ID-Based Multi-Proxy Signature and Blind Multisignature from Bilinear Pairings

Xiaofeng Chen[1], Fangguo Zhang[2] and Kwangjo Kim[1]

[1] International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{crazymount,kkj}@icu.ac.kr
[2] School of Information Technology and Computer Science
University of Wollongong, NSW 2522 Australia
fangguo@uow.edu.au

Abstract. Multi-proxy signature allows the original signer delegate his singing power to a group of proxy signers. Blind proxy-signature allows the user to obtain a signature of a message from several signers in a way that each signer learns neither the message nor the resulting signature. Plenty of multi-proxy signature and blind multisignature schemes have been proposed under the certificate-based (CA-based) public key systems. In this paper, we firstly propose an identity-based (ID-based) multi-proxy signature scheme and an ID-based blind multisignature scheme from bilinear pairings. Since there seems no ID-based threshold signature schemes up to now, both the proposed schemes can be regarded as a special case of corresponding variants of ID-based threshold signature.

Key words: Multi-proxy signature, Blind multisignature, Bilinear pairings, ID-based cryptography.

1 Introduction

The concept of proxy signature was first introduced by Mambo, Usuda, and Okamoto in 1996 [15]. In the proxy signature scheme, an original signer is allowed to delegate his signing power to a designated person, called the proxy signer and the proxy signer is able to sign the message on behalf of the original signer. There are three types of delegation: full delegation; partial delegation and delegation by warrant. In the full delegation, the original signer just gives his signing (private) key to the proxy signer as the proxy signing key. Therefore, the signature generated between the original signer and the proxy signer are indistinguishable. In the case of partial delegation, the proxy singing key is derived from the original signer's private key by the original signer. On the other side, it is computational hard for the proxy signer to derive the private key of the original signer. However, the original signer can still forge a proxy signature

of the proxy signer. In the delegation by warrant [12], the original signer signs a warrant that certifies the legitimacy of the proxy signer.

There are several kinds of proxy signature schemes. The multi-proxy signature scheme was first proposed in [11]. In a multi-proxy signature scheme, an original signer could authorize a group of proxy member and only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. Multi-proxy signature scheme can be regard as a special case of the (t, n) threshold proxy signature scheme [20] for $t = n$.[1] A contrary concept, called proxy multi-signature is introduced by Yi *et al* in 2000 [17], where a designated proxy signer can generate the signature on behalf of a group of original signers. Recently, Hwang and Chen [10] introduced the multi-proxy multi-signature scheme. Only the cooperation of all members in the original group can authorize a proxy group; only the cooperation of all members in the proxy group can sign messages on behalf of the original group.

From the viewpoint of proxy signers, the multi-proxy signature is a special multisignature. Another concept related to multisignature is the blind multisignature, firstly proposed by Horster *et al* in 1995 [9]. Blind multisignature allows the user to obtain a signature of a message from several signers in a way that each signer learns neither the message nor the resulting signature. It is a special case of the blind (t, n) threshold signature scheme for the case of $t = n$. Blind multisignature has many applications, like shared anonymous access control or multiparty pseudonymous credentials.

Plenty of multi-proxy signature and blind multisignature schemes have been proposed under the CA-based public key systems. However, there seems no such schemes under the ID-based public key systems up to our knowledge. The concept of ID-based public key system, proposed by Shamir in 1984 [16], allows a user to use his identity as the public key. It can simplify key management procedure compared to CA-based system, so it can be an alternative for CA-based public key system in some occasions, especially when efficient key management and moderate security are required. Many ID-based schemes have been proposed after the initial work of Shamir, but most of them are impractical for low efficiency. Recently, the bilinear pairings have been found various applications in cryptography, more precisely, they can be used to construct ID-based cryptographic schemes [2–4, 8, 18].

[1] As [1] noted, a multisignature scheme is different from a (t, n) threshold signature. Firstly, the goal of a multisignature is to prove that each member of the stated subgroup signed the message and the size of the subgroup can be arbitrary, while the goal of a threshold signature is to prove that some group of efficient size signed the message and the minimal size of subgroup is known in advance. Second, a threshold signature does not reveal the identity of individual signers; furthermore, the verification of a threshold signature scheme does not depend on the current subgroup of signers. However, let the stated subgroup be the whole original group, the differences between a multisignature scheme and a (n, n) threshold signature scheme are vanished. Therefore, a multi-proxy signature can be regarded as a special case of (t, n) threshold proxy signature scheme for $t = n$.

Recently, Zhang and Kim proposed an efficient ID-based blind signature and proxy signature from bilinear pairings [19]. In this paper, we propose an ID-based multi-proxy signature scheme (IDMPS) and an ID-based blind multisignature scheme (IDBMS) from bilinear pairings. Both the schemes can be regarded as a special case of corresponding variants of ID-based threshold signature scheme.

The rest of the paper is organized as follows: Some definitions and preliminary works are given in Section 2. The proposed ID-based multi-proxy signature scheme and blind multisignature scheme from bilinear pairings are given separately in Section 3 and Section 4. Finally, conclusions are giveb in Section 5.

2 Preliminary Works

In this section, we will briefly describe the basic definition and properties of bilinear pairings and gap Diffie-Hellman group. We also present ID-based public key setting from pairings.

2.1 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. Let a, b be elements of Z_q^*. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairings is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

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

2.2 Gap Diffie-Hellman Group

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, assume that the inversion and multiplication in G_1 can be computed efficiently. We first introduce the following problems in G_1.

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

We call G_1 a Gap Diffie-Hellman Group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. Such group can be found in supersingular elliptic curve or hyperelliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [2, 7, 8].

2.3 ID-based Setting from Bilinear Pairings

The ID-based public key systems allow some public information of the user such as name, address and email *etc.*, rather than an arbitrary string to be used his public key. The private key of the user is calculated by a trusted party, called PKG and sent to the user via a secure channel.

ID-based public key setting from bilinear pairings can be implemented as follows:

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 the map $e : G_1 \times G_1 \rightarrow G_2$. Define two cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow Z_q$ and $H_2 : \{0,1\}^* \rightarrow G_1$.

- **Setup:** PKG chooses a random number $s \in Z_q^*$ and set $P_{pub} = sP$. He publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s secretly as the *master-key*.
- **Extract:** A user submits his/her identity information ID and authenticates him to PKG. PKG computes the user's private key $S_{ID} = sQ_{ID} = sH_2(ID)$ and sends it to the user via a secure channel.

3 ID-based Multi-Proxy Signature Scheme from Pairings

3.1 Properties of Proxy Signature Scheme

A proxy signature scheme consists of three entities: original signer, proxy signer group and verifier. Depending on whether the original signer can generate the same proxy signature as the proxy signers do, the proxy signature schemes can be classified proxy-unprotected (the original signer can generate the proxy signatures) and proxy-protected (the original signer can not generate the proxy signatures). In this paper, we focus on the proxy-protected proxy signatures. A strong proxy signature should have the following properties [13]:

- **Verifiability:** From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.
- **Strong identifiability:** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
- **Strong undeniability:** Once a proxy signer creates a valid proxy signature of an original signer, he cannot repudiate the signature creation.
- **Distinguishability:** Proxy signatures are distinguishable from normal signatures by everyone.
- **Prevention of misuse:** The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature. That is, he cannot sign, with the proxy key, messages that have not been authorized by the original signer.
- **Strong unforgeability:** 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.

3.2 Proposed Multi-Proxy Signature Scheme from Pairings

The proposed scheme involves four roles: the Private Key Generator (PKG), the original signer, a set of proxy signers $L = \{PS_1, PS_2, \cdots, PS_l\}$ and the verifier. It consists of the following five algorithms:

[**Setup**]
PKG publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, here G_1 is a cyclic additive group generated by P with prime order q, and G_2 is a cyclic multiplicative group of the same order q, $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing, $H_1 : \{0,1\}^* \rightarrow Z_q$ and $H_2 : \{0,1\}^* \rightarrow G_1$ are two cryptographic hash functions, $P_{pub} = sP$. PKG keeps s secretly as the *master-key*.

[**Private key extraction**]
Let Alice be the original signer with identity ID_A and private key $S_A = sQ_A = sH_2(ID_A)$, and $\{PS_i\}$ be the proxy signers with identity $\{ID_{PS_i}\}$ and private key $\{S_{PS_i} = sQ_{PS_i} = sH_2(ID_{PS_i})\}$.

[**Generation of the proxy key**]
To delegate the signing capacity to proxy signers, the original signer Alice uses Hess's ID-based signature scheme [8] to generate the signed warrant m_w[2] and each proxy signer PS_i computes his proxy key S_{P_i}.

- Alice computes $r_A = e(P,P)^k$, where $k \in_R Z_q^*$, and computes $c_A = H_1(m_w||r_A)$ and $U_A = c_A S_A + kP$. Then sends (m_w, c_A, U_A) to the proxy group L.
- Each $PS_i \in L$ verifies the validity of the signature on m_w: Computes $r_A = e(U_A, P)e(Q_A, P_{pub})^{-c_A}$, accepts this signature if and only if $c_A = H_1(m_w||r_A)$. If the signature is valid, PS_i computes the proxy key S_{P_i} as $S_{P_i} = c_A S_{PS_i} + U_A$.

[**Multi-proxy signature generation**]
Suppose the proxy group L want to sign a delegated message m on behalf of the original signer. Each proxy signer PS_i generates the partial signature and an appointed clerk C, who is one of the proxy signers, combines the partial proxy signature to generate the final multi-proxy signature.

- Each PS_i randomly selects an integer $k_{P_i} \in_R Z_q^*$, computes $r_{P_i} = e(P,P)^{k_{P_i}}$ and broadcasts r_{P_i} to the remaining $l-1$ proxy signers.
- Each PS_i computes $r_P = \prod_{i=1}^{l} r_{P_i}$ and $c_P = H_1(m||r_P)$, $U_{P_i} = c_P S_{P_i} + k_{P_i} P$. Finally the individual proxy signature of the message m is (c_P, U_{P_i}).
- Each PS_i sends U_{P_i} to the clerk C.
- The clerk C computes $r_P = \prod_{i=1}^{l} r_{P_i}$, $c_P = H_1(m||r_P)$, and verifies the individual proxy signatures:

$$c_P = H_1(m||e(U_{P_i}, P)(e(Q_A + Q_{PS_i}, P_{pub})^{H_1(m_w||r_A)} \cdot r_A)^{-c_P})$$

[2] There is an explicit description of the delegation relation, such as the identity information of original signer and proxy group member and the limit of the delegated signing capacity *etc.*, in the warrant m_w.

Once all individual proxy signatures are correct, C computes $U_P = \sum_{i=1}^{l} U_{P_i}$. The valid multi-proxy signature is the tuple: $< m, c_P, U_P, m_w, r_A >$.

[**Verification**]
A verifier computes

$$r_P = e(U_P, P)(e(\sum_{i=1}^{l}(Q_A + Q_{PS_i}), P_{pub})^{H_1(m_w||r_A)} \cdot r_A^l)^{-c_P}$$

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

3.3 Analysis of the Proposed IDMPS Scheme

- **Correctness and Verifiability**: The verification of the signature is justified by the following equations:

$$\begin{aligned}
& e(U_P, P)(e(\sum_{i=1}^{l}(Q_A + Q_{PS_i}), P_{pub})^{H_1(m_w||r_A)} \cdot r_A^l)^{-c_P} \\
&= e(\sum_{i=1}^{l} U_{P_i}, P)(e(\sum_{i=1}^{l}(S_A + S_{PS_i}), P)^{c_A} \cdot r_A^l)^{-c_P} \\
&= e(\sum_{i=1}^{l} U_{P_i}, P)(e(\sum_{i=1}^{l}(S_{P_i} - kP), P) \cdot r_A^l)^{-c_P} \\
&= e(\sum_{i=1}^{l}(c_P S_{P_i} + k_{P_i} P), P)(e(\sum_{i=1}^{l} S_{P_i}, P))^{-c_P} \\
&= e(\sum_{i=1}^{l} k_{P_i} P, P) \\
&= \prod_{i=1}^{l} r_{P_i} = r_P
\end{aligned}$$

  So, we have $c_P = H_1(m||r_P)$.
- **Strong identifiability**: Because identity pubic key Q_{PS_i} of all proxy signers are involved in the verification of the proxy signature, anyone can identity all the proxy signers.
- **Strong undeniability**: The clerk verifies the individual proxy signature of each proxy signer, so no one can be deniable of his signature.
- **Distinguishability**: It is trivial.
- **Prevention of misuse**: Due to using the warrant m_w, the proxy signers can only sign messages that have been authorized by the original signer.
- **Strong unforgeability**: As [9] discussed, there are mainly three kinds of attacks: *outsiders*, who are not participating the issue of the proxy signature; some *signers* who play an active in the signing protocol and the *user* (signature owner). Furthermore, some of these attackers might collude.

The outsider-attack consists of the original signer attack and any third adversary attack. We assume that the third adversary can get the original signer's signature on warrant m_w (So, our scheme need not the secure channel for the delivery of the signed warrant). Even this, he forges the multi-proxy signature of the message m' for the proxy group L and the original signer Alice, this is equivalent to forge a Hess's ID-based signature with some public key Q, here $e(\sum_{i=1}^{l} c_A(Q_A + Q_{PS_i}), P_{pub}) \cdot r_A^l = e(Q, P_{pub})$. On the other hand, the original signer cannot create a valid multi-proxy signature since each proxy key includes the private key S_{P_i} of each proxy signer.
In our scheme, the clerk is one of the proxy signers, but he has more power than other proxy signers. Assume that the clerk wants the proxy group to sign the false message m'. He can change his r_{P_i}, therefor r_P can be changed, but from the security of the basic ID-based signature scheme and public one-way hash function H_1, it is impossible for the clerk to get c'_P and U'_P such that $< m', c'_P, U'_P, m_w, r_A >$ is a valid multi-proxy signature. Also, the attack of some signers collude can be prevented for the identity of each proxy signer is involved in the verification of the signature.
Finally, the user can not forge the multi-proxy signature because he can not obtain more information than the clerk.

4 ID-Based Blind Multisignature Scheme from Pairings

4.1 Properties of Blind Multisignature Scheme

A blind multisignature scheme allows a user obtains a digital signature from a group of signers such that each signer of the group can not know a relationship between the blinded and the unblinded message and signature parameters, which can be regarded as an extended version of blind signature [5] with a group of signers.[3] Therefore, blind multisignature should have the following properties:

- **Verifiability:** Everyone can verify the validity of the signature and be convinced that each member of the designated group participated in the signature generation.
- **Strong undeniability:** Each signer cannot repudiate his signature generation.
- **Dishonest signers identification**: The dishonest signers who try to generate an invalid partial signature will be identified by the user.
- **Strong blindness**: Each signer of the group can not know a relationship between the blinded and the unblinded message and signature parameters.

[3] Note that blind multisignature is different from group blind signature [14], which combines the notations of both group signature [6] and blind signature. In the blind multisignature, all the members of the group are involved in the signature issuing protocol. While in the group blind signature, any member of the group can sign the message on behalf of the whole group and the signature also satisfies all the properties of group signature.

– **Strong unforgeability:** Only cooperation of all signers can generate a valid blind multisignature for the designated message. Other third parties or some (not all) signers can not forge a valid blind multisignature.

4.2 Proposed Blind Multisignature Scheme from Pairings

Let G_1 be a gap Diffie-Hellman group of prime order q. G_2 be a multiplicative group of the same order q. The bilinear pairing is given as $e : G_1 \times G_1 \rightarrow G_2$. Suppose there are n signers with identity ID_i in our scheme, where $i = 1, 2, \cdots, n$.

[**Setup**]
PKG publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keep s secretly as the *master-key*.

[**Extract**]
Given an identity ID_i and let $Q_{ID_i} = H_2(ID_i)$, PKG returns the private key $S_{ID_i} = sQ_{ID_i}$.

[**Blind multisignature issuing protocol**]
Suppose that m is the message to be signed. Let $\in_R$ denotes the uniform random selection. The signature issuing protocol is shown in Fig. 1.

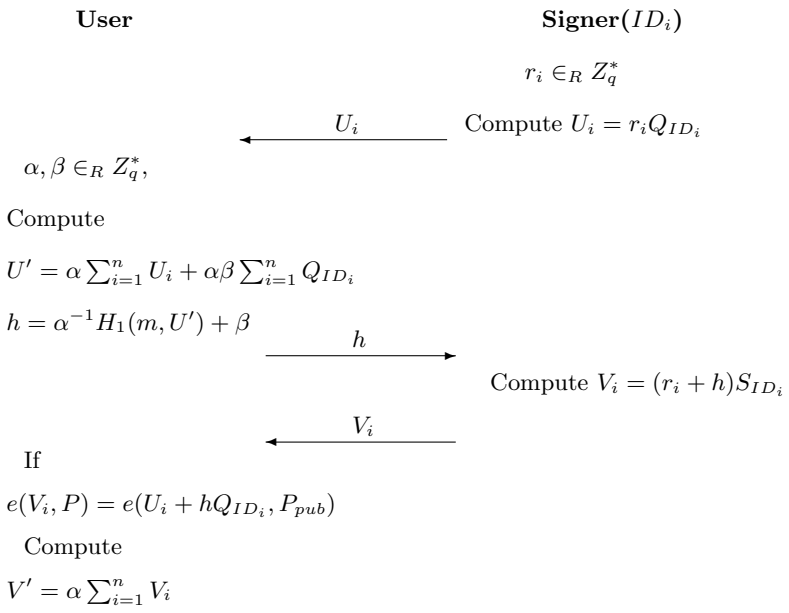

Fig. 1. The blind multisignature issuing protocol

- Each signer randomly chooses a number $r_i \in Z_q^*$, computes $U_i = r_i Q_{ID_i}$, and sends U_i to the user as a commitment.
- (Blinding) After the user received all U_i, he randomly chooses $\alpha, \beta \in Z_q^*$ as the blinding factors. He computes $U' = \alpha \sum_{i=1}^{n} U_i + \alpha\beta \sum_{i=1}^{n} Q_{ID_i}$ and $h = \alpha^{-1} H_1(m, U') + \beta$, then sends h to the signer.
- (Signing) Each signer sends $V_i = (r_i + h) S_{ID_i}$ to the user.
- (Unblinding) The user computes $V' = \alpha \sum_{i=1}^{n} V_i$ and outputs $\{m, U', V'\}$.

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

[**Verification:**]
Accept the signature if and only if

$$e(V', P) = e(U' + H_1(m, U') \sum_{i=1}^{n} Q_{ID_i}, P_{pub}).$$

4.3 Analysis of the Proposed IDBMS Scheme

- **Correctness and Verifiability:** The verification of the signature is justified by the following equations:

$$\begin{aligned} & e(V', P) \\ = & e(\alpha \sum_{i=1}^{n} (r_i + h) Q_{ID_i}, P_{pub}) \\ = & e(\alpha \sum_{i=1}^{n} (r_i + \alpha^{-1} H_1(m, U') + \beta) Q_{ID_i}, P_{pub}) \\ = & e(U' + H_1(m, U') \sum_{i=1}^{n} Q_{ID_i}, P_{pub}) \end{aligned}$$

- **Strong undeniability:** It is trivial.
- **Dishonest signer identification**: The user can identify the dishonest signer by checking whether the equation $e(V_i, P) = e(U_i + h Q_{ID_i}, P_{pub})$ holds or not.
- **Strong blindness**: We consider the following game:
  Let adversary $\mathcal{A}$ be a probabilistic polynomial-time algorithm which controls the signer. Let m_0, m_1 be two message, select $b \in_R \{0, 1\}$, which is kept secret from A. Denote m_b and m_{b-1} to M_0 and M_1 with read-only private tape respectively. $\mathcal{A}$ engages in the signature issuing protocol with M_0 and M_1 in arbitrary order. Let the output is $\sigma(m_b)$ and $\sigma(m_{b-1})$, if the signatures are both valid, $\mathcal{A}$ output $b' \in_R \{0, 1\}$; else, terminated the protocol. We say $\mathcal{A}$ wins the game if $b = b'$. Now we prove that the probability of $\mathcal{A}$ wins is $1/2$. For $j = 0, 1$, let $U_{i,j}, h_j, V_{i,j}$ be the data exchanged during the issuing protocol and U_0', V_0', U_1', V_1' are given to $\mathcal{A}$, where $i = 1, 2, \cdots, n$. It is easy to see that there always exist two randomly chosen factors α, β that map

$U_{i,j}, h_j, V_{i,j}$ to U'_j, V'_j for each $j, l \in \{0,1\}$. We define $\alpha = log_{\sum_i V_{i,j}} V'_j$, $\beta = h_j - \alpha^{-1} H_1(m_{b+j \mod 2}, U'_j)$. Furthermore, we check whether

$$U'_j = \alpha \sum_{i=1}^{n} U_{i,j} + \alpha\beta \sum_{i=1}^{n} Q_{ID_i}$$

Due to non-degenerate of the bilinear pairings, it is equivalent to

$$e(U'_j, P_{pub}) = e(\alpha \sum_{i=1}^{n} U_{i,j} + \alpha\beta \sum_{i=1}^{n} Q_{ID_i}, P_{pub})$$

For U'_j, V'_j is the valid signature for message $m_{b+j \mod 2}$, we have

$$e(V'_j, P) = e(U'_j + H_1(m_{b+j \mod 2}, U'_j) \sum_{i=1}^{n} Q_{ID_i}, P_{pub})$$

With $\alpha = log_{\sum_i V_{i,j}} V'_j$, $\beta = h_j - \alpha^{-1} H_1(m_{b+j \mod 2}, U'_j)$, we can easily verify that

$$e(U'_j, P_{pub}) = e(\alpha \sum_{i=1}^{n} U_{i,j} + \alpha\beta \sum_{i=1}^{n} Q_{ID_i}, P_{pub})$$

Therefore, the blinding factors always exists which lead to the same relation defined in the blind signature issuing protocol. Even an infinitely powerful $\mathcal{A}$ succeeds to determine b with probability 1/2.

– **Strong unforgeability:** We still consider three kinds of attacks: *outsiders*, who are not participating the issue of the blind signature; some *signers* who play an active in the signing protocol and the *user* (signature owner).
Firstly, the possibility of outsiders to forge a signature relies on the security of the underlying signature scheme. Therefore, we know that an outside adversary can not forge a blind signature of any signer for a message m', otherwise he can forge a Cha-Cheon's ID-based signature for some public key. However, Cha-Cheon's ID-based signature is proved to be secure against on existential adaptively chosen message and ID attack under the random oracle model. Another possibility is replay attack: he eavesdrops U_i and V_i from a certain signer and uses it for generating a new signature. He then sends U_i to the user as the new parameter U'_i. As he can not compute the corresponding V'_i, he just sends V_i as the responding value. This is correct only for $h = h'$. Therefore, this attack is not successful.
Secondly, as [9] mentioned, the attack of some signers collude can be prevented by adding the identity of the signers to the signed message. So, it is trivial that the proposed ID-based scheme can prevent this attack.
Finally, the user may reveal individual signature but this will not endanger the security of the scheme. The owner must compute the blind multisignature correctly from all individual signatures, otherwise, any verifier will discover this attack.

5 Conclusions

Multi-proxy signature and blind multisignature have plenty of applications, however, previous schemes are proposed under the traditional CA-based pubic key infrastructure. In this paper, we propose an ID-based multi-proxy signature scheme and blind multisignature scheme from bilinear pairings. Since there seems no ID-based threshold signature schemes up to now, both the proposed schemes can be regarded as a special case of corresponding variants of ID-based threshold signature.

References

1. A. Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme*, Public Key Cryptography 03, LNCS 2567, pp.31–46, Springer-Verlag, 2003.
2. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 01, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
3. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology-Asiacrypt 01, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
4. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Public Key Cryptography 03, LNCS 2139, pp.18-30, Springer-Verlag, 2003.
5. D. Chaum, *Blind signature for untraceable payments*, Advances in Cryptology-Eurocrypt 82, Plenum Press, pp.199-203, 1982.
6. D. Chaum and E.van Heijst, *Group Signatures*, Advances in Cryptology-Eurocrypt 91, LNCS 547, Springer-Verlag, pp.257-265, 1991.
7. S. D. Galbraith, K. Harrison and D. Soldera, *Implementing the Tate pairings*, ANTS 02, LNCS 2369, pp.324-337, Springer-Verlag, 2002.
8. F. Hess, *Efficient identity based signature schemes based on pairings*, SAC 02, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.
9. P. Horster, M. Michels and H. Petersen, *Blind multisignature schemes and their relevance for electronic voting*, Proc. of 11th Annual Computer Security Applications Conference, New Orleans, pp. 149-155, IEEE Press, 1995.
10. J. Hwang, and C.H. Chen, *A New multi-proxy multi-signature scheme*, 2001 National Computer Symposium: Information Security, Taiwan, pp. F019-F026, 2001.
11. J. Hwang, and C.H. Shi, *A simple multi-proxy signature scheme*, Communications of the CCISA, Vol. 8, No. 1, pp. 88-92, 2001.
12. S. Kim, S. Park and D. Won, *Proxy signatures, revisited*, ICICS 97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.
13. B. Lee, H. Kim and K. Kim, *Secure mobile agent using strong non-designated proxy signature*, ACISP 01, LNCS 2119, Springer- Verlag, pp.474-486, 2001.
14. A.Lysyanskays and Z.Ramzan, *Group blind signatures: A scalable solution to electroniccash*, Financial Cryptography 98, LNCS 1465, Springer-Verlag, pp.184-197, 1998.
15. 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, pp. 1338-1353, 1996.
16. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.

17. L. Yi, G. Bai and G. Xiao, *Proxy multi-signature scheme: A new type of proxy signature scheme*, Electronic Letters, Vol.36, No.6, pp.527-528, 2000.
18. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, Advances in Cryptology-Asiacrypt 02, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.
19. F. Zhang and K. Kim, *Efficient ID-based blind signature and proxy signature from bilinear pairings*, ACISP 03, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.
20. K. Zhang, *threshold proxy signature schemes*, 1997 Information Security Workshop, Japan, pp.191-197, 1997.