Efficient Identity-Based Signatures and Blind Signatures*

Zhenjie Huang[1,2,3], Kefei Chen[1], and Yumin Wang[3]

[1] Department of Computer Science and Engineering,
Shanghai Jiaotong University, Shanghai 200030, P.R. China
zhj_huang@hotmail.com, chen-kf@cs.sjtu.edu.cn
[2] Department of Mathematics and Information Science,
Zhangzhou Normal University, Fujian, 363000, P.R. China
[3] State Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an, Shaanxi, 710071, P.R. China
ymwang@xidian.edu.cn

Abstract. In this paper, we first propose an efficient provably secure identity-based signature (IBS) scheme based on bilinear pairings, then propose an efficient identity-based blind signature (IBBS) scheme based on our IBS scheme. Assuming the intractability of the Computational Diffie-Hellman Problem, our IBS scheme is unforgeable under adaptive chosen-message and ID attack. Efficiency analyses show that our schemes can offer advantages in runtime over the schemes available. Furthermore, we show that, contrary to the authors claimed, Zhang and Kim's scheme in ACISP 2003 is one-more forgeable, if the ROS-problem is solvable.

Keywords: Identity-based, Signature, Blind signature, Bilinear pairings, Gap Diffie-Hellman group.

1 Introduction

The key generation procedure in the usual sense of public-key cryptography renders all public keys random. Consequently, it is necessary to associate a public key with the identity information of its owner. Such an association can be realized by a public-key authentication framework: a tree-like hierarchical public-key certification infrastructure (e.g., X.509 certification framework). In a certificate-based public key system, before using the public key of a user, the participants must verify the certificate of the user at first. As a consequence, this system requires a large storage and computing time to store and verify each user's public key and the corresponding certificate. In 1984 Shamir [16] introduced the concept of identity-based (simply ID-based) public key cryptosystem to simplify key management procedures in certificate-based public key setting. Since then, many ID-based encryption and signature schemes have been proposed.

* This work is supported by the National Natural Science Foundation of China under Grant No.60273049.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 120–133, 2005.

ID-based cryptosystems have a property that a user's public key can be easily calculated from his identity by a publicly available function, while his private key can be calculated for him by a trusted authority, called Key Generation Center (KGC). 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 a trusted key generation center 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.

Early, the bilinear pairings, namely Weil pairing and Tate pairing of algebraic curves, were used in cryptography for the Menezes-Okamoto-Vanstone (MOV) attack [11] (using Weil pairing) and Frey-Rück (FR) attack [7] (using Tate pairing) to reduce the discrete logarithm problem on some elliptic curves or hyperelliptic curves to the discrete logarithm problem in a finite field. Recently, the bilinear pairings have been found positive applications in cryptography to construct new ID-based cryptographic primitives. In 2000, Joux [10] used the Weil pairing to construct a tripartite one round Diffie-Hellman key agreement protocol. After Joux's breakthrough, many ID-based cryptographic schemes have been proposed using the bilinear pairings [5]. In Crypto 2001, Boneh and Franklin [2] presented an ID-based encryption scheme based on bilinear pairings which to be the first fully functioning, efficient and provably secure ID-based encryption scheme. In Asiacrypt 2001, Boneh, Lynn and Shacham [3] proposed a basic signature scheme using pairings which has the shortest length among signature schemes in classical cryptography.

There are five ID-based signature (IBS) schemes based on bilinear pairings have been proposed. Sakai, Ohgishi and Kashara proposed a first IBS Scheme using Weil pairing in 2000.Then, in 2002, Paterson proposed a new IBS scheme using bilinear pairing. But, these two schemes without any formal proof of security. In 2003, there are three provably secure IBS scheme have been proposed. Yi proposed a provably secure IBS scheme using Weil pairing in [18], Cha and Cheon [4] proposed a provably secure IBS scheme from Gap Diffie-Hellman group in PKC2003, and Hess proposed a efficient scheme [9] in SAC 2002.

Blind signature, first introduced by Chaum [6] at Crypto'82, is a variant of digital signatures, 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. Up to now, two ID-based blind signature (IBBS) schemes based on bilinear pairings have been proposed. The first scheme was proposed by Zhang and Kim [19] in Asiacrypt 2002. Later, in ACISP 2003, Zhang and Kim [20] proposed a new ID-based blind signature scheme based on bilinear pairings. They claim that the security against generic parallel attack to their new scheme doesn't depend on the difficulty of ROS-problem.

In this paper, we first propose an efficient provably secure ID-based signature scheme based on bilinear pairings, then propose an efficient ID-based blind signature scheme based on our IBS scheme. We discuss the security and efficiency of our schemes. We prove that our IBS scheme is unforgeable in the random oracle model and show that our schemes can offer advantages in runtime, communication and memory requirements over the schemes available. Furthermore, we show that, contrary to the authors claimed, Zhang and Kim's scheme in [20] is one-more forgeable under the generic parallel attack if the ROS-problem is solvable, namely the security against generic parallel attack to this scheme also depends on the difficulty of ROS-problem.

The rest of the paper is organized as follows: Section 2 gives some notions. In Section 3, we first give definitions for ID-based signature, and then propose a provably secure ID-based signature scheme with a proof of security. ID-based blind signature is discussed in Section 4. We give some definitions and propose an efficient ID-based blind signature scheme there. We conclude in Section 5.

2 Bilinear Pairings and Gap Diffie-Hellman Groups

Let G_1 be a cyclic additive group generated by P with order prime q, and G_2 be a cyclic multiplicative group with the same order q. A bilinear pairing is a map $e : G_1 \times G1 \rightarrow G_2$ with the following properties:

Bilinear: For all $P_1, P_2, Q_1, Q_2 \in G_1$,

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1),$$
$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2).$$

These two equations above imply that $e(aP, bQ) = e(P, Q)^{ab}$, for all a, b .

Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;

Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Modified Weil pairing [17] and Tate pairings [1, 8] are examples of bilinear maps.

Following are three important mathematical problems.

Discrete Logarithm Problem (DLP): Given $P, Q \in G_1$, find an integer a such that $Q = aP$, whenever such an integer exists.

Decisional Diffie-Hellman Problem (DDHP): For a, b, c, given P, aP, bP, $cP \in G_1$, decide whether $c = ab \bmod q$.

Computational Diffie-Hellman Problem (CDHP): For a, b, given P, aP, $bP \in G_1$, compute abP.

We call G a **Gap Diffie-Hellman (GDH) group** if DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial time in G.

In the following, we use the notation $a \in_R A$ to mean that a is randomly chosen from A.

3 ID-Based Signatures

3.1 Definitions

Definition 1. *(ID-Based Signature, IBS) An ID-based signature scheme consists of four algorithms,* ***Setup****,* ***Extract****,* ***Sign*** *and* ***Verify****, where*

Setup *is a probabilistic polynomial-time algorithm for the key generation center KGC, which takes a security parameter* 1^n*, and returns system parameters* SP *and master key.*

Extract *is a probabilistic polynomial-time algorithm for the KGC, which takes input security parameter* 1^n*, system parameters* SP*, master key and signer's identity ID, returns the signer's private key* S_{ID}*.*

Sign *is a probabilistic polynomial-time signature issuing algorithm, which takes input security parameter* 1^n*, system parameters* SP*, message* m*, signer* S*'s identity ID and his private key* S_{ID}*, outputs a signature* $\sigma_{m,ID}$ *on message* m*.*

Verify *is a polynomial-time algorithm that takes input security parameter* 1^n*, system parameters* SP*, signer's identity ID, message* m *and signature* $\sigma_{m,ID}$*, outputs either "Accept" or "Reject", simply* 1 *or* 0*.*

The same as the normal signature, a secure ID-based signature scheme should have two properties: completeness and unforgeability.

Definition 2. *(IBS-Completeness) If the signer* S *runs the signature issuing algorithm and outputs signature* $\sigma_{m,ID}$*, then for any constant* c*, and for sufficiently large* n*,*

$$\Pr[\mathbf{Verify}(1^n, SP, m, ID, \sigma_{m,ID}) = 1] > 1 - n^{-c}.$$

Definition 3. *(****Game A****) Let* $\mathcal{A}$ *be a probabilistic polynomial-time algorithm and let* $\mathcal{C}$ *be a challenger.*

1. $\mathcal{C}$ *runs* ***Setup*** *and sends the system parameters* SP *to* $\mathcal{A}$*.*
2. $\mathcal{A}$ *can issue the following queries as he wants:*
   (a) ***Hash function query.*** $\mathcal{C}$ *computes the value of the hash function for the requested input and sends the value to* $\mathcal{A}$*.*
   (b) ***Extract query.*** *Given an identity ID,* $\mathcal{C}$ *runs* ***Extract*** *and sends the private key corresponding to ID to* $\mathcal{A}$*.*
   (c) ***Sign query.*** *Given an identity ID and a message* m*, returns a signature* $\sigma_{m,ID}$ *to* $\mathcal{A}$*.*
3. $\mathcal{A}$ *outputs a signature* $(ID, m, \sigma_{m,ID})$*, where ID and* (ID, m) *never query to* ***Extract*** *and* ***Sign****, respectively.*

$\mathcal{A}$ *wins the Game A iff* $(ID, m, \sigma_{m,ID})$ *is a valid signatures.*

Definition 4. *(IBS-Unforgeability) An ID-based signature scheme is unforgeable if any probabilistic polynomial-time algorithm* $\mathcal{A}$ *wins Game A with a advantage* $\epsilon \leq n^{-c}$ *for any constant* c *and sufficiently large* n*.*

3.2 Provably Secure ID-Based Signature Scheme

1. **Setup.** Choose a GDH group G_1, which is a cyclic additive group generated by P with prime order q. Choose a cyclic multiplicative group G_2 with the same order q and a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. Pick a random $s \in_R \mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$, set $P_{pub} = sP$. Choose cryptographic hash functions $H_1 : \{0,1\}^* \times G_2 \rightarrow \mathbb{Z}_q^*$ and $H_2 : \{0,1\}^* \rightarrow G_1$. Publish the system parameter $SP = (G_1, G_2, e, q, P, P_{pub}, H_1, H_2)$, and keep the master key s privately.

2. **Extract.** Given an identity ID, compute $P_{ID} = H_2(ID)$ and return the corresponding private key $S_{ID} = sP_{ID}$.

3. **Sign.** The signer randomly chooses $r \in_R \mathbb{Z}_q^*$, computes

$$\begin{aligned} R &= e(P_{ID}, P_{pub})^r, \\ h &= H_1(m, R), \\ V &= (rh + 1)S_{ID}, \end{aligned}$$

and publishes the signature $\sigma_{m,ID} = (R, V)$ on message m.

(For notational purposes, in the proof of the security, signatures will be denoted by (m, ID, R, h, V).)

4. **Verify.** To verify a signature $\sigma_{m,ID} = (R, V)$ on message m for an identity ID, the verifier checks whether

$$e(V, P) = R^{H_1(m,R)} e(P_{ID}, P_{pub}).$$

3.3 Security

The completeness can easily be proved by straightforward calculating. In the following, we prove the unforgeability in the **Random Oracle Model**. The proof is done in two steps. We firstly reduce ID attacks to *given* ID attacks and then treat given ID attacks.

For the first case, we have below Lemma 1, since the **Setup** and **Extract** of our scheme is the same as that of the Cha-Cheon scheme [4].

Lemma 1. *If there is an algorithm $\mathcal{A}_0$ for an adaptively chosen message and ID attack to our scheme with running time t_0 and advantage ϵ_0, then there is an algorithm $\mathcal{A}_1$ for an adaptively chosen message and given ID attack which has running time $t_1 \leq t_0$ and advantage $\epsilon_1 \geq \epsilon_0(1 - \frac{1}{q})/q_{H_2}$, where q_{H_2} is the maximum number of queries to H_2 asked by $\mathcal{A}_0$. In addition, the numbers of queries to hash function H_2, **Extract**, and **Sign** asked by $\mathcal{A}_1$ are the same as those of $\mathcal{A}_0$.*

Lemma 2. *Let $\mathcal{A}$ be a probabilistic polynomial time algorithm and let q_{H_1} and q_S be the maximum number of queries to the random oracle H_1 and **Sign** oracle asked by $\mathcal{A}$, respectively. If $\mathcal{A}$ can produce a valid signature (m, ID, R, h, V) with probability $\epsilon \geq 10(q_S + 1)(q_S + q_{H_1})/q$, then there is another algorithm $\mathcal{B}$ can produce two valid signatures (m, ID, R, h, V) and (m, ID, R, h', V') such that $h \neq h'$ in expected time $t' \leq 120686 q_{H_1} t/\epsilon$.*

Proof. We only have to prove that the signature can be simulated with an indistinguishable distribution probability without the knowledge of the signer's private key. Once this is done, the result directly follows from Theorem 3 (The Forking Lemma) in [13].

We first gave a simulator $\mathcal{S}$: In order to sign the message m, $\mathcal{S}$ chooses $r \in_R \mathbb{Z}_q, h \in_R \mathbb{Z}_q^*$, then computes $V = rP_{pub}$ and $R = e(V,P)^{h^{-1}} e(P_{ID}, P_{pub})^{-h^{-1}}$. If $R = 1$, $\mathcal{S}$ restarts the simulation. Otherwise, it returns the triple (R, h, V).

Now we consider the following distributions:

$$\xi = \left\{ (R,h,V) \left| \begin{array}{l} r \in_R \mathbb{Z}_q^* \\ h \in_R \mathbb{Z}_q^* \\ R = e(P_{ID}, P_{pub})^r \\ V = (rh+1)S_{ID} \end{array} \right. \right\}$$

and

$$\zeta = \left\{ (R,h,V) \left| \begin{array}{l} r \in_R \mathbb{Z}_q \\ h \in_R \mathbb{Z}_q^* \\ V = rP_{pub} \\ R = e(V,P)^{h^{-1}} e(P_{ID}, P_{pub})^{-h^{-1}} \neq 1 \end{array} \right. \right\}$$

Let (T, a, U) be a valid signature, namely $T \in G_2 \setminus \{1\}, a \in \mathbb{Z}_q^*, U \in G_1$ such that $e(U,P)e(P_{ID}, P_{pub})^a = T \neq 1$, we have following probabilities of this signature appearing in above distributions:

$$\Pr_{\xi}[(R,h,V) = (T,a,U)] = \Pr_{r \neq 0, h} \left[\begin{array}{l} e(P_{ID}, P_{pub})^r = T \\ a = h \\ (rh+1)S_{ID} = U \end{array} \right] = \frac{1}{(q-1)^2}$$

$$\Pr_{\zeta}[(R,h,V) = (T,a,U)] = \Pr_{T \neq 1, h} \left[\begin{array}{l} e(V,P)^{h^{-1}} e(P_{ID}, P_{pub})^{-h^{-1}} = T \\ a = h \\ rP_{pub} = U \end{array} \right] = \frac{1}{(q-1)^2}$$

It shows that two distributions above are the same, thus the signature can be simulated by simulator $\mathcal{S}$ with an indistinguishable distribution probability without the knowledge of the signer's private key.

Theorem 1. *If there is an algorithm $\mathcal{A}$ for an adaptively chosen message and ID attack to our scheme with running time t and advantage $\epsilon \geq 10(q_S+1)(q_{H_1}+q_S)q_{H_2}/(q-1)$, then CDHP can be solved within expected time $t' \leq 120686 q_{H_1} t/\epsilon$ with probability $1-1/(q-1)$, where q_{H_1}, q_{H_2} and q_S be the maximum number of queries to the random oracle H_1, H_2 and **Sign** oracle asked by $\mathcal{A}$, respectively.*

Proof. Under the assumption of the theorem, from Lemma 1, there is an algorithm $\mathcal{A}_1$ can forge a valid signature (m, ID, R, h, V) with running time $t_1 \leq t$ and advantage $\epsilon_1 \geq \epsilon(1 - \frac{1}{q})/q_{H_2} \geq 10(q_S+1)(q_S+q_{H_1})/q$ under adaptively chosen message and given ID attack. Then from Lemma 2, there is algorithm $\mathcal{B}$ can produce two valid signatures (m, ID, R, h, V) and (m, ID, R, h', V') such that $h \neq h'$ in expected time $t' \leq 120686 q_{H_1} t/\epsilon$.

Armed with these two valid signatures (m, ID, R, h, V) and (m, ID, R, h', V'), we can solve CDHP with probability $1 - 1/(q-1)$ as follows.

We run the simulator $\mathcal{S}$ in Lemma 2 with $P_{ID} = xP, P_{pub} = yP, x, y \in_R \mathbb{Z}_q^*$. As signatures (m, ID, R, h, V) and (m, ID, R, h', V') are validly, we have

$$e(V, P) = R^h e(P_{ID}, P_{pub}) = R^h e(xyP, P),$$
$$e(V', P) = R^{h'} e(P_{ID}, P_{pub}) = R^{h'} e(xyP, P),$$

then have

$$h^{-1}(V - xyP) = h'^{-1}(V' - xyP),$$

so

$$xyP = (h^{-1}V - h'^{-1}V')/(h'^{-1} - h^{-1}),$$

when $h' \neq h$.

Since both h and h' are randomly chose from $\mathbb{Z}_q^*$, the probability of $h' = h$ is $1/(q-1)$. So, we can compute xyP from (P, xP, yP), i.e. solve CDHP, with probability $1 - 1/(q-1)$.

3.4 Efficiency

We compare our schemes to the five available ID-based signature schemes based on bilinear pairings. In the following we denote by E an exponentiation in G_2, by M a scalar multiplication in G_1, by A a addition in G_1, by SM a simultaneous scalar multiplication of the form $aP + bQ$ in G_1, and by P a computation of the pairing. The **Setup** and **Extract** stages are virtually identical for all six schemes. We do not take hash evaluations into account, since all schemes are require two hash evaluations. Five out of these six schemes (excepting the Scheme in [4]) can be optimized by precomputing some pairings, such as $e(P_{ID}, P_{pub})$ in our scheme, and using in later when it needed. So we will eliminate these pairing computation. The computation overheads of all six schemes (optimized by precomputing) are summarized in Table 1.

The pairing computation is the operation which by far takes the most running time, the simultaneous scalar multiplication and the scalar multiplication are the second and third time-consuming, respectively. The Table 1 shows that

Table 1. Comparison of Six IBS Schemes

Schemes	Sign	Verify	Security
Our Scheme	1M+1E	1P+1E	Provable
Scheme in [9]	1M+1E	1P+1E	Provable
Scheme in [4]	2M	2P+1M+1A	Provable
Scheme in [18]	1SM+1M	2P+1M+1A	Provable
Scheme in [12]	1SM+1M	1P+2E	
Scheme in [14]	2M	2P	

our schemes only require 1P+1M and are far more efficient than other schemes except [9].

We conclude that our schemes can offer advantage in runtime over other schemes except [9].

4 ID-Based Blind Signatures

4.1 Definitions

Definition 5. *(ID-Based Blind Signature, IBBS) An ID-based blind signature scheme, which involves three parties, the key generation center KGC, the signer S and the user U, consists of four algorithms,* ***Setup****,* ***Extract****,* ***Sign*** *and* ***Verify****, where*

Setup *is a probabilistic polynomial-time algorithm for the key generation center KGC, which takes a security parameter* 1^n*, and returns system parameters SP and master key.*

Extract *is a probabilistic polynomial-time algorithm for the KGC, which takes input security parameter* 1^n*, system parameters SP, master key and signer's identity ID, returns the signer's private key* S_{ID}*.*

Sign *is an interactive probabilistic polynomial-time signature issuing protocol between the signer S and the user U, in which they input security parameter* 1^n*, system parameters SP, the signer S's identity ID in common, the signer S inputs his private key* S_{ID} *and the user U inputs message m privately, respectively. They engage in the signature issuing protocol and stop in polynomial-time. When they stop, the user outputs either "False" or a signature* $\sigma_{m,ID}$ *on message m.*

Verify *is a polynomial-time algorithm that takes input security parameter* 1^n*, system parameters SP, signer's identity ID, message m and signature* $\sigma_{m,ID}$*, outputs either "Accept" or "Reject", simply* 1 *or* 0*.*

A secure ID-based blind signature scheme should have the property of blindness.

Definition 6. *(Blindness) Let* $\mathcal{S}'$ *be a probabilistic polynomial-time algorithm,* U_0 *and* U_1 *be two honest users.* U_0 *and* U_1 *engage in the signature issuing protocol with* $\mathcal{S}'$ *on messages* m_b *and* m_{1-b}*, and output signatures* σ_b *and* σ_{1-b}*, respectively, where b is randomly chosen from* $\{0,1\}$*. Sends* $(m_0, m_1, \sigma_b, \sigma_{1-b})$ *to* $\mathcal{S}'$ *and then* $\mathcal{S}'$ *outputs* $b' \in \{0,1\}$*. For all such* $\mathcal{S}'$*,* U_0 *and* U_1*, for any constant c, and for sufficiently large n,*

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

4.2 Our ID-Based Blind Signature Scheme

The **Setup**, **Extract** and **Verify** are the same as that of ID-based signature scheme above. The **Sign** is as follows. The user may chooses $P_1 \in G_1$ and computes $e(P_1, P)$ beforehand outside of the signing protocol.

Sign.

a. The signer randomly chooses $r \in_R \mathbb{Z}_q^*$, computes

$$R' = e(P_{ID}, P_{pub})^r,$$

and sends R' to the user as the commitment.

b. The user randomly chooses $t_1, t_2 \in_R \mathbb{Z}_q^*$ as blinding factors, and computes

$$\begin{aligned} R &= R'^{t_1} e(P_1, P)^{t_2}, \\ h &= H_1(m, R), \\ h' &= ht_1, \end{aligned}$$

then sends h' to the signer as the challenge.

c. The signer computes

$$V' = (rh' + 1)S_{ID},$$

then sends V' to the user as the response.

d. The user checks whether

$$e(V', P) = R'^{h'} e(P_{ID}, P_{pub}).$$

If the user accepts, he computes

$$V = V' + ht_2 P_1,$$

and publishes the signature $\sigma_{m,ID} = (R, V)$ on message m. Otherwise, outputs "False".

The protocol is shown in Fig. 1.

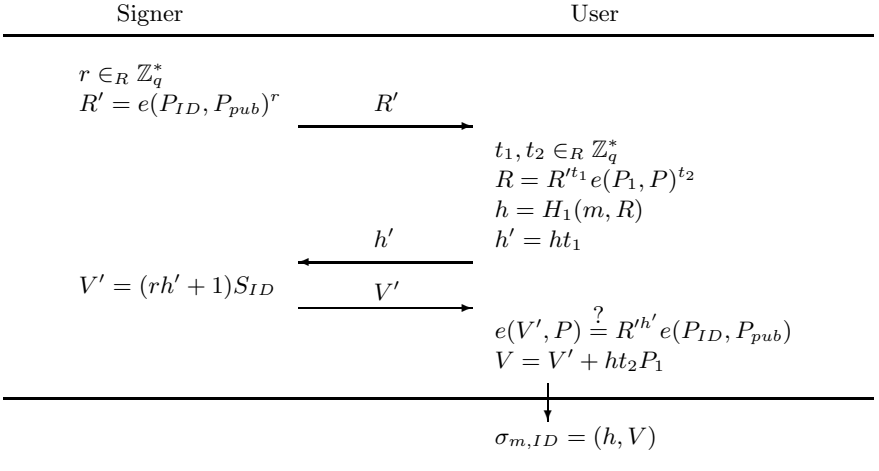

Fig. 1. ID-Based Blind Signature Scheme

4.3 Security and Efficiency

The completeness can easily be proved by straightforward calculating.

Blindness. For $i = 0, 1$, let (R'_i, h'_i, V'_i, r_i) be data appearing in the view of the signer during the execution of the signature issuing protocol with the user on message m_i, and let (m_i, R_i, h_i, V_i) be the corresponding message-signature pair. It is sufficient to show that there exists factors (t_1, t_2) that maps (R'_i, h'_i, V'_i, r_i) to (m_j, R_j, h_j, V_j) for each $i, j \in \{0, 1\}$. To this end, we define $t_1 = h'_i h_j^{-1}$, and t_2 satisfying $V_j = V'_i + h_j t_2 P_1$. Since

$$e(V'_i, P) = R_i'^{h'_i} e(P_{ID}, P_{pub}),$$
$$e(V_j, P) = R_j^{h_j} e(P_{ID}, P_{pub}),$$

we have

$$R_i'^{h'_i} = e(V'_i, P) e(P_{ID}, P_{pub})^{-1},$$
$$R_j = e(V_j, P)^{h_j^{-1}} e(P_{ID}, P_{pub})^{-h_j^{-1}}.$$

Then we see that

$$\begin{aligned} R_i'^{t_1} e(P_1, P)^{t_2} &= R_i'^{h'_i h_j^{-1}} e(P_1, P)^{t_2} \\ &= e(V'_i, P)^{h_j^{-1}} e(P_{ID}, P_{pub})^{-h_j^{-1}} e(P_1, P)^{t_2} \\ &= e(V'_i + h_j t_2 P_1, P)^{h_j^{-1}} e(P_{ID}, P_{pub})^{-h_j^{-1}} \\ &= e(V_j, P)^{h_j^{-1}} e(P_{ID}, P_{pub})^{-h_j^{-1}} \\ &= R_j \end{aligned}$$

Thus, (R'_i, h'_i, V'_i, r_i) and (m_j, R_j, h_j, V_j) have exactly the same relation defined by the signature issuing protocol. Such (t_1, t_2) always exist regardless of the values of (R'_i, h'_i, V'_i, r_i) and (m_j, R_j, h_j, V_j). Therefore, even an infinitely powerful S' outputs a correct value b' with probability exactly $1/2$, so the scheme is unconditional blind.

Unforgeability. Our blind scheme is based on the provably secure signature scheme above. The **Setup** and **Extract** stages and the signing and verification equations of our blind scheme are the same as those of the provably secure signature scheme above. If an adversary can forge a valid signature of our blind scheme, he can forge a valid signature of the scheme above too. The scheme above was proven to be unforgeable under the hardness assumption of CDHP, so we believe that our scheme is unforgeable too.

The most powerful attack on blind signature is one-more forgery introduced by Pointcheval and Stern [13]. Unfortunately, up to now, there is no ID-based blind signature scheme based on bilinear pairings can be proved secure in this model, neither our scheme nor Zhang and Kim's schemes. Finding a provably secure ID-based blind signature scheme or finding a formal proof for some available scheme remains an open problem.

In [20], the authors claim that the security against generic parallel attack to their scheme doesn't depend on the difficulty of ROS-problem. Unfortunately, in fact, the scheme in [20] is also forgeable under the generic parallel attack if the ROS-problem is solvable, namely the security against generic parallel attack to this scheme also depends on the difficulty of ROS-problem.

First we describe the ROS-problem.

ROS-Problem [15]: 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 of Eqs. (1) in the unknowns $c_1, c_2, \cdots, c_l$ over $\mathbb{Z}_q$.

$$a_{k,1}c_1 + \cdots + a_{k,l}c_l = F(a_{k,1}, \cdots, a_{k,l}) \tag{1}$$

for $k = 1, 2, \cdots, t$.

Next we describe how an adversary $\mathcal{A}$ uses the generic parallel attack to forge $l+1$ valid ID-based blind signatures of the scheme in [20], assuming the ROS-problem is solvable. Let q_{H_1} be the maximum number of queries of H_1 from adversary.

1. The signer sends commitments $R_1 = r_1 P_{ID}, R_2 = r_2 P_{ID}, \cdots, R_l = r_l P_{ID}$.
2. $\mathcal{A}$ randomly chooses $a_{k,1}, \cdots, a_{k,l} \in_R \mathbb{Z}_q$ and messages $m_1, m_2, \cdots, m_t$. He computes $U_k = \sum_{i=1}^{l} a_{k,i} R_i$ and $H_1(m_k, U_k)$ for $k = 1, 2, \cdots, t$. Here $t < q_{H_1}$.
3. $\mathcal{A}$ solves $l+1$ of t Eqs. (2) in the unknowns $c_1, c_2, \cdots, c_l$ over $\mathbb{Z}_q$.

$$H_1(m_k, U_k) = \sum_{j=1}^{l} a_{k,j} c_j \tag{2}$$

for $k = 1, 2, \cdots, t$.

4. $\mathcal{A}$ sends the solutions $c_1, c_2, \cdots, c_l$ as challenge to the signer.
5. The signer sends back $V_i = (r_i + c_i) S_{ID}$ for $i = 1, 2, \cdots, l$.
6. For each solved Eq. (2), $\mathcal{A}$ gets a valid signature (m_k, V'_k, U'_k) by setting

$$U'_k = U_k = \sum_{i=1}^{l} a_{k,i} R_i$$

$$V'_k = \sum_{i=1}^{l} a_{k,i} V_i$$

7. $\mathcal{A}$ outputs $l+1$ signatures (m_k, V'_k, U'_k) for $k = 1, 2, \cdots, l+1$. It is easy to see that the forged signatures are valid. According to Eq. (2), we have

$$\begin{aligned} e(U'_k + H_1(m_k, U'_K) P_{ID}, P_{pub}) &= e(\sum_{i=1}^{l} a_{k,i} R_i + (\sum_{i=1}^{l} a_{k,i} c_i) P_{ID}, P_{pub}) \\ &= e((\sum_{i=1}^{l} a_{k,i} r_i) P_{ID} + (\sum_{i=1}^{l} a_{k,i} c_i) P_{ID}, P_{pub}) \\ &= e(\sum_{i=1}^{l} a_{k,i} (r_i + c_i) P_{ID}, P_{pub}) \end{aligned}$$

$$= e(\sum_{i=1}^{l} a_{k,i}(r_i + c_i)S_{ID}, P)$$
$$= e(\sum_{i=1}^{l} a_{k,i}V_i, P)$$
$$= e(V'_k, P)$$

for $k = 1, 2, \cdots, l + 1$.

Efficiency. We compare our scheme to the two available ID-based blind signature schemes based on bilinear pairings. We also do not take hash evaluation and the pairing computation which can be precomputed into account.

In Zhang and Kim's schemes [19, 20], before issuing a signature, the user does not check whether the response that the signer sent is valid or not, namely the user issues a signature regardless whether the signer performs the signature issuing protocol right or not. This will damage the completeness. To avoid a dishonest signer cheating a user, like our schemes, checking the response before issuing a signature is necessary in these two schemes too. Thus, we take it into account in the following discussion.

The computation overheads of all three schemes (optimized by precomputing) are summarized in Table 2. (The number in bracket is the computation overhead for checking response).

Table 2. Comparison of Three IBBS Schemes

Schemes	Sign	Verify
Our Scheme	2M+3E+1A+(1P+1E)	1P+1E
Scheme in [19]	1P+2SM+2M+2A+(1P+1E)	1P+1E
Scheme in [20]	1SM+3M+(2P+1M+1A)	2P+1M+1A

The Table 2 shows that our scheme only require 2P+2M and is far more efficient than the schemes of [19] and [20], while the scheme in [19] requires 3P+2SM+2M and the scheme in [20] requires 4P+1SM+5M. The **Sign** stage of our scheme taking less than half the runtime of [19] and [20], and the **Verify** stage of our scheme and [19] taking less than half the runtime of [20]. The scheme in [20] is hence the slowest. We conclude that our scheme can offer advantage in runtime over the schemes [19, 20].

5 Conclusion

ID-based cryptosystem has a property that a user's public key can be easily calculated from his identity by a publicly available function, and can be hence a good alternative for certificate-based public key infrastructure. Blind signature

has the anonymity and plays a central role in applications such as electronic voting and electronic cash systems. In this paper, we first propose a efficient provably secure identity-based signature scheme based on bilinear pairings, then propose an efficient identity-based blind signature scheme based on our IBS scheme. Furthermore, we show that the scheme in [20] is also forgeable under the generic parallel attack if the ROS-problem is solvable.

Up to now, there is no ID-based blind signature scheme can be proved secure, neither our scheme nor Zhang and Kim's schemes. Finding a provably secure ID-based blind signature scheme or finding a formal proof for some available scheme remains an open problem.

References

1. P. Barreto, H. Kim, B. Lynn and M. Scott, Efficient algorithms for pairingbased cryptosystems, In: *Advances in Cryptology-Crypto 2002*, Lecture Notes in Computer Science, Vol.2442, Springer-Verlag, 2002, pp.354- 368.
2. D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, In: *Advances in Cryptology - Crypto 2001*, Lecture Notes in Computer Science, Vol.2139, Springer-Verlag, 2001, pp.213-229.
3. D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, In: *Advances in Cryptol-ogy-Asiacrypt 2001*, Lecture Notes in Computer Science, Vol.2248, Springer-Verlag, 2001, pp.514-532.
4. J. Cha, J.Cheon, An identity-based signature from gap Diffie-Hellman groups, In: *Public Key Cryp-tography - PKC 2003*, Lecture Notes in Computer Science, Vol. 2567, Springer- Verlag, 2003, pp.18-30.
5. R. Dutta, R. Barua, P. Sarkar, Pairing-based cryptography: a survey, *IACR preprint sever*, submission 2004/064, 2004.
6. D. Chaum, Blind signatures for untraceable payments, In: *Advances in Cryptology-Crypto 82*, 1983, Plenum, NY, pp.199-203.
7. G. Frey, H. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Mathematics of Computation*, 1994, 62: 865-874.
8. S. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing, In: *Algorithm Number Theory Symposium- ANTS 2002*, Lecture Notes in Computer Science, Vol.2369, Springer-Verlag, 2002, pp.324-337.
9. F. Hess, Efficient identity based signature schemes based on pairings, In: *Selected Areas in Cryptography - SAC 2002*, Lecture Notes in Computer Science, Vol.2595, Springer-Verlag, 2002, pp.310-324.
10. A. Joux, The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems, In: *Algorithm Number Theory Symposium- ANTS 2002*, Lecture Notes in Computer Science, Vol.2369, Springer-Verlag, 2002, pp.20-32.
11. A. Menezes, T. Okamoto, and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transaction on Information Theory*, 1993, 39:1639-1646.
12. K. Paterson, ID-based signatures from pairings on elliptic curves, *Electronics Letters*, 2002, 38(18):1025-1026.
13. D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, *J. of Cryptology*, 2000, 13: 361-396.

14. R. Sakai, K. Ohgishi and M. Kasahara, Cryptosystems based on pairing, In: *2000 Symposium on Cryptography and Information Security (SCIS2000)*, Okinawa, Japan, 2000, pp.26-28.
15. C. Schnorr, Security of blind discrete log signatures against interactive attacks, In: *Information and Communications Security - ICICS 2001*, Lecture Notes in Computer Science, Vol.2229, Springer-Verlag, 2001, pp. 1-12.
16. A. Shamir, Identity-base cryptosystems and signature schemes, In: *Advances in Cryptology - Crypto'84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, 1985, pp. 47-53.
17. K. Shim, Efficient ID-based authenticated key agreement protocol based on Weil pairing, *Electronics Letters*, 2003, 39(8): 653-654.
18. X. Yi, Efficient ID-based key agreement from Weil pairing, *Electronics Letters*, 2003, 39(2): 206-208.
19. F. Zhang, K. Kim, ID-based blind signature and ring signature from pairings, In: *Advances in Cryptology - Asiacrpt2002*, Lecture Notes in Computer Science, Vol.2501, Springer-Verlag, 2002, pp.533-547.
20. F. Zhang, K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, In: *Proc. of ACISP2003 (The 8th Australasian Conference on Information Security and Privacy)*, Lecture Notes in Computer Science, Vol. 2727, Springer-Verlag, 2003, pp.312-3323.