Round-Optimal ID-Based Blind Signature Schemes without ROS Assumption

Wei Gao
Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
Department of Mathematics and Informatics, Ludong University, Yantai, China
Guilin Wang
School of Computer Science & Software Engineering, University of Wollongong, NSW 2522, Australia
Email: guilin@uow.edu.au
Xueli Wang*
School of Mathematics, South China Normal University, Guangzhou, China
*Corresponding Author Email: wangxuyuyan@gmail.com
Fei Li
Department of Mathematics and Informatics, Ludong University, Yantai, China
Email: miss_lifei@163.com

***Abstract*—This paper presents two Identity-Based Blind Signature (IBBS) schemes based on bilinear pairings. Both of them enjoy the following features. First, they achieve the optimal bound of round complexity for blind signatures, i.e., each signature can be blindly generated with one round (or two moves) of message exchanges between the signature requesting user and signer. Second, their security is proved without the ROS assumption, which assumes that it is infeasible to find an overdetermined, solvable system of linear equations modulo q with random inhomogenities. Due to this reason, the order of underlying group does not need to be very large any more, as compared to the previous work. Third, the key extraction algorithm used is the most popular one in ID-based cryptography. In fact, the proposed two constructions are first IBBS schemes enjoying all the above advantages. Different from other IBBS schemes, these two IBBS schemes are constructed from scratch in the sense that new ID-based signature schemes are customized and new assumptions (e.g., two versions of one-more bilinear Diffie-Hellman inversion assumption) are formalized. We also show that the new ID-based schemes and new assumptions may have other interesting applications.**

***Index Terms*—Provable security, Identity-based signature, Blind signature , Bilinear pairing, ROS assumption**

I. Introduction

In 1984, Shamir [34] introduced the concept of identity-based (ID-based for short) public key cryptosystems in which a user's public key can be easily derived from his identity by applying a publicly available function, while his private key can only be calculated for him by a trusted authority, called Private Key Generator (PKG). ID-based cryptosystems are a good alternative for conventional public key primitives working in certificate-based public key infrastructure (PKI). In 2000, Joux [26] used the Weil pairing to construct the first one-round tripartite Diffie-Hellman key agreement protocol. In 2001, Boneh and Franklin [2] presented the first ID-based encryption scheme from bilinear pairings. Since then, in the so-called *identity-based cryptography* field, many ID-based cryptographic schemes have been proposed [14], [18] and bilinear pairing has become the most popular tool for constructing ID-based cryptography.

Blind signature, introduced by Chaum in 1982 [13], is a variant of digital signatures, in which a user can get a signature from a signer without revealing the message signed to the signer. Blind signatures play an important role in many security applications, such as e-cash and e-voting, where privacy is crucial. In security, they should satisfy blindness and unforgeability. Informally, blindness requires that the signer's view during signing process and the resulting signature should be statistically independent. Unforgeability can be formalized as one-more forgery under a parallel attack in [32]: the attacker cannot output $l+1$ signatures, if it interacts in parallel with the signer no more than l times. In 2001, Bellare et al. [5] proved the security of the Chaum's RSA-based blind signature scheme in the random oracle model under the novel "one-more-RSA-inversion" assumption. In 2003, Boldyreva proposed a blind signature scheme based on pairing and proved its security under the one-more computational Diffie-Hellman (CDH) assumption [8]. In 2001, Schnorr [35] showed that the Schnorr's blind signature scheme is provably secure under the ROS assumption (refer to Definition 6) in the generic group model [19] and the random oracle model [7]. Unfortunately, at Crypto 2002 Wagner [36] showed that there is a subexponential time algorithm to break the ROS-problem. Consequently, a group of order $q > 2^{1600}$ may be needed for ensuring 80-bit security. Furthermore, the ROS assumption is not related to the well known discrete logarithm (DL) assumption, although the latter is necessary for DL-based signature schemes. In addition, round complexity is also an important factor for an blind signature scheme,

This work is partially supported by National Natural Science Foundation of China (No. 60973135, 60970111,61202475) and Humanities and Social Science Research Project of the Ministry of Education (11YJCZH039).This work was partly presented at the conference of Pairing 2008 [22] and is significantly extended and improved here.

doi:10.4304/jcm.7.12.909-920

especially for some applications like e-voting and e-cash. One round (i.e. two moves) is the optimal bound of round complexity. Namely, to generate a signature blindly at least two messages must be exchanged between the signer and signature requesting user. In fact, there are a few PKI-based blind signature schemes [8], [13], [20], [28] with round-optimal signature generation protocols. Hence, the one-round blind signature scheme without ROS assumption, such as Boldyreva's blind signature scheme, are more desirable than Schonorr's blind signature scheme which requires 3 moves of communication and the ROS assumption.

The combination of the two above concepts, ID-based cryptography and blind signatures, results in the concept of ID-based blind signature (IBBS) schemes. Roughly speaking, the existing IBBS schemes can be divided into two classes. We note that the first class including the results in [24], [25], [37], [38] are similar to the Schnorr's blind signature scheme as follwos: (1) The underlying ID-based signature schemes (or Schonrr signature scheme) can be seen as modularly transformed from identity-based identification (or Schnorr Identification scheme) using the Fiat-Shamir trnasform [3]; (2) These IBBS schemes can be seen as constructed based on the corresponding identity-based signature scheme using the well formalized techniques [33] to construct the Schnorr blind signature scheme. As a result of this similarity, like Schnorr's blind signature scheme, their security has to rely on the generic group model and the ROS assumption, in addition to the random oracle model and the discrete logarithm assumption. On the other hand, all of the aforementioned IBBS schemes require two rounds (more specifically, three moves) of message exchange between the signer and the user.

The other class of IBBS schemes is due to Galindo et al's generic transformation [21], which transforms a standard blind signature scheme into an ID-based blind signature scheme. The main idea is a folklore and can be traced back to Shamir [34] and Bellare et al [3]. We briefly review this approach as follows. The PKG first selects a key pair (sk_i, pk_i) for a signer ID_i, issues a certificate $Cert_i$ to certify the string $ID_i||pk_i$ by using the PKG's PKI-based private key, and then forwards $(sk_i, Cert_i)$ to the signer ID_i. To get an ID-based blind signature, a user first enquires the signer ID_i for its $Cert_i$ and checks the validity of $Cert_i$. If this procedure is successful, the user and the signer can engage in the standard blind signature issuing protocol to output a signature σ for a message m under the public key pk_i. The final ID-based signature is a pair $(\sigma, Cert_i)$, which is valid if $Cert_i$ is a certificate for ID_i together with some public key pk_i issued by the PKG, and σ is a valid signature for message m with respect to pk_i.

Although this work is a very interesting result of ID-based signatures, there are several restrictions in Galindo et al.'s approach. (1) It requires that PKG maintain a directory for all users to avoid issuing two different private keys for the same user. So the advantage of ID-based cryptography in simple key management is somewhat destroyed. (2) If the meaning of "ID-based" due to Galindo et al. [21] is adopted, traditional PKI-based signature schemes can also be seen as ID-based signature schemes [2] and even enjoy better properties. Here, note that for Galindo et al.'s method, the meaning of "ID-based" is taken as that the verifier needs to know only the authority's public key and the signer's identity. In this sense, the PKI-based signature can be seen as "ID-based", when the identity is embedded in the certificate and the public key is included in a signature. On the other hand, the disadvantage of key escrow problem for ID-based signature schemes does not work for PKI-based signature schemes. (3) Under this kind of key extraction method, the ID-based encryption scheme can never be deployed. Especially, the key extracting algorithm is completely different from that for the most popular and somewhat standard ID-based encryption scheme due to Boneh and Franklin [2]. Although, in practice, the decryption key and the signing key could be different, it is usually desirable if they can be generated and managed by PKG in a unified form. (4) Galindo et al.'s method somewhat destroys the most important idea for ID-based cryptography: the public key of a user can be directly derived from his identity and therefore digital certificates are avoidable.

In 2009, Phong and Ogata [31] propose a new IBBS scheme in the standard model based on blind HIBE schemes. This result is very interesting in theory, because it is secure in the standard model under the CDH assumption. However, there are oblivious disadvantages in practice. On one hand, it needs additional rounds of communication for the involved complicated zero knowledge proof with 21 variables. On the other hand, the length of the public key is very long, about 25 elements in elliptic curve group.

So, we are naturally motivated to consider how to construct one-round IBBS scheme without ROS assumption which, unlike the Galindo et al.'s generic method, is well suitable for the ID-based setting. In this paper, we propose two one-round ID-based blind signature schemes without ROS assumption. They are constructed from scratch by a way different from the above two classes of IBBS schemes, i.e., the proposed IBBS schemes rely on newly formalized computational assumptions and new basic ID-based signature schemes. More specifically, our contribution can be summarized as follows. (1) The round complexity of our IBBS schemes is optimal. Namely, each interactive signature generation requires the signature requesting user and the signer to transmit only one message to the other. (2) The security proof against generic parallel attack doesn't depend on the ROS assumption and hence the order of underlying group does not need to be very large any more, as compared to the previous work. (3) To prove their security, we introduce new plausible computational assumptions, called two versions of *one-more bilinear Diffie-Hellman inversion assumptions* (**1m-BDHI-1,1m-BDHI-2**, for short). These new assumptions may be of independent interest, since other recently pro-

posed computational assumptions in one-more flavor, such as one-more-RSA-inversion [5], one-more CDH [8], one-more discrete logarithm [4], have found many applications in provable security for blind signatures [5], [8], transitive signatures [4], identification protocols [6] and so on. (4) Our IBBS schemes avoid the restrictions in the Galindo et al.'s IBBS scheme as mentioned above. For example, it is fully "ID-based" in the sense that the public key for each user can be fixed and publicly generated by anyone from only the identity information. (5) The underlying ID-based signature schemes may be of independent interest, since they avoid using the most popular paradigm of Fiat-Shamir transform [6] and have a loose algebraic structure which already allows the efficient extension to blind signatures.

The rest of the paper is organized as follows. In Section 2, we first review some preliminaries on bilinear pairings and some computational problems, and then formalize the 1m-BDHI-1 assumption and 1m-BDHI-2 assumption. Section 3 deals with the security model of IBBS schemes. We then present the first IBBS scheme in Section 4, and prove its security in Section 5. In Section 6, we then simply present the second IBBS scheme by omitting many details, as it can be similarly constructed and analyzed as the first IBBS scheme. After giving a comprehensive comparison between the proposed constructions and other IBBS schemes in Section 7, we point out that new identity-based signatures derived from our IBBS schemes and the proposed new computational assumptions in one-more flavor may be of independent interest in Section 8. Finally, Section 9 concludes the paper.

II. Preliminaries

In this section, we present the definitions of bilinear pairings and some computational assumptions relative to the new ones of ours. Then we propose the four new assumptions of BDHI-1, BDHI-2, 1m-BDHI-1 and 1m-BHI-2. And we point out the relations between these new assumptions and some existing assumptions.

Definition 1: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be cyclic groups of prime order q and let P be a generator of $\mathbb{G}_1$ (i.e., $\mathbb{G}_1 = \langle P \rangle$). Here, $\mathbb{G}_1$ is written additively, and $\mathbb{G}_2$ multiplicatively. A map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is said to be an bilinear pairing 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. $e(P, P) \neq 1$, where 1 is the identity of group $\mathbb{G}_2$;
(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 G_1, G_2, the prime order q, the generator P of 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 $abP \in G_1$, where $a, b \in_R \mathbb{Z}_q$.
- **Bilinear Diffie-Hellman (BDH) Problem** [2]: 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** [27]: Given $h \in G_2$, find a pair $(S, T) \in G_1 \times G_1$ such that $e(S, T) = h$, where $e : G_1 \times G_1 \to G_2$ denotes the Tate pairing.
- **Modified Generalized Bilinear Inversion (MGBI)** [1]: Given $h \in G_2$ and the generator $P \in G_1$, find a point $S \in G_1$ such that $e(P, S) = h$, where e denotes the bilinear pairing.

Somewhat like the above GTI and MGBI problems, we propose two new computational problems as follows.

Definition 2: (Bilinear Diffie-Hellman Inversion 1 (BDHI-1) Problem.) Given three random elements $xP, yP, zP \in \mathbb{G}_1 = \langle P \rangle$, compute two elements $S, T \in G_1$ such that $e(S, T) = e(P, P)^{xyz}$, where $x, y, z \in_R \mathbb{Z}_q$. Accordingly, the **Bilinear Diffie-Hellman Inversion 1 (BDHI-1) assumption** states that: there is no probabilistic polynomial time (PPT) algorithm that can solve the BDHI-1 problem with non-negligible probability.

Definition 3: (Bilinear Diffie-Hellman Inversion 2 (BDHI-2) Problem.) Given three random elements $xP, Y = yP, Z = zP \in \mathbb{G}_1 = \langle P \rangle$, compute two elements $S, T \in G_1$ such that $\frac{e(S,Z)}{e(Y,T)} = e(P, P)^{xyz}$, where $x, y, z \in_R \mathbb{Z}_q$. Accordingly, the **Bilinear Diffie-Hellman Inversion 2 (BDHI-2) assumption** states that: there is no PPT algorithm that can solve the BDHI-2 problem with non-negligible probability.

It is obvious that the BDH problem can be solved if either the BDHI-1 or the BDHI-2 problem can be solved. And it is also obvious that the BDHI problems can solved if the CDH problem can be solved. So BDHI-1 (BDHI-2) assumption is somewhere between CDH assumption and BDH assumption. That is:

Fact 1: Both BDHI-1 and BDHI-2 assumptions are weaker than the BDH assumption, but stronger than the CDH assumption.

Remark 1: However, it is not clear about the relationship between the BDHI-1 assumption and the BDHI-2 assumption.

By extending the assumptions of BDHI-1 and BDHI-2 to the one-more version, we obtain two new computational assumptions called one-more bilinear Diffie-Hellman Inversion assumption 1 and 2 (1m-BDHI-1 and 1m-BDHI-2). In fact, there exist many computational assumptions in the one-more flavor, such as one-more-RSA-inversion [5], one-more CDH [8], 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 [6], blind signature schemes [4], [8], transitive signatures [5]. Just like the one-more-RSA-inversion assumption and one-more-CDH assumption are formalized for security proof of Chaum's blind signature scheme and Boldyreva blind signature scheme respectively, the 1m-BDHI-1 and 1m-BDHI-2 are also formalized for security proof for the two proposed IBBS schemes.

Definition 4 (1m-BDHI-1 Assumption): Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing, where G_1 and G_2 be groups of prime order q and P be a generator of G_1. Let x, y be random elements in $\mathbb{Z}_q$ and let $X = xP, Y = yP$. The adversary $\mathcal{A}$ is given $(e, G_1, G_2, q, P, X, Y)$ and has access to two oracles.

- The first one is a target oracle $\mathcal{TO}$ that returns a random point $Z \in G_1$ for each time it is invoked (it takes no inputs).
- The second one is the helper oracle $\mathcal{HO}$ which takes as input the value $Z \in G_1$, and returns $S, T \in G_1$ randomly from
$$\{(S,T)|e(S,T) = e(xyP, Z)\}.$$
Additionally, this help oracle $\mathcal{HO}$ returns a piece of auxiliary information R which satisfies the equations
$$e(R,S) = e(xP, yP) \text{ and } e(R,Z) = e(P,T).$$
Here note that R is the proof for the equation $e(S,T) = e(Y,Z)^x$. In fact, suppose that $R = rP$. Then the above two equations imply the following two equations:
$$S = r^{-1}xyP \text{ and } T = rZ.$$
So we have $e(S,T) = e(xyP, Z) = e(Y,Z)^x$.

We say that $\mathcal{A}$ wins if its output is a sequence of points $S_1, T_1, \ldots, S_n, T_n \in G_1$ satisfying $e(S_1, T_1) = e(xyP, Z_1), \ldots, e(S_n, T_n) = e(xyP, Z_n)$, where all different $Z_1, \ldots, Z_n$ are random points returned by $\mathcal{TO}$ and the number of queries made by $\mathcal{A}$ to its helper oracle $\mathcal{HO}$, is strictly less than n. The 1m-BDHI-1 advantage of $\mathcal{A}$, denoted $Adv_{\mathcal{A}}^{1m-BDHI-1}(k)$, is the probability that $\mathcal{A}$ wins, taken over the coins used in the generation of $(e, G_1, G_T, q, P, X, Y)$, 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 $Adv_{\mathcal{A}}^{1m-BDHI-1}(k)$ is negligible for all polynomial-time adversaries $\mathcal{A}$.

Remark 2: Note that in Definition 4, we require that the adversary $\mathcal{A}$ should output multiple pairs (S_i, T_i) corresponding to random Z_i's which are selected by the target oracle $\mathcal{TO}$, rather than $\mathcal{A}$ itself. Otherwise, 1m-BDHI-1 assumption were invalid. The reason is that for fixed $X = xP$ and $Y = yP$, if given a pair (S,T) satisfying $e(S,T) = e(xyP, Z)$, $\mathcal{A}$ can trivially create a new pair (S', T') satisfying $e(S', T') = e(xyP, Z')$ by setting $S' = aS$, $T' = bT$, and $Z' = abZ$, where $a, b \in_R \mathbb{Z}_q$ are random numbers selected by $\mathcal{A}$.

Definition 5 (1m-BDHI-2 Assumption): Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing, where G_1 and G_2 be groups of prime order q and P be a generator of G_1. Let x, y be random elements in $\mathbb{Z}_q$ and let $X = xP, Y = yP$. The adversary $\mathcal{A}$ is given $(e, G_1, G_2, q, P, X, Y)$ and has access to two oracles.

- The first one is a target oracle $\mathcal{TO}$ that returns a random point from G_1 for each time it is invoked (it takes no inputs).
- The second one is the helper oracle $\mathcal{HO}$ which given $Z \in G_1$, returns $S, T \in G_1$ randomly from
$$\{(S,T)|\tfrac{e(S,Z)}{e(Y,T)} = e(xyP, Z)\}.$$
Additionally, this help oracle $\mathcal{HO}$ returns a piece of auxiliary information R such that
$$e(P,S) = e(R + xP, yP) \text{ and } e(R,Z) = e(P,T).$$
Hence R is the proof for the equation $\frac{e(S,Z)}{e(Y,T)} = e(xyP, Z)$. In fact, suppose that $R = rP$ for some r. Then the above two equations imply the following two equations:
$$S = (r + x)yP \text{ and } T = rZ.$$
So we have
$$\tfrac{e(S,Z)}{e(Y,T)} = \tfrac{e((r+x)yP,Z)}{e(yP,rZ)} = e(xyP, Z).$$

We say that $\mathcal{A}$ wins if its output is a sequence of points $S_1, T_1, \ldots, S_n, T_n \in G_1$ satisfying $\frac{e(S_1,Z_1)}{e(Y,T_1)} = e(xyP, Z_1), \ldots, \frac{e(S_n,Z_n)}{e(Y,T_n)} = e(xyP, Z_n)$ where all different $Z_1, \ldots, Z_n$ are random points returned by $\mathcal{TO}$ and the number of queries made by $\mathcal{A}$ to its helper oracle $\mathcal{HO}$, is strictly less than n. The 1m-BDHI-2 advantage of $\mathcal{A}$, denoted $Adv_{\mathcal{A}}^{1m-BDHI-2}(k)$, is the probability that $\mathcal{A}$ wins, taken over the coins used in the generation of $(e, G_1, G_T, q, P, X, Y)$, 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 $Adv_{\mathcal{A}}^{1m-BDHI-2}(k)$ is negligible for all polynomial-time adversaries $\mathcal{A}$.

For BDHI-1, BDHI-2, 1m-BDHI-1, 1m-BDHI-2, it is easy to see:

Fact 2: The hard problems of BDHI-1, BDHI-2, 1m-BDHI-1 and 1m-BDHI-2 have the trapdoor xyP.

In the definitions of 1m-BDHI-1 assumption and 1m-BDHI-2 assumption respectively, (S,T) is randomly chosen from the set $\{(S,T)|\frac{e(S,Z)}{e(Y,T)} = e(xyP, Z)\}$ and $\{(S,T)|\frac{e(S,Z)}{e(Y,T)} = e(xyP, Z)\}$ which are of order q. So we have:

Fact 3: In the assumptions of 1m-BDHI-1 and 1m-BDHI-2, the output (S,T) is statically independent of the trapdoor xyP.

Based on Facts 1, 2, 3 and comparison with other assumptions, we can confidently say that the assumptions of BDHI-1, BDHI-2, 1m-BDHI-1, 1m-BDHI-2 are plausible and reasonable. In fact, Fact 1 shows BDHI-1 (DBHI-2) problem is not easier than the famous BDH problem. As extending RSA assumption or CDH asusmption to their one-more version, we analogously extended BDHI-1 (BDHI-2) to 1m-BDHI-1 (BDHI-2) and then assume that it is intractable too. Furthermore, Fact 2 and Fact 3 shows the 1m-BDHI assumption seems a better computational assumption in the one-more version, since the answer provided to the adversary is independent of the the trapdoor. In contrast, for the 1m-RSA assumption or 1m-CDH assumption, the answer is dependent on the trapdoor, although it is infeasible to compute the trapdoor from given answer.

Remark 3: It may be better to provide more formal arguments for 1m-BDHI-1 and 1m-BDHI-2, as one reviewer suggested. However, I find that it seems somewhat difficult to do so. If it is not very difficult to completely formally explain the hardness of one more computational problems, then the security proof of Chaum's blind

signatures would not remain open for so long time [5]. Furthermore, almost all previous works relative to one-more computational assumptions [4]–[6], [8], [10] did not provide the formal arguments such as formal analysis in the generic group model. In fact, to provide the formal analysis in the generic group model, it is usual to provide a reduction between the object assumption and the supporting assumption. However, according the results of [10], it is very unlike to provide such reduction. Hence, maybe we should leave as an open problem to provide formal arguments for all existing one-more computational assumptions including 1m-BDHI-1 and 1m-BDHI-2.

Finally, we review the ROS problem.

Definition 6 (ROS Problem [35]): Given an oracle random function $F : \mathbb{Z}_q^l \rightarrow \mathbb{Z}_q$, 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.

To analyze the security of Schnorr's blind signature scheme, Schnorr [35] introduced the ROS-problem and shows that one-more-forgeries in the parallel attack for Schnorr's blind signature scheme is equivalent to solving the ROS-problem in the generic group model and random oracle model. Wagner [36] solves the ROS-problem for $l+1 = 2^t$ in $O(2^t q^{\frac{1}{(t+1)}})$-average time and space by a tree-like general birthday method. For $t = 9$, $|G| = 2^{160}$, this attack succeeds in $O(2^{25})$ average time performing $2^9 - 1$ parallel interactions with the signer. Consequently, it seems that we need a group of order $q > 2^{1600}$ if we wish to enjoy 80-bit security. In other words, the size of the group order in bits must be an order of magnitude larger than one might otherwise expect from the best currently-known algorithms for discrete logs in elliptic curve groups. So the ROS assumption is not so plausible and we should try to avoid using it when designing blind signature schemes.

III. Security Model of ID-based Blind Signatures

This section formally describes the syntax of ID-based blind signatures (Definition 7), and the two security requirements, i.e., blindness (Definition 8) and unforgeability (Definition 9).

Definition 7: An identity-based blind signature scheme $\mathcal{IBBS}$ can be described as a collection of the following four components (i.e. 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 8 (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 [7], $\mathcal{C}$ 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 $Adv_{IBBS}^{unforge}$ 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 9 (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) $Adv_{IBBS}^{unforge}$ 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 4: 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 [11], 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 which is the most powerful attack for blind signatures.

IV. First Construction: IBBS-I

Before describing the construction, we explain the basic idea. The signer first transforms the ID-based private key $D_{ID} \in G_1$ into a temporary private key $x_{ID} \in \mathbb{Z}_q$ and publishes the corresponding public key $x_{ID}P$. Additionally, it also publishes $x_{ID}^{-1} D_{ID}$ as the linking information between $x_{ID} \in \mathbb{Z}_q$ and D_{ID}. Then, by using similar blind signature technique due to Boldyreva [8], we can get the the first IBBS scheme: IBBS-I, which is described in detail below.

- Setup. The Private Key Generator (PKG) generates parameters and master keys as follows:
  - generates groups G_1 and G_2 of prime order q with bilinear pairing $e : G_1 \times G_1 \to G_2$;
  - $P \xleftarrow{R} G_1$;
  - $s \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP$;
  - chooses cryptographic hash functions $H_1, H_2 : \{0,1\}^* \to G_1$. The PKG's public parameter is $params = (G_1, G_2, e, q, P, P_{pub}, H_1, H_2)$; 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 $Q_{ID} = H_1(ID) \in G_1$.
- 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 $A' = x_{ID} P'_m, B' = x_{ID}^{-1} D_{ID}, C' = x_{ID} P, x_{ID} \xleftarrow{R} \mathbb{Z}_q$.
  - Unblind. First, the user verifies the blind signature (A', B', C') by checking whether $e(A', P) = e(P'_m, C')$ and $e(Q_{ID}, P_{pub}) = e(B', C')$.

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

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:

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

In fact, we can see that a valid signature σ for a message m has the following form: $(A, B, C) = (rH_2(m), r^{-1} D_{ID}, rP)$, where $r \in_R \mathbb{Z}_q$.

Similarly, it is easy to show that the blind signature generated by the honest signer in Bsign must be accepted by the user in the step Unblind.

Remark 5: After we submitted this work to ePrint (archive 2007-007), Sherman S.M. Chow informed us that the ID-based signature scheme implied by our above IBBS scheme is similar to the ID-based signature scheme due to him [16]. As we stated in Introduction, our IBBS scheme is motivated by solving some open problems related to ID-based blind signature schemes (see also the basic idea described at the beginning of this section), while the ID-based signature scheme in [16] is proposed as one of applications of the so-called *verifiable pairing*. Moreover, our IBBS scheme also implies a new construction of verifiable paring.

V. SECURITY PROOF OF IBBS-I

We first show that our scheme IBBS-I meets the property of *blindness*. Intuitively, this is true due to the fact that the signer receives only random elements in G_1, which are independent of the outputs of the user.

Theorem 5.1: The proposed ID-based blind signature scheme IBBS-I 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

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

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

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

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

Next, we analyze the unforgeability of the scheme IBBS-I as follows. Here note that it is obvious that our blind signature scheme is not strongly unforgeable (see Remark 1 in Section 3). Instead, we will prove that its security satisfies the standard definition given in Section 3. As in [12], 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 5.1: For the IBBS scheme IBBS-1, 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 $\mathsf{Extract}(ID)$ 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 $H'_1(ID_i), \mathsf{Extract}'(ID_i), \mathsf{Issue}'(ID_i, m)$ to be $H_1(ID'_i)$, $\mathsf{Extract}(ID'_i)$, $\mathsf{Issue}(ID'_i, m)$, 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, $\mathsf{Extract}'$, 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

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

Combining these,

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

as desired. □

Lemma 5.2: For the IBBS scheme IBBS-1, 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, 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 $(e, G_1, G_2, q, P, X, Y)$, 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 $(e, G_1, G_2, q, P, P_{pub})$ and the fixed identity ID^*, where $P_{pub} = X$.
- H_1-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 $Z_j \in G$ 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 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 $e(A_i, B_i) = e(H_1(ID^*), H_2(m_i))^x = (Y, H_2(m_i))^x$, 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 5.2: If the one-more BDHI assumption is true in the group G_1, then the proposed ID-based blind signature scheme IBBS-I is secure against one-more forgery under parallel chosen message and ID attacks in the random oracle model.

VI. Second Construction: IBBS-II

In this section, we presents the second IBBS scheme: IBBS-II, which is a result parallel to IBBS-I. It is designed using the same basic idea used for constructing IBBS-I. Roughly speaking, the signer first transforms the private key $D_{ID} \in G_1$ into the temporary private key $x_{ID} \in \mathbb{Z}_q$ and publishes the additional information $x_{ID}P$, $D_{ID} + x_{ID}Q_{ID}$. Then, the blind signature technique due to Boldyreva [8] is used to generate signatures blindly. As IBBS-II is very similar to IBBS-I, we here only describe the scheme and give the security results without details of security proof. It is straightforward to adapt the security proof of IBBS-I for IBBS-II.

IBBS-II is described as follows.

- Setup. The Private Key Generator (PKG) generates parameters and master keys as follows:
  - generates groups G_1 and G_2 of prime order q with bilinear pairing $e : G_1 \times G_1 \to G_2$;

- $P \xleftarrow{R} G_1$;
- $s \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP$;
- chooses cryptographic hash functions $H_1, H_2 : \{0,1\}^* \rightarrow G_1$. The PKG's public parameter is $params = (G_1, G_2, e, q, P, P_{pub}, H_1, H_2)$; 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 $Q_{ID} = H_1(ID) \in G_1$.
- 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 $A' = x_{ID}P'_m, B' = x_{ID}Q_{ID} + D_{ID}, C' = x_{ID}P, x_{ID} \xleftarrow{R} \mathbb{Z}_q$.
  - Unblind. First, the user verifies the blind signature (A', B', C') by checking whehter
    $$e(A', P) = e(P'_m, C') \text{ and } e(B', P) = e(Q_{ID}, P_{pub} + C').$$
    Next, the user selects a random number $r_2 \in \mathbb{Z}_q$ and computes the signature as (A, B, C), where $A = r_2 P_m + r_1^{-1} A', B = r_2 Q_{ID} + B', C = r_2 P + C'$, and $P_m = H_2(m)$.
- Verify. Let (A, B, C) be the signature on the message m and $P_m = H_2(m)$. The verifier checks that:
  $$e(A, P) = e(P_m, C) \text{ and } e(B, P) = e(Q_{ID}, P_{pub} + C).$$

Correctness. If a blind signature $\sigma = (A, B, C)$ on a message m has been issued by following the above Issue protocol, it is not difficult to see that

$$A = (r_2 + x_{ID})P_m, \ B = (r_2 + x_{ID} + s)Q_{ID},$$
$$\text{and } C = (r_2 + x_{ID})P).$$

By letting $r = r_2 + x_{ID} \bmod q$, we can see that a valid signature σ has the form $(A, B, C) = (rP_m, rQ_{ID} + D_{ID}, rP)$. Then, the signature verification equations are justified by

$$\begin{aligned} e(A, P) &= e(rP_m, P) = e(P_m, rP) = e(P_m, C), \text{ and} \\ e(B, P) &= e(rQ_{ID} + D_{ID}, P) = e(Q_{ID}, (r+s)P) \\ &= e(Q_{ID}, P_{pub} + C). \end{aligned}$$

Theorem 6.1: The proposed ID-based blind signature scheme IBBS-II is blind.

Theorem 6.2: If the one-more BDHI-2 assumption holds in the group G_1, then the proposed ID-based blind signature scheme IBBS-II is secure against one-more forgery under parallel chosen message and ID attacks in the random oracle model.

Remark 6: From the above descriptions given in Sections 4, 5, and 6, we can see that IBBS-I and IBBS-II are very similar with regarding to their structures, efficiency and security. The underlying computational assumptions, i.e., BDHI-1 and BDHI-2, are close to each other but they may be different (More exactly, as mentioned in Remark 1 we do not know if they implies each other or not). Since a small but subtle difference on computational assumptions may result in essential impact on the real security of cryptosystems, we believe that such paralleling work like BDHI-1 and BDHI-2 are also interesting.

VII. Comparison between IBBS-I and Other IBBS scheme

Table 1. Efficiency Comparison of ID-based Blind Signatures

Schemes	Signer	User	Verifier	Move	Signature Size
Our IBBS-I	3M (1M)*	4M+4e	4e	2	$3\|q\|$
Our IBBS-II	3M (1M)*	4M+4e	4e	2	$3\|q\|$
ZK02 [37]	3M	3M+3e	1E+2e	3	$3\|q\|$
ZK03 [38]	2M	4M+2e	1M+2e	3	$2\|q\|$
HCW05 [25]	2M+1e	1M+3E+3e	1M+2e	3	$2\|q\|$
PO09 [31]	2M	3M+4e+ *	4e	2+*	$3\|q\|$
Schnorr [32], [35]	1E	3E	2E	4	$2\|q\|$+Cert
Chaum [13], [21]	1E	2E	2E	4	$\|n\|$+Cert
Boldyreva [8], [21]	1M	2M+4e	4e	4	$\|q\|$+Cert
CKW04 [11], [21]	25E	38E	2E	10	$\|p\| + 2\|q\|$+Cert
KZ05 [21], [28]	5M+10E+6e	7M+15E+18e	1M+6e	6	$3\|q\|$+Cert
Okamoto [21], [30]	6M+3E	10M+5E+4e	3M+4e	6	$\|p\| + 2\|q\|$+Cert
Fischlin [20], [21]	1E	NIZK	NIZK	4	NIZK+Cert

: In IBBS-I and IBBS-II, fixed B', C' can be used by the signer. "" is the time and rounds number for the proof knowledge with 21 variables.

In this Section, we give a comprehensive comparison of ID-based blind signatures (IBBS) (see Table 1 and Table 2 below for details). The purpose is to show the advantages of our schemes IBBS-I and IBBS-II compared with existing solutions. Namely, they are first two round-optimal ID-base blind signature schemes, which are secure against generic parallel attack without relying on the intractability of ROS problem.

Table 1 compares the efficiency of ID-based blind signatures. First of all, we remark that the first five schemes (including our two constructions) in Table 1 are explicit IBBS schemes, while all other schemes are deduced from the underlying blind signatures by using the certificate-based generic transformation [21], which extends the result given in [3]. More specifically, we get these ID-based blind signature schemes from the corresponding blind signatures [8], [11], [13], [20], [30], [32], [35]. 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 IBBS 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 [35], the RSA signature with a full domain hash in the ID-based Chaum [13] and CKW04 [11] blind signature schemes, and the BLS short signature [9] in the ID-based Boldyreva [8], KZ [28], and Okamoto [30] blind signature schemes. For the generic scheme proposed by Fishlin [20], there are no concrete values since his scheme relies on general NIZK to prove the correctness of a ciphertext. 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 IBBS schemes. For example, though the standard blind signature schemes in [8], [13], [20] are round-optimal (i.e., they are one-round or 2-move solutions), the correspond ID-based blind signatures become 4-move schemes.

Note that Galindo et al.'s IBBS schemes can become 2-move if the user has already known the public key of the signer during an execution of the underlying blind signing protocol. The reason is that in this case, with the knowledge of the signer's ("ID-based") public key the signature requesting user can send the blinded message to the signer in the first round of signature issuing protocol. The IBBS scheme based on pairings due to Galindo et al. is an example for this case. In addition, as stated in Introduction we point out again that the functional limitations in Galind et al.'s generic approach are avoided in our scheme. In other words, compared with our IBBS schemes, Galindo et al.'s IBBS schemes can not be seen as "fully ID-based".

Table 2. Security Comparison of ID-based Blind Signatures

Schemes	ROM or SM	No CRS	No ROS	Assumptions	Proofs
Our IBBS-I	ROM	Yes	Yes	1m-BDHI-1	Yes
Our IBBS-II	ROM	Yes	Yes	1m-BDHI-2	Yes
ZK02 [37]	ROM	Yes	No	CDH	No
ZK03 [38]	ROM	Yes	No	CDH	No
HCW05 [25]	ROM	Yes	No	CDH	No
PO09 [31]	SM	NO	NO	CDH	Yes
Schnorr [32], [35]	ROM	Yes	No	DL	Yes
Chaum [13], [21]	ROM	Yes	Yes	1m-RSA	Yes
Boldyreva [8], [21]	ROM	Yes	Yes	1m-CDH	Yes
CKW04 [11], [21]	SM	No	Yes	SRSA	Yes
KZ05 [21], [28]	SM	No	Yes	DLDH+LRSW	Yes
Okamoto [21], [30]	SM	No	Yes	2SDH+DCR	Yes
Fischlin [20], [21]	SM	No	Yes	GC	Yes

On the security comparison of ID-based blind signatures, we mainly consider the following five aspects (Refer to Table 2): (1) whether the scheme is secure in the random oracle model (ROM) or standard model (SM); (2) whether a scheme does not need common reference string (CRS); (3) whether a scheme does not rely on the ROS assumption; (4) what the computational assumptions are required; and (5) whether rigorous security proofs have provided. According to Table 2, we can see that the last four schemes are all provably secure in the standard model but need common reference strings. At the same time, these schemes are not very efficient, since in the blind signature issuing protocols some kinds of zero knowledge proofs are involved (Check Table 1). In addition, note that the CKW04 scheme is only claimed to be secure in the scenario of sequential attacks, which are weaker than generic parallel attacks. The directly constructed schemes in [25], [37], [38] are computationally efficient, but their security against one-more forgery is not formally proved even under the ROS assumption. Based on the result in [21], [32], [35], the ID-based Schnorr blind signature scheme is secure against one-more forgery, but needs the ROS assumption, which leads to the loss of practical efficiency. That is, to guarantee the 80-bit security one has to select q as large as 1600 bits. Compared with efficient ID-based blind signatures deduced from [8], [13], both of our two scheme are round-optimal (i.e. two moves rather than 4 moves) and have shorter signatures (without using a certificate to binding a random public key with each signer).

Now, we compare the computational assumptions. The IBBS schemes proposed in [37], [38], [25] all rely on the CDH assumption. In contrast, the security of our schemes IBBS-I and IBBS-II are based on two one-more BDHI assumptions which are one-more versions of two BDHI assumptions. According to Fact 1, the BDHI assumptions are stronger than the CDH assumption. So, these three schemes seems better than ours as they need a weaker assumption. However, as just mentioned the security of all these schemes rely on the ROS assumption and formal security results are not yet established. Therefore, they are not useable in practice due to both efficiency and uncertain security. Additionally, He et al. [24] recently propose a new IBBS scheme without pairings. Since it follows the Schnorr's construction method as formalized in [32], [33], [35], it remains to be disadvantageous in terms of round efficiency (3 rounds) and assumptions (ROS).

On the other hand, Fact 1 states that BDHI assumptions are weaker than the well-known bilinear Diffie-Hellman (BDH) assumption. Literature [2] argued that a 160-bit q can ensure the difficulty of the BDH problem on the bilinear group G_1 of order q. In [5], the one-more-RSA-inversion problem and its analogues are fully discussed. These discussions of [5] can be straightforwardly extended to the case of one-more-BDHI problems. So, although the one-more BDHI assumptions are stronger than the relative BDHI assumptions, it *seems reasonable* to believe that the 160-bit q is enough to ensure the difficulty of the 1m-BDHI problems on the bilinear group G_1 of order q. Due to this reason, our schemes based on 160-bit q-order bilinear groups will be dramatically efficient than the previous analogues [25], [37], [38], which should need to be based on 1600-bit q-order bilinear groups. So we can claim that our IBBS-I and IBBS-II are the first practical ID-based blind signature schemes from pairings. In addition, note that these discussions also apply to the ID-based blind signature derived from Schnorr [32], [35] via using Galindo et al.'s generic transformation [21], as Schnorr blind signature also relies on the ROS assumption though it only need a further weaker computational assumption, i.e., discrete logarithm (DL) assumption.

ID-based blind signatures derived from Chaum [13] and Boldyreva [8] require one-more RSA (1m-RSA) and one-more CDH (1m-CDH) assumptions. Due to the above discussions, originated from [2], [5], these are two plausible assumptions and hence the corresponding IBBS schemes can guarantee security in using practical parameters. However, as shown in Table 1 they are not round-optimal and the resulting signatures are longer than ours, due to the attached certificate issued by the PKG. Similarly, the last four ID-based blind signatures in Table 2 are not very efficient in aspects of computation, round complexity, and signature size. In addition, they rely on common reference strings, though they are all provably secure in standard model. With regarding to computation-

al assumptions, CKW04 [11] requires the Strong RSA (SRSA) assumption; KZ05 [28] the Lysyanskaya-Rivest-Sahai-Wolf (LRSW) assumption [29], the Decisional Linear Diffie-Hellman (DLDH) assumption, and Decisional Composite Residuosity (DCR) assumption; Okamoto [30] the 2-variable Strong Diffie-Hellman (2SDH) assumption and DCR assumption; and Fischlin [20] the general complexity (GC) assumptions, like the existence of trapdoor permutations. So, Fischlin's scheme needs the weakest assumption but it is also the most inefficient one as general non-interactive zero-knowledge (NIZK) proofs are involved to show the correctness of blind signatures.

Here note the computational efficiency advantage of our schemes over the others holds under the condition that the gap between the BDHI problems and the 1m-BDHI problems can be neglected. Therefore, it is an interesting but technically difficult topic to formally discuss the gap between a computational problem and its one-more version, such as CDH vs one-more CDH. In fact, in [15], Cheon showed that for a *special* GDH (Gap Diffie-Hellman) group (Note that *not all* GDH groups), a greater order is needed to ensure the security of the blind signature scheme proposed in [8]. This result can be also easily extended to our scheme based on the special bilinear group. However, we can also avoid to choose this special bilinear group, if we do not want to use a greater order q.

Remark 7: We are especially grateful to one reviewer of Pairing 2008 who pointed out that one IBBS scheme from the generic construction [21], with some improvements, could also be round-optimal and more efficient than our scheme. However, we remark that such a scheme with these potential improvements is not mentioned in [21], though this scheme mentioned by the referee is very interesting and deserves further study. In addition, as stated in Section 1, both the motivation and method of our work are different from that in [21].

VIII. Other Considerations

First, the new formalized 1m-BDHI-1 and 1m-BDHI-2 assumptions may be of independent interest, since other recently proposed computation assumptions in one-more flavor, such as one-more-RSA-inversion [5], one-more CDH [8], one-more discrete logarithm [4], have found many applications in provable security for blind signatures [5], [8], transitive signatures [4], identification protocols [6] and so on.

Second, the underlying ID-based signature schemes of IBBS-I and IBBS-II may be of independent interest, since they do not use the proof of knowledge paradigm and has a loose algebraic structure. Without using the proof of knowledge paradigm enables us to avoid employing the forking lemma [32] in the security proofs and hence we can get tighter security reductions. The efficiency is also satisfactory, as we can use fixed the values of B and C in a signature so that to generate a signature only one scalar multiplication should be performed. Furthermore, the good algebraic structure of our schemes is an advantageous property and may deserve more attentions than other ID-based signature schemes. Since this property already enables the efficient extensions to blind signatures, other functionalities, such as threshold signatures and aggregate signatures, could also be constructed efficiently. We note that the underlying ID-based signature schemes are not strongly unforgeable, but satisfy the well-known standard definition of existential unforgeability. However, a non-strongly unforgeable signature may have some advantages over the strongly unforgeable one. For example, the authors of [23] constructed the first constant-length ID-based aggregate signature scheme from an non-strongly unforgeable ID-based signature scheme.

IX. Conclusions

In this paper, we proposed two secure and practical one-round identity-based blind signature (IBBS) schemes from bilinear pairings without resorting to the ROS assumption. This means that the proposed constructions are not only optimal in the sense of round complexity, but also practically efficient in contrast to existing solutions proposed in [25], [37], [38], which are actually inefficient due to the requirement of a great-order group for ensuring the difficulty of ROS problem. Compared with other identity-based blind signature schemes that can be deduced from a generic result [21], our IBBS schemes are more efficient in terms of round-complexity, computation, and signature size. Furthermore, our ID-based signature schemes avoid the restrictions which make Galindo's generic construction less "ID-based". Different from previous IBBS schemes, the proposed schemes are constructed from scratch in terms of the underlying ID-based signature schemes and the new assumptions which may be applicable for constructing other primitives in pairing-based cryptography. As the future work, several interesting topics can be further investigated: (a) Constructing efficient and secure IBBS schemes in the standard model without the ROS assumption; (b) Study the relations between computational assumptions, like BDHI-1 and BDHI-2, BDHI-1 (2) and 1m-BDHI-1 (2); and (c) Explore more applications of (1m-) BDHI-1 and (1m-) BDHI-2.

References

[1] J. Baek, Y. Zheng, Identity-based Threshold Signature Scheme From the Bilinear Pairings. In: *Proc. of IAS'04 track of ITCC'04*, pp. 124-128. IEEE Computer Society, 2004.

[2] D. Boneh, M. Franklin, Identity-based Encryption from the Weil Pairing. In: *Proc. of Advances in Cryptology - CRYPTO 2001*, LNCS 2139, pp. 213-229. Springer-Verlag, 2001.

[3] M. Bellare, C. Namprempre, G. Neven, Security Proofs for Identity-Based Identification and Signature Schemes. In: *Proc. of Advances in Cryptology - EUROCRYPT 2004*, LNCS 3027, pp. 268–286. Springer-Verlag, 2004.

[4] M.Bellare, G. Neven, Transitive Signatures Based on Factoring and RSA. In: *Proc. of Advances in Cryptology - ASIACRYPT 2002*, LNCS 2501, pp. 397-414. Springer-Verlag, 2002.

[5] M. Bellare, C.Namprempre, D. Pointcheval,M. Semanko,The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. *Journal of Cryptology*, 16(3): 185-215 (2003). Preliminary version of this paper appears in the *Proc. of FC 2001*, Springer-Verlag, 2001.

[6] M. Bellare, A. Palacio, GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attack. In: *Proc. of Advances in Cryptology - CRYPTO 2002*, LNCS 2442, pp. 162-177. Springer-Verlag, 2002.

[7] M. Bellare, 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.

[8] A. Boldyreva, Efficient Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-group Signature Scheme. In: *Proc. of PKC 2003*, LNCS 2567, pp. 31-46. Springer-Verlag, 2003.

[9] D. Boneh, B. Lynn, and H. Shacham, Short Signatures from the Weil Pairing. In: *Proc. of Advances in Cryptology - ASIACRYPT 2001*, LNCS 2248, pp. 514–532. Springer-Verlag, 2002.

[10] E. Bresson, J. Monnerat, D Vergnaud, Separation Results on the "One-More" Computational Problems. In: *Proc. of CT-RSA 2008*, LNCS 4964, pp.71-87, Springer-Verlag, 2008.

[11] J. Camenisch, M. Koprowski, B. Warinschi, Efficient Blind Signatures Without Random Oracles. In: *Proc. of Security in Communication Networks 2004*, LNCS 3352, pp. 134-148. Springer-Verlag, 2005.

[12] J. C.Cha,J. H. Cheon, An Identity-based Signature from Gap Diffie-Hellman Groups. In: *Proc. of PKC 2003*, LNCS 2567, pp. 18-30. Springer-Verlag, 2003.

[13] D. Chaum, Blind Signatures for Untraceable Payments. In: *Proc. of Advances in Cryptology - CRYPTO'82*, pp. 199-203. New York: Plenum Press, 1983.

[14] L Chen, An interpretation of identity-based cryptography, in: Foundations of Security Analysis and Design V, LNCS 4677, pp.183-208. Springer-Verlag, 2007.

[15] J. H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In: *Proc. of Eurocrypt 2006*, LNCS 4004, pp. 1-11. Springer-Verlag, 2006.

[16] S. M. Chow, Verifiable Pairing and its Applications. In: *Proc. of WISA 2004*, LNCS 3325, pp. 170-187. Springer-Verlag, 2004.

[17] Christodoulakis, D., Vaitis, M., Papadopoulos, A., Tzagarakis, M.: "The Callimachus approach to distributed hypermedia"; Proc. 10^{th} ACM Conf. Hypert., ACM, New York (Feb 1999).

[18] R. Dutta, R. Barua, P.Sarkar, Pairing-based Cryptography: a Survey. IACR preprint sever, submission 2004/064, 2004.

[19] M. Fischlin, A Note on Security Proofs in the Generic Model. In: *Proc. of Asiacrypt'00*, LNCS 1976, pp. 458-469. Springer-Verlag, 2000.

[20] M. Fischlin, Round-Optimal Composable Blind Signatures in the Common Reference String Model. In: *Proc. of Advances in Cryptology - CRYPTO 2006*, LNCS 4117, pp. 60-77. Springer-Verlag, 2006.

[21] D. Galindo, J. Herranz, E. Kiltz, On the Generic Construction of Identity-Based Signatures with Additional Properties. In: *Proc. of Advances in Cryptology - ASIACRYPT 2006*, LNCS 4284, pp. 178-193. Springer-Verlag, 2006.

[22] W. Gao, G. Wang, X. Wang, F. Li, One-Round ID-based blind signature scheme without ROS assumption, in: Proceedings of Pairing'2008. LNCS 5209, pp. 316-331. Springer-Verlag, 2008.

[23] C. Gentry, Z. Ramzan, Identity-Based Aggregate Signatures. In: *Proc. of PKC 2006*, LNCS 3958, pp. 257-273. Springer-Verlag, 2006.

[24] D. He, J. Chen, R. Zhang, An efficient identity-based blind signature scheme withoutbilinear pairings. Computers and Electrical Engineering 37, pp.444 - 450, 2011.

[25] Z. Huang., K. Chen, Y. Wang, Efficient Identity-Based Signatures and Blind Signatures. In: *Proc. of CANS 2005*, LNCS 3810, pp. 120-133. Springer-Verlag, 2005.

[26] A. Joux, A one-round protocol for tripartite diffie-hellman, in: ANTS-IV Conference, LNCS 1838, pp. 385-394. Springer-Verlag, 2000.

[27] A. Joux, The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems. In: *Proc. of Algorithm Number Theory Symposium - ANTS 2002*, LNCS 2369, pp. 20-32. Springer-Verlag, 2002.

[28] A. Kiayias, H. Zhou, Two-Round Concurrent Blind Signatures without Random Oracles. In: *Proc. of Security and Cryptography for Networks 2006*, LNCS 4116, pp. 49-62. Springer-Verlag, 2006.

[29] A. Lysyanskaya, R. Rivest, A. Sahai, and Wolf S. Pseudonym Systems. In: *Prof. of 6th Annual Int. Workshop on Selected Areas in Cryptography*, LNCS 1758, pp. 184-199.

[30] T. Okamoto, Efficient Blind and Partially Blind Signatures Without Random Oracles. In: *Proc. of 3rd Theory of Cryptography (TCC'06)*, LNCS 3876, pp. 80-99. Springer-Verlag, 2006.

[31] L. Phong, W. Ogata, New identity-based blind signature and blind decryption scheme in the standard model. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E92A(8), pp.1822-1835, 2009.

[32] D. Pointcheval, J. Stern, Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, 2000, 13(3): 361-396.

[33] W. Qiu, Converting Normal DLP-based Signatures into Blind. *Applied Mathematics and Computation*, 170(1): 657-665, 2005.

[34] A. Shamir, Identity-based Cryptosystems and Signature Schemes. In: *Proc. of Advances in Cryptology - CRYPTO'84*, LNCS 196, pp. 47-53. Springer-Verlag, 1984.

[35] C. P. Schnorr, Security of Blind Discrete Log Signatures against Interactive Attacks. In: *Proc. of ICICS 2001*, LNCS 2229, pp. 1-12. Springer-Verlag, 2001.

[36] D. Wagner, A Generalized Birthday Problem. In: *Proc. of Advances in Cryptology - CRYPTO 2002*, LNCS 2442, pp. 288-303. Springer-Verlag, 2002.

[37] F. Zhang, K. Kim, ID-based Blind Signature and Ring Signature from Pairings. In: *Proc. of Advances in Cryptology - ASIACRYPT 2002*, LNCS 2501, pp. 533-547. Springer-Verlag, 2002.

[38] F. Zhang, K. Kim, Efficient ID-based Blind Signature and Proxy Signature from Bilinear Pairings. In: *Proc. of ACISP2003*, LNCS 2727, pp. 312-323. Springer-Verlag, 2003.

Wei Gao received his Ph.D. and MS degrees in applied mathematics from Hunan University in 2006, Guangzhou University 2003 respectively. He is a lecturer in Ludong University from 2007. From 2010, he is Posdoc at Shanghai Jiaotong University. His research interests include security, cryptography and number theory.

Guilin Wang received her Ph.D degree in computer science, from Institute of Software, Chinese Academy of Sciences, P. R. China, in 2001. He is currently a senior lecturer in University of Wollongong, Australia. His research interests include cryptography and information security.

Xueli Wang received his PhD degree in mathematics from the Academy of China in 1991, his MS degree in mathematics from Shannxi Normal University in 1987. He is currently Professor of Computer Science at South China Normal University. His research interests include cryptography and elliptic curves.

Fei Li received her MS degree in applied mathematics, Guangzhou University, China, in 2008. She is currently a lecturer in Ludong University, China. Her research interests include cryptography and algebra.