Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

Abstract. Blind signature and proxy signature are very important technologies in secure e-commerce. Identity-based (simply ID-based) public key cryptosystem can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. In this paper, we propose a new ID-based blind signature scheme and an ID-based partial delegation proxy signature scheme with warrant based on the bilinear pairings. Also we analyze their security and efficiency. We claim that our new blind signature scheme is more efficient than Zhang and Kim's scheme [27] in Asiacrypt2002.

Key words: Blind signature, Proxy signature, Bilinear pairings, ID-based cryptography.

1 Introduction

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 [24] proposed ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting. Since then, many ID-based encryption and signature schemes have been proposed. The main idea of ID-based cryptosystems is that the identity information of each user works as his/her public key, in other words, the user's public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA). ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required.

The bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for study on algebraic geometry. Their usage in cryptography goes back to Victor Miller's [18] unpublished paper in 1986, and in particular the results of Menezes-Okamoto-Vanstone [17] and Frey-Rück [7].

However, most of the initial application was to attack elliptic curve or hyperelliptic curve cryptosystems (*i.e.*, using pairings to transform the ECDLP or HCDLP into a discrete logarithm problem (DLP) in the multiplicative group of a finite field). In the last couple of years, the bilinear pairings have been found various applications in cryptography, they can be used to realize some cryptographic primitives that were previously unknown or impractical [2–4, 11, 22]. More precisely, they are basic tools for construction of ID-based cryptographic schemes, many ID-based cryptographic schemes have been proposed using them. Examples are Boneh-Franklin's ID-based encryption scheme [3], Smart's ID-based authentication key agreement protocol [25], several ID-based signatures schemes [5, 10, 20, 22, 27]. In this paper we concentrate ourselves to design ID-based blind signature and ID-based proxy signature scheme.

Blind signature firstly introduced by Chaum [6] in 1983 plays the central role in cryptographic protocols to provide the anonymity of users in e-cash or e-voting systems. Such signatures allow the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. ID-based blind signature is attractive since one's public key is simply his/her identity. The first ID-based blind signature scheme was proposed by Zhang and Kim [27] in Asiacrypt2002. Their scheme is based on the bilinear pairings, but the security against the *generic parallel attack* to their ID-based blind signature scheme depends on the difficulty of ROS-problem [23]. In Crypto2002, Wagner [26] claimed that there is subexponential time to break ROS-problem. To be resistant against this attack, the size of q may need to be at least 1,600 bits long. In this paper, we propose a new ID-based blind signature scheme from the bilinear pairings and expect that the security against *generic parallel attack* to our new scheme doesn't depend on the difficulty of ROS-problem.

The concept of proxy signature was first introduced by Mambo, Usuda, and Okamoto in 1996 [16]. A proxy signature scheme consists of three entities: original signer, proxy signer and verifier. If an original signer wants to delegate the signing capability to a proxy signer, he/she uses the original signature key to create a proxy signature key, which will then be sent to the proxy signer. The proxy signer can use the proxy signature key to sign messages on behalf of the original signer. Proxy signatures can be verified using a modified verification equation such that the verifier can be convinced that the signature is generated by the authorized proxy entity of the original signer. There are three types of delegation, full delegation, partial delegation and delegation by warrant. After Mambo *et al.*'s first scheme was announced, many proxy signature schemes have been proposed such as [13, 14, 19, 28]. In [13], S. Kim *et al.* gave a new type of delegation called partial delegation with warrant, which can be considered as the combination of partial delegation and delegation by warrant. In this paper, we will give an ID-based version of partial delegation with warrant proxy signature scheme.

The rest of the paper is organized as follows: The next section gives the definition of ID-based blind signature and proxy signature; Section 3 briefly explains the bilinear pairing and ID-based public key setting from pairings. Section

4 gives a detailed description of our ID-based blind signature scheme. In Section 5, an analysis about our ID-based blind signature scheme is presented. Section 6 and Section 7 give our ID-based partial delegation with warrant proxy signature scheme and its analysis, respectively. Section 8 concludes this paper.

2 ID-based Blind Signature and Proxy Signature

An ID-based blind signature scheme is considered be the combination of a general blind signature scheme and an ID-based one, *i.e.*, it is a blind signature, but its public key for verification is just the signer's identity. It consists of the following four algorithms, **Setup**, **Extract**, **Blind signature issuing protocol**, and **Verification**. The security of an ID-based blind signature scheme consists of two requirements: the blindness property and the non-forgeability. We say *the blind signature scheme is secure* if it satisfies these two requirements. For detailed description of the definition of ID-based blind signature, the readers can refer to [27].

The ID-based proxy signature can be viewed as the combination of a general proxy signature and an ID-based signature. It consists of four participants: a Key Generation Center (KGC) or Trust Authority (TA), an original signer, a proxy signer, verifier, and the following five algorithms, **Setup**, **Extract**, **Generation of the proxy key**, **Proxy signature generation**, and **Verification**.

Like the general proxy signature, an ID-based proxy signature scheme should satisfy the following requirements [14–16]:

- **Distinguishability:** Proxy signatures are distinguishable from normal signatures by everyone.
- **Verifiability:** From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.
- **Strong non-forgeability:** A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.
- **Strong identifiability:** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
- **Strong non-deniability:** Once a proxy signer creates a valid proxy signature of an original signer, he/she cannot repudiate the signature creation.
- **Prevention of misuse:** The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature. That is, he/she cannot sign messages that have not been authorized by the original signer.

3 ID-Based Public Key Setting with Pairing

In this section, we briefly describe the basic definition and properties of the bilinear pairing. We also present the ID-based public key setting based on pairing.

3.1 Bilinear Pairings

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

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Now we describe some mathematical problems in G_1.

- **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.
- **Decision Diffie-Hellman Problem (DDHP):** For $a, b, c \in Z_q^*$, given P, aP, bP, cP, decide whether $c \equiv ab \bmod q$.
- **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in Z_q^*$, given P, aP, bP, compute abP.

We assume through this paper that CDHP and DLP are intractable. When the DDHP is easy but the CDHP is hard on the group G, we call G a *Gap Diffie-Hellman* (*GDH*) *group*. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear parings can be derived from the Weil or Tate pairing. We can refer to [3, 5, 10] for more details.

3.2 ID-based Public Key Setting Using Pairings

In ID-based public key cryptosystem (IDPKC), everyone's public keys are predetermined by information that uniquely identifies them, such as name, social security number, email address, *etc.*, rather than an arbitrary string. This concept was first proposed by Shamir [24]. Since then, many researchers devote their effort on ID-based cryptographic schemes. How to construct ID-based schemes using Weil or Tate pairings on supersingular elliptic curves or abelian varieties recently receives much research interest [3, 5, 9, 10, 20, 22, 25].

ID-based public key setting involves a KGC and users. The basic operations consists of **Setup** and **Private Key Extraction** (simply **Extract**). When we use bilinear pairings to construct IDPKC, **Setup** and **Extract** can be implemented as follows:

Let P be a generator of G_1. Remember that G_1 is an additive group of prime order q and the bilinear pairing is given by $e : G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H_1 : \{0, 1\}^* \to Z_q$ and $H_2 : \{0, 1\}^* \to G_1$.

- **Setup:** KGC chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. The center publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s as the *master-key*, which is known only by itself.
- **Extract:** A user submits his/her identity information ID to KGC. KGC computes the user's public key as $Q_{ID} = H_2(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key.

4 New ID-Based Blind Signature Scheme

Recently, many ID-based signature schemes have been proposed using the bilinear pairings [5, 10, 20, 22]. In these ID-based signature schemes, Cha-Cheon's scheme [5] is not only efficient but exhibits the provable security relative to CDHP. In this section, we propose a new ID-based blind signature scheme, which can be regarded as the blind version of Cha-Cheon's ID-based signature scheme.

Let G_1 be a GDH group of prime order q. The bilinear pairing is given as $e : G_1 \times G_1 \to G_2$.

[**Setup:**]

KGC publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s as the *master-key*, which is known only by itself.

[**Extract:**]

Given an identity ID, which implies the public key $Q_{ID} = H_2(ID)$, the private key $S_{ID} = sQ_{ID}$.

[**Blind signature issuing protocol:**]

Suppose that m is the message to be signed. Let $a \in_R$ denote the uniform random selection. The protocol is shown in Fig. 1.

User		**Signer**
		$r \in_R Z_q^*$
	$\xleftarrow{\quad U \quad}$	Compute $U = rQ_{ID}$
$\alpha, \beta \in_R Z_q^*$,		
Compute		
$U' = \alpha U + \alpha\beta Q_{ID}$		
$h = \alpha^{-1} H_1(m, U') + \beta$	$\xrightarrow{\quad h \quad}$	
		Compute $V = (r + h)S_{ID}$
	$\xleftarrow{\quad V \quad}$	
Compute		
$V' = \alpha V$		

Fig. 1. The blind signature issuing protocol

- The signer randomly chooses a number $r \in_R Z_q^*$, computes $U = rQ_{ID}$, and sends U to the user as a commitment.
- (Blinding) The user randomly chooses $\alpha, \beta \in_R Z_q^*$ as blinding factors. He/She computes $U' = \alpha U + \alpha\beta Q_{ID}$ and $h = \alpha^{-1} H_1(m, U') + \beta$, sends h to the signer.
- (Signing) The signer sends back V, where $V = (r + h)S_{ID}$.

– (Unblinding) The user computes $V' = \alpha V$. He/She outputs $\{m, U', V'\}$.

Then (U', V') is the blind signature of the message m.

[**Verification:**]

Accept the signature if and only if

$$e(V', P) = e(U' + H_1(m, U')Q_{ID}, P_{pub}).$$

Our signature consists of two elements in G_1. In practice, the size of the element in G_1 (elliptic curve group or hyperelliptic curve Jacobians) can be reduced by a factor of 2 with compression techniques.

5 Analysis of the IDBSS

5.1 Correctness

The verification of the signature is justified by the following equations:

$$\begin{aligned}
&e(V', P) \\
&= e(\alpha V, P) \\
&= e((\alpha r + \alpha h)S_{ID}, P) \\
&= e((\alpha r + H_1(m, U') + \alpha\beta)Q_{ID}, P_{pub}) \\
&= e((\alpha r + \alpha\beta)Q_{ID} + H_1(m, U')Q_{ID}, P_{pub}) \\
&= e(U' + H_1(m, U')Q_{ID}, P_{pub})
\end{aligned}$$

5.2 Efficiency

We compare our blind signature scheme with the scheme in [27] from computation overhead and summarize the result in Table 1 (we ignore the operation of hash in all schemes). We denote *Pa* the pairing operation, *Pm* the point scalar multiplication on G_1, *Ad* the point addition on G_1, *Mu* the multiplication in Z_q, *Div* the division in Z_q and *MuG2* the multiplication in G_2. From Table 1, it is

Schemes	*Blind signature issuing*	*Verification*
Proposed scheme	$User:\ 3Pm + 1Ad + 1Mu + 1Div$ $Signer: 2Pm$	$2Pa + 1Pm + 1Ad$
The scheme in[27]	$User:\ 1Pa + 3Pm + 3Ad$ $Signer: 3Pm + 1Ad$	$2Pa + 1Pm + 1MuG2$

Table 1. Comparison of our blind scheme and the scheme in [27]

easy to see that our scheme is more efficient than the scheme in [27]. We note that the computation of the pairing is the most time-consuming. Although there has been many papers discussing the complexity of pairings and how to speed up the pairing computation [1, 8], the computation of the pairing still remains time-consuming. In the blind signature issuing protocol of our scheme, the user need not compute the pairing, but there is one pairing operation in [27] scheme.

The efficiency of the system is of paramount importance when the number of verifications is considerably large (*e.g.*, when a bank issues a large number of electronic coins and the customer wishes to verify the correctness of the coins). Our scheme is very efficient when we consider the batch verification. Assuming that $(U_1', V_1'), (U_2', V_2'), \cdots, (U_n', V_n')$ are ID-based blind signatures on messages $m_1, m_2, \cdots, m_n$ which issued by the signer with identity ID. The batch verification is then to test if the following equation holds:

$$e(\sum_{i=1}^{n} V_i', P) = e(\sum_{i=1}^{n} U_i' + (\sum_{i=1}^{n} H_1(m_i, U_i'))Q_{ID}, P_{pub}).$$

If we verify these signatures one by one, then we need $2nPa + nPm + nAd$, but at above batch verification, we only need $2Pa + 1Pm + 3(n-1)Ad$. Similar discussion can be applied to Cha-Cheon's ID-based signature scheme [5].

5.3 Security Proofs

Blindess Property. To prove the blindness we show that given a valid signature (m, U', V') and any view (U, h, V), there always exists a unique pair of blinding factors $\alpha, \beta \in Z_q^*$. Since the blinding factors $\alpha, \beta \in Z_q^*$ are chosen randomly, the blindness of the signature scheme naturally satisfy. We can find more formal definition about the blindness in [12, 27].

Given a valid signature (m, U', V') and any view (U, h, V), then the following equations must hold for $\alpha, \beta \in Z_q^*$:

$$U' = \alpha U + \alpha\beta Q_{ID} \tag{1}$$

$$h = \alpha^{-1} H_1(m, U') + \beta \pmod q \tag{2}$$

$$V' = \alpha V \tag{3}$$

It is obvious that $\alpha \in Z_q^*$ is existed uniquely from Eq (3) denoted by $log_V V'$. So we can get $\beta = h - (log_V V')^{-1} H_1(m, U')$ from Eq (2), and it is unique in Z_q. Next, we show that such α, β satisfy the first equation too. Obviously, due to the $non-degenerate$ of the bilinear pairing, we have

$$U' = \alpha U + \alpha\beta Q_{ID} \Leftrightarrow e(U', P_{pub}) = e(\alpha U + \alpha\beta Q_{ID}, P_{pub})$$

So we only need to show that such α and β satisfy

$$e(U', P_{pub}) = e(\alpha U + \alpha\beta Q_{ID}, P_{pub}).$$

Notice that (m, U', V') is a valid signature, *i.e.*,

$$e(V', P) = e(U' + H_1(m, U')Q_{ID}, P_{pub}).$$

We have

$$
\begin{aligned}
&e(\alpha U + \alpha\beta Q_{ID}, P_{pub}) \\
&= e(log_V V'U + log_V V' \cdot (h - (log_V V')^{-1} H_1(m, U'))Q_{ID}, P_{pub}) \\
&= e(log_V V' \cdot rQ_{ID} + log_V V' \cdot hQ_{ID}, P_{pub}) e(H_1(m, U')Q_{ID}, P_{pub})^{-1} \\
&= e(log_V V' \cdot (r + h)S_{ID}, P) e(V', P)^{-1} e(U', P_{pub}) \\
&= e((log_V V')V, P) e(V', P)^{-1} e(U', P_{pub}) \\
&= e(U', P_{pub})
\end{aligned}
$$

Thus the blinding factors always exist which lead to the same relation defined in the blind signature issuing protocol.

Non-forgeability. Assume that $\mathcal{A}$ is the adversary (he/she can be a user or any third party) holding the system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$ and the identity public key Q_{ID} of the signer ID. $\mathcal{A}$ tries to forge a valid message-signature of the signer.

First, we assume that $\mathcal{A}$ performs the ID attack, *i.e.*, $\mathcal{A}$ queries **Extract** q_E ($q_E > 0$) times with (PARAMS, $ID_i \neq ID$) for $i = 1, \cdots, q_E$. **Extract** returns to $\mathcal{A}$ the q_E corresponding secret key S_{ID_i}. We assume that q_E is limited by a polynomial in k. If $\mathcal{A}$ can get a $(ID'_i, S_{ID'_i})$, such that $H_1(ID'_i) = H_1(ID) = Q_{ID}$, then he/she can forge a valid blind signature of the signer ID. But since H_1 is random oracle, **Extract** generates random numbers with uniform distributions. This means that $\mathcal{A}$ learns nothing from query results.

Next we assume that $\mathcal{A}$ had interacted with the signer ID, and let (U, h, V) be the view in the blind signature issuing phase. Since $V = (r + h)S_{ID}$, and $\mathcal{A}$ knows V, h, from V to get S_{ID}, $\mathcal{A}$ must know r, but r is chosen randomly by the signer. $\mathcal{A}$ knows $U = rQ_{ID}$, but from U to get r, this is DLP in G_1. We assume that DLP in G_1 is intractable, so $\mathcal{A}$ cannot get the private information of the signer at the blind signature issuing phase.

On the other hand, the signature and the verifying equation are same as Cha-Cheon's ID-based signature scheme. For any message m, if $\mathcal{A}$ can construct U' and V', such that $e(V', P) = e(U' + H_1(m, U')Q_{ID}, P_{pub})$, then $\mathcal{A}$ can forge a valid signature of Cha-Cheon's ID-based signature scheme on the message m. Due to Cha-Cheon's proof on their ID-based signature scheme (*i.e.*, Cha-Cheon's scheme is proven to be secure against existential forgery on adaptively chosen message and ID attacks, under the hardness assumption of CDHP and the random oracle model), we claim that this attack is impossible.

The most powerful attack on blind signature is *one-more signature forgery* introduced by Pointcheval and Stern in [21]. But at the moment we believe that their method can't be applied to our scheme, since multiple key components involve their blind signature scheme, while only one single private key is engaged in our scheme. Zhang and Kim proved that the security against the *generic parallel attack* to their ID-based blind signature scheme depends on the difficulty of ROS-problem. Since the signature of our ID-based blind signature scheme consists of two elements in G_1 (the signatures of Zhang-Kim's scheme in [27] and Schnorr scheme [23] are all consisted by one element in base group and one hash value), we believe that the security against *generic parallel attack* to our scheme doesn't depend on the difficulty of ROS-problem. We remain an open problem to find a formal proof against *one-more signature forgery* on our scheme.

6 ID-Based Proxy Signature Scheme from Pairings

Proxy signatures are very useful tools when one needs to delegate his/her signing capability to other party. In this section, we present an ID-based proxy signature scheme from pairings. Our ID-based proxy signature scheme is similar to Kim *et al.*'s scheme [13] which is based on certificate-based public key setting.

[**Setup:**]
KGC publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s as the *master-key*, which is known only by itself.

[**Extract:**]
Let Alice be the original signer with identity public key Q_A and private key S_A, and Bob be the proxy signer with identity public key Q_B and private key S_B.

[**Generation of the proxy key:**]
To delegate the signing capacity to proxy signer, the original signer Alice uses Hess's ID-based signature scheme [10] to make the signed warrant m_w. There is an explicit description of the delegation relation in the warrant m_w. If the following process is finished successfully, Bob gets a proxy key S_P.

- After computing $r_A = e(P, P)^k$, where $k \in_R Z_q^*$, $c_A = H_1(m_w||r_A)$ and $U_A = c_A S_A + kP$, Alice sends (m_w, c_A, U_A) to a proxy signer Bob.
- Bob verifies the validity of the signature on m_w: Compute

  $$r_A = e(U_A, P)e(Q_A, P_{pub})^{-c_A},$$

  and accept this signature if and only if $c_A = H_1(m_w||r_A)$. If the signature is valid, Bob computes the proxy key S_P as $S_P = c_A S_B + U_A$.

Of course, we can choose others ID-based signature schemes as the basic signature scheme, such as [5] [20] or [22].

[**Proxy signature generation:**]
Bob uses Hess's ID-based signature scheme [10] (takes the signing key as S_P) and obtains a signature (c_P, U_P) for any delegated message m. Here $c_P = H_1(m||r_P)$, $U_P = c_P S_P + k_P P$, where $r_P = e(P, P)^{k_P}$, $k_P \in_R Z_q^*$. The valid proxy signature will be the tuple

$$< m, c_P, U_P, m_w, r_A > .$$

[**Verification:**]
A recipient can verify the validity of the proxy signature as follows: Compute

$$r_P = e(U_P, P)(e(Q_A + Q_B, P_{pub})^{H_1(m_w||r_A)} \cdot r_A)^{-c_P}.$$

Accept the signature if and only if $c_P = H_1(m||r_P)$.

7 Analysis of the proposed protocol

7.1 Correctness

The verification of the signature is justified by the following equations:

$$
\begin{aligned}
& e(U_P, P)(e(Q_A + Q_B, P_{pub})^{H_1(m_w||r_A)} \cdot r_A)^{-c_P} \\
&= e(U_P, P)(e(c_A \cdot (S_A + S_B), P) \cdot r_A)^{-c_P} \\
&= e(U_P, P)(e(S_P - kP, P) \cdot r_A)^{-c_P} \\
&= e(U_P, P)(e(S_P, P) \cdot e(-kP, P) \cdot r_A)^{-c_P} \\
&= e(c_P S_P + k_P P, P)e(S_P, P)^{-c_P} \\
&= e(k_P P, P) \\
&= r_P
\end{aligned}
$$

So, we have: $c_P = H_1(m||r_P)$.

7.2 Security

We will show that our ID-based proxy signature scheme satisfies all the requirements stated in Section 2.

- **Distinguishability:** This is obvious, because there is a warrant m_w in a valid proxy signature, at the same time, this warrant m_w and the public keys of the original signer and the proxy signer must occur in the verification equation of proxy signature.
- **Verifiability:** The valid proxy signature for message m will be the tuple $< m, c_P, U_P, m_w, r_A >$, and from the construction of (c_P, U_P, r_A) and the verification phase, the verifier can be convinced that the proxy signer has the original signer's signature on the warrant m_w. In general the warrant contains the identity information and the limit of the delegated signing capacity and so satisfies the verifiability.
- **Strong non-forgeability:** The third adversary who wants to forge the proxy signature of the message m' for the proxy signer Bob and the original signer Alice must have the original signer's signature on a warrant m_w, but cannot forge this signature, since the original signer Alice uses Hess's ID-based signature scheme: This signature scheme is proven to be secure against existential forgery on adaptive chosen-message attacks under the random oracle model assumption. On the other hand, the original signer cannot create a valid proxy signature. Since the proxy signature is obtained by the proxy signer using Hess's ID-based signature scheme [10] (take the signing key as the proxy key S_P), and the proxy key includes the private key S_B of the proxy signer.
- **Strong identifiability:** It contains the warrant m_w in a valid proxy signature, so anyone can determine the identity of the corresponding proxy signer from the warrant m_w.

- **Strong non-deniability:** As the identifiability, the valid proxy signature contains the warrant m_w, which must be verified in the verification phase, it cannot be modified by the proxy signer. Thus once a proxy signer creates a valid proxy signature of an original signer, he cannot repudiate the signature creation.
- **Prevention of misuse:** In our proxy signature scheme, using the warrant m_w, we had determined the limit of the delegated signing capacity in the warrant m_w, so the proxy signer cannot sign some messages that have not been authorized by the original signer.

Like the discussion in [15], our ID-based proxy signature scheme need not the secure channel for the delivery of the signed warrant. More precisely, the original signer Alice can send (m_w, c_A, U_A) to a proxy signer Bob through a public channel, in other word, any third adversary can get the original signer's signature on warrant m_w. Even this, the third adversary forges the proxy signature of the message m' for the proxy signer Bob and the original signer Alice, this is equivalent to forge a Hess's ID-based signature with some public key Q, here $e(c_A(Q_A + Q_B), P_{pub}) \cdot r_A = e(Q, P_{pub})$.

8 Conclusion

ID-based public key cryptosystem can be an alternative for certificate-based public key infrastructures. Blind signature and proxy signature are important in secure e-commerce. In this paper, we proposed a new ID-based blind signature scheme and an ID-based partial delegation proxy signature scheme with warrant. Both are based on the bilinear pairings. Also we analyze their security and efficiency. Our blind signature scheme is more efficient than Zhang and Kim's scheme in Asiacrypt2002, and the security against *generic parallel attack* doesn't depend on the difficulty of ROS-problem.

For a further work, we expect that we can find a security proof about our ID-based blind signature scheme against *one-more signature forgery.*

References

1. P.S.L.M. Barreto, H.Y. Kim, B.Lynn, and M.Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
2. A. Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman -group signature scheme*, Public Key Cryptography - PKC 2003, LNCS 2139, pp.31-46, Springer-Verlag, 2003.
3. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
4. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, In C. Boyd, editor, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

5. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Public Key Cryptography - PKC 2003, LNCS 2139, pp.18-30, Springer-Verlag, 2003.
6. D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology-Crypto 82, Plenum, NY, pp.199-203, 1983.
7. G. Frey and H.Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation, 62, pp.865-874, 1994.
8. S. D. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing*, ANTS 2002, LNCS 2369, pp.324-337, Springer-Verlag, 2002.
9. C. Gentry and A. Silverberg, *Hierarchical ID-based cryptography*, Proc. of Asiacrpt2002, LNCS 2501, pp. 548-566, Springer-Verlag, 2002.
10. F. Hess, *Efficient identity based signature schemes based on pairings*, SAC 2002, LNCS 2595, pp.310-324, Springer-Verlag, 2002.
11. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, ANTS IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000.
12. A. Juels, M. Luby and R. Ostrovsky, *Security of blind digital signatures*, Advances in Cryptology-Crypto 97, LNCS 1294, pp.150-164, Springer-Verlag, 1997.
13. S. Kim, S. Park, and D. Won, *Proxy signatures, revisited*, In Pro. of ICICS 97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.
14. B. Lee, H. Kim and K. Kim, *Secure mobile agent using strong non-designated proxy signature*, Proc. of ACISP2001, LNCS 2119, pp.474-486, Springer Verlag, 2001.
15. J.Y. Lee, J.H. Cheon and S. Kim, *An analysis of proxy signatures: Is a secure channel necessary?*, CT-RSA 2003, LNCS 2612, pp. 68-79, Springer-Verlag, 2003.
16. M. Mambo, K. Usuda, and E. Okamoto, *Proxy signature: Delegation of the power to sign messages*, In IEICE Trans. Fundamentals, Vol. E79-A, No. 9, Sep., pp. 1338-1353, 1996.
17. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transaction on Information Theory, Vol.39, pp.1639-1646, 1993.
18. V. Miller, *Short programs for functions on curves*, unpublished manuscript, 1986.
19. T. Okamoto, M. Tada and E. Okamoto, *Extended proxy signatures for smart cards*, ISW'99, LNCS 1729, Springer-Verlag, pp. 247-258, 1999.
20. K.G. Paterson, *ID-based signatures from pairings on elliptic curves*, Electron. Lett., Vol.38, No.18, pp.1025-1026, 2002.
21. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, Vol.13, No.3, pp.361-396, 2000.
22. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystems based on pairing*, SCIS 2000-C20, Jan. 2000, Okinawa, Japan.
23. C. P. Schnorr, *Security of blind discrete log signatures against interactive attacks*, ICICS 2001, LNCS 2229, pp. 1-12, Springer-Verlag, 2001.
24. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
25. N.P. Smart, *An identity based authenticated key agreement protocol based on the Weil pairing*, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.
26. D. Wagner, *A generalized birthday problem*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.288-303, Springer-Verlag, 2002.
27. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, Proc. of Asiacrpt2002, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.
28. K. Zhang, *Threshold proxy signature schemes*. 1997 Information Security Workshop, Japan, Sep., 1997, pp.191-197.