and Franklin that revives ID-based cryptography [8]. Of course, the practical application of the ID-based signature schemes with additional properties [18]under so limited ID-based framework will not be very exiting. In contrast, our ID-based blind signature scheme is completely compatible with all ID-based cryptographic primitives from bilinear pairings including ID-based encryption scheme in [8].

7 Other Considerations

First, the new formalized 1m-BDHI assumption may be of independent interest, since other recently proposed computation assumptions in one-more flavor, such as One-more-RSA-inversion [3], one-more CDH [7], one-more discrete logarithm [4], have found many applications in provable security for blind signatures [3,7], transitive signatures [4], identification protocols [2] and so on.

Second, the underlying ID-based signature scheme may be of independent interest, since it avoids to use the proof of knowledge paradigm and has a loose algebraic structure which already allows the efficient extension to blind signatures. In fact, the underlying ID-based signature scheme is not strongly unforgeable, but satisfy the well-known standard definition of unforgeability. However, a non-strongly unforgeable signature may have other advantages over the strongly unforgeable one. For example, in [17], the authors constructed the first constant-length ID-based aggregate signature scheme based on an non-strongly unforgeable ID-based signature scheme.

8 Conclusion

In this paper, we proposed a new ID-based blind signature scheme based on bilinear pairings. More specifically, the proposed scheme has been proved to be secure in the random oracle model, under the one-more bilinear Diffie-Hellman inversion (1m-BDHI) assumption. To the best of our knowledge, our ID-base blind signature scheme is the first one with optimal round-complexity. In addition, we argued that our scheme is a practical identity-based blind signature scheme from bilinear pairings, compared existing solutions [25,26,15], which are actually inefficient and rely on the difficulty of ROS-problem. We specially showed the advantages of our ID-based blind signature schemes over Galindo et al.'s generic construction in terms of the PKG's overload and the compatibility, which are among the most important reasons for the revival of ID-based cryptography.

References

1. J. Baek and Y. Zheng. Identity-based threshold signature scheme from the bilinear pairings. In IAS'04 track of ITCC'04, pp.124-128. IEEE Computer Society, 2004. The full paper is available at: http://www1.i2r.a-star.edu.sg/~jsbaek/publications/pub_list.html.
2. M. Bellare and A. Palacio. GQ and Schnorr identication schemes: Proofs of security against impersonation under active and concurrent attack. In CRYPTO 2002, LNCS 2442, pp.162-177. Springer-Verlag, August 2002.
3. M. Bellare, C. Namprempre, D. Pointcheval and M. Semanko. The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. In Financial Cryptography 01, LNCS 2339, pp.319-338. Springer-Verlag, 2001. The full paper is available at: eprint.iacr.org/2001/002.pdf
4. M. Bellare and G. Neven. Transitive Signatures Based on Factoring and RSA. In ASIACRYPT '02, LNCS 2501, pp. 397–414. Springer-Verlag, 2002. The full paper is available at http://eprint.iacr.org/2004/215.pdf.
5. M. Bellare, C. Namprempre, G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In Eurocrypt'2004, LNCS 3027, pp. 268–286. Springer-Verlag,2004.
6. M. Bellare and P. Rogaway. Random Oracles Are Practical: a Paradigm for Designing Efficient Protocols. In Proc. of the 1st CCS, pp. 62-73. ACM Press. New York, 1993.
7. A. Boldyreva. Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In PKC 2003, LNCS 2567, pp.31-46. Springer-Verlag, 2003.
8. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Crypto 2001, LNCS 2139, pp.213-229. Springer-Verlag, 2001.
9. D. Boneh, B. Lynn, H. Shacham. Short signatures from the Weil pairing. In Asiacrypt'2001, LNCS 2248, pp. 514–532. Springer-Verlag, 2002.
10. J. Camenisch, M. Koprowski, B. Warinschi. Efficient Blind Signatures Without Random Oracles. In Security in Communication Networks (SCN 2004), LNCS 3352, pp. 134-148. Springer-Verlag, 2005
11. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In PKC 2003, LNCS 2567, pp.18-30. Springer-Verlag, 2003.
12. D. Chaum. Blind signatures for untraceable payments. In Crypto'82, pp. 199-203. New York: Plenum Press, 1983.
13. J. H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In Eurocrypt 2006, LNCS 4004, pp.1-11. Springer-Verlag, 2006.
14. R. Dutta, R. Barua, P. Sarkar. Pairing-based cryptography: a survey. IACR preprint sever, submission 2004/064, 2004.
15. M. Fischlin. Round-Optimal Composable Blind Signatures in the Common Reference String Model. In Crypto 2006, LNCS 4117, pp. 60-77. Springer-Verlag, 2006.
16. Z. Huang, K. Chen, Y. Wang. Efficient Identity-Based Signatures and Blind Signatures. In CANS 2005, LNCS 3810, pp.120-133. Springer-Verlag, 2005.
17. C. Gentry, Z. Ramzan. Identity-Based Aggregate Signatures. In Public Key Cryptography 2006, LNCS 3958, pp.257-273. Springer-Verlag, 2006
18. D. Galindo, J. Herranz, and Eike Kiltz. On the Generic Construction of Identity-Based Signatures with Additional Properties. In: Asiacrypt 2006 (to appear). Full paper is available at http://eprint.iacr.org/2006/296.

19. R Granger and N.P. Smart. On Computing Products of Pairings. IACR preprint sever, submission 2006/172, 2006.
20. A. Joux. The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems. In Algorithm Number Theory Symposium- ANTS 2002, LNCS 2369, pp.20-32. Springer-Verlag, 2002.
21. A. Kiayias, H. Zhou. Two-Round Concurrent Blind Signatures without Random Oracles. Number 2005/435 in Cryptology eprint archive. eprint.iacr.org, 2005.
22. D. Pointcheval, J. Stern. Security arguments for digital signatures and blind signatures. J. of Cryptology, 2000, 13: 361-396.
23. T. Okamoto. Efficient Blind and Partially Blind Signatures Without Random Oracles. In: Pro. of 3rd Theory of Cryptography (TCC'06), LNCS 3876, pp. 80-99. Springer-Verlag, 2006.
24. W. Qiu. Converting normal DLP-based signatures into blind. Applied Mathematics and Computation, Volume 170, Issue 1, 1 November 2005, pp.657-665.
25. C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In ICICS 2001, LNCS 2229, pp. 1-12. Springer-Verlag, 2001.
26. A. Shamir. Identity-based cryptosystems and signature schemes. In Crypto 84, LNCS 196, pp.47-53. Springer-Verlag, 1984.
27. D. Wagner. A generalized birthday problem. In Crypto 2002, LNCS 2442, pp.288-303. Springer-Verlag, 2002.
28. F. Zhang, K. Kim. ID-based blind signature and ring signature from pairings. In Asiacrypt 2002, LNCS 2501, pp.533-547. Springer-Verlag, 2002.
29. F. Zhang, K. Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings. In ACISP2003, LNCS 2727, pp.312-323. Springer-Verlag, 2003.