A New ID-based Group Signature Scheme 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. We argue that traditional ID-based systems from pairings seem unsuitable for designing group signature schemes due to the problem of key escrow. In this paper we propose new ID-based public key systems without trusted PKG (Private Key Generator) from bilinear pairings. In our new ID-based systems, if the dishonest PKG impersonates an honest user to communicate with others, the user can provide a proof of treachery of the PKG afterwards, which is similar to CA-based systems. Therefore, our systems reach the Girault's trusted level 3. Furthermore, we propose a group signature scheme under the new systems, the security and performance of which rely on the new systems. The size of the group public key and the length of the signature are independent on the numbers of the group.

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

1 Introduction

Group signature, introduced by Chaum and van Heijst [12], allows any member of a group to sign on behalf of the group. Anyone can verify the signature with a group public key while no one can know the identity of the signer except the Group Manager. Further, it is computational hard to decide whether two different signatures were issued by the same member. Plenty of group signature schemes [2, 8, 13, 14, 23] have been presented after the Chaum and van Heijst's initial works. However, most of them are much inefficient for large groups because the group public key and the length of the signature depend on the size of the group. Also, new member addition and revocation require re-issuing all members' keys and changing the group public key. Camenisch [9] presented the first efficient group signature schemes for large groups in which the group public key and the length of signature are both of constant size. The state of the art is the provably coalition-resistant secure scheme proposed by Ateniese *et al* [1].

ID-based group signature scheme is firstly proposed by Park, Kim and Won [22]. The scheme is much inefficient: the length of the group public key and signature are proportional to the size of the group; more precisely, the identity of each member must be included in the group public key. Furthermore, Mao and Lim [21] showed that the anonymity of the scheme was not guaranteed. Tseng and Jan [28] presented a novel ID-based group scheme. However, it is universally forgeable [18] and not coalition-resistant [17].

Recently, the bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, have initiated some completely new fields in cryptography, making it possible to realize cryptographic primitives that were previously unknown or impractical [6, 7]. More precisely, they are important tools for construction of ID-based cryptographic schemes. Plenty of ID-based cryptographic schemes from bilinear pairings have been proposed in last two years [4, 6, 16, 25, 29].

However, It is still an open problem to design an ID-based group signature scheme from bilinear pairings. The reasons are as follows: Firstly, the problem of key escrow is a fatal disadvantage for ID-based systems, *i.e.*, the trusted third party, called PKG, knows the private key of each member. Therefore dishonest PKG can forge the signature of any member. Secondly, the public key ID of a user should not reveal his/her real identity information otherwise anonymity of the group signature scheme is not guaranteed. However, if we use an arbitrary string as the public key [10],[1] an inherent problem is that PKG can *misattribute* a valid group signature to frame an honest member. Similarly, a member can deny his signature because PKG can also generate a public key and computes the corresponding private key. No one knows who indeed generates the certain public key since it does not reveal any information of the identity. For example, given a public key "h80fef6je59", who can provide a proof that the public key is generated by PKG or the members? So, It seems that the traditional ID-based systems from bilinear pairings are unsuitable for designing ID-based group signature.

In this paper we firstly propose new ID-based systems from pairings to solve the key-escrow problem. Contrasting with previous schemes, we assume that there is only one PKG in our systems and the PKG is not a trusted party anymore. In our systems, if the dishonest PKG impersonation an honest user to sign a document, the user can provide a proof that the PKG is dishonest, which is similar to CA-based systems. We then propose a group signature scheme from bilinear pairings under the new ID-based systems.

[1] Recently, Castelluccia [10] described how to convert any ID-based signature scheme into a group signature scheme. In his scheme, ID of the user is the public key of a RSA key pair generated by the user himself. The group signature can not forge the user's signature because because he does not know the secret key of the key pair. However, the group manager can misattibute a valid group signature to frame any user because for no one can judge who, the group manager or the user, generated the certain key pair.

The rest of the paper is organized as follows: The formal model of a secure group signature scheme is presented in Section 2. Some preliminary works are given in Section 3. Our new ID-based systems from bilinear pairings are given in Section 4. In Section 5, we propose a new ID-based group signature scheme under the new systems. The security and efficiency analysis of our scheme are given in section 6. Finally, concluding remarks will be made in Section 7.

2 Group Signature

In this section we introduce the definition and security properties of group signatures.

Definition 1. *A group signature scheme is a digital signature scheme consisted of the following four procedures:*

- **Setup:** On input a security k, the probabilistic algorithm outputs the initial group public key $\mathcal{Y}$ and the secret key $\mathcal{S}$ of the group manager.
- **Join:** A protocol between the group manager and a user that results in the user becoming a new group member. The user's output is a membership certificate and a membership secret.
- **Sign:** A probabilistic algorithm that on input a group public key, a membership certificate, a membership secret and a message m. Outputs is the group signature Sig of m.
- **Verify:** An algorithm takes as input the group public key $mathcalY$, the signature Sig, the message m to output 1 or 0.
- **Open:** The deterministic algorithm takes as input the message m, the signature Sig, the group manager's secret key $\mathcal{S}$ to return "Identity" or "failure".

A secure group signature must satisfy the following properties:

- *Correctness*: Signatures produced by a group member using **Sign** must be accepted by **Verify**.
- *Unforgeability*: Only the group members can sign messages on behalf of the group.
- *Anonymity*: Given a valid signature, it is computationally hard to identify the signer for anyone except the group manager.
- *Unlinkability*: Deciding whether two different valid signatures were computed by the same group member is computationally hard for anyone except the group manager.
- *Traceability*: The group manager is always able to open a valid signature and identify the signer.
- *Exculpability*: Neither the group manager nor a group member can sign messages on behalf of other group members. Also, the group manager or colludes with some group members can not misattribute a valid group signature to frame a certain member, *i.e.*, the member should responsible for a valid signature that he did not produce.

- *Coalition-resistance*: A colluding subset of group members (even if comprised of the whole group) cannot produce a valid signature that the group manager cannot open.
- *Efficiency*: The efficiency of group signature is based on the parameters: the size of the group public key, the length of the group signatures and the efficiency of the algorithms and protocols of the group signatures.

3 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.

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. 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 $P, Q \in G_1$.

3.2 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 [6, 11, 16].

3.3 ID-based Public Key Setting from Bilinear Pairings

The ID-based public key systems, introduced by Shamir [24], 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 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 a 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 $P_{pub} = sP$. The center publishes systems parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keep s as the *master-key*, which is known only himself.
- **Extract:** A user submits his/her identity information ID to PKG. PKG 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 Systems without Trusted PKG

Key escrow is a fatal drawback for traditional ID-based systems. So it is assumed that PKG must be trusted unconditionally. Otherwise, the systems will be soon collapsed. However, it will be difficult to find a trusted party in the *adhoc* network. If PKG acts as the group manager of a group, he can forge the signature of any users. Therefore, the most important thing to design an ID-based group signature is to solve the problem of key escrow.

In this section, we present new ID-based systems to solve key escrow problem from bilinear pairings.[2] In our systems, PKG is assumed no longer to be a trusted party and trust cannot be built by multiple PKGs.

Let G_1 be a Gap Diffie-Hellman group of prime order q, G_2 be a cyclic multiplicative group of the same order q. A bilinear pairings is a map $e : G_1 \times G_1 \rightarrow G_2$. Define two cryptographic hash functions $H_1 : \{0,1\}^* \times G_1 \rightarrow Z_q$ and $H_2 : \{0,1\}^* \times G_1 \rightarrow G_1$.

4.1 New ID-based Public Key Setting from Bilinear Pairings

[**Setup**]

PKG chooses a random $s \in Z_q^*$ and sets $P_{pub} = sP$. The public parameters of the systems are $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$. PKG keeps s secretly

[2] In this paper, we will not present the key agreement protocol and encryption scheme for our aim is to design an ID-based group signature scheme.

as the *master-key*.

[**Extract**]

A user submits his (or her) identity information ID and authenticates himself (or herself) to PKG. The user then randomly chooses an integer $r \in Z_q^*$ as his long-term private key and sends rP to PKG. PKG computes $S_{ID} = sQ_{ID} = sH_2(ID||T, rP)$ and sends it to the user via a secure channel, here T is the life span of r. The user's private key pair are S_{ID} and r and the public key is ID.

The user should update his key pair after period of T. For simplicity, we do not discuss this problem here.

4.2 New ID-based Signature Scheme from Bilinear Pairings

Recently, Cha and Cheon [11] proposed an ID-based signature scheme from pairings under the trusted PKG. The scheme is not only efficient but also provable secure relative to CDHP. In this paper, we propose a new ID-based signature scheme from pairings without trusted PKG. Our scheme can be regarded as the extended version of Cha and Cheon's signature scheme.

The public key setting is the same as before. Suppose that the message to be signed is m.

[**Signing Protocol**]

- Suppose the signer's public key is ID. He randomly chooses an integer $a \in Z_q^*$ and computes $U = aQ_{ID}$.
- The signer computes $V = rH_2(m, U)$.
- The signer computes $h = H_1(m, U + V)$.
- The signer computes $W = (a + h)sQ_{ID}$.

Then (U, V, W, T, rP) is the signature of the message of m.

[**Verification**]

The verifier firstly computes $Q = H_2(ID||T, rP)$, $H_2(m, U)$ and $h = H_1(m, U+V)$. He then accepts the signature if the following equations hold:

$$e(W, P) = e(U + hQ, P_{pub})$$
$$e(V, P) = e(H_2(m, U), rP)$$

We argue that an identity ID corresponds a unique rP for a period T. Therefore, the signer firstly proved that identity ID indeed corresponds to rP, which is ensured by the PKG's *master-key* s. Then the signer proved that he knows r without revealing any information of r.

[**Tracing protocol**]

Consider the following impersonation attack by the dishonest PKG:

Suppose PKG (or colludes with a dishonest user) wants to impersonate an honest user whose identity information is ID. He (or they) can do as follows:

- PKG randomly chooses an integer $r' \in Z_q^*$ and let $Q_{ID'} = H_2(ID||T, r'P)$.
- He then performs the above signing protocol for the message m.
- Output $(U', V', W', r'P)$.

Because $e(W', P) = e(U' + hQ'_{ID}, P_{pub})$, $e(V', P) = e(H_2(m, U'), r'P)$ and $Q_{ID'} = H_2(ID||T, r'P)$, PKG forged a "valid" signature of the honest user.

However, the user can provide a proof to convince that the signature is forged by PKG, which is similar to CA-based systems.[3] He firstly sends rP to the arbiter, and then provides a "knowledge proof" that he knows $S_{ID} = sH_2(ID||T, rP)$: the arbiter randomly chooses a secret integer $a \in Z_q$ and sends aP to the user; the user then computes $e(S_{ID}, aP)$. If the equation $e(S_{ID}, aP) = e(H_2(ID||T, rP), P_{pub})^a$ holds, *i.e.*, identity ID corresponds to rP and $r'P$ for a same period T, the arbiter deduces PKG dishonest because the *master-key s* is only known to PKG.

Theorem 1. *Our signature scheme is secure against on existential adaptively chosen message and ID attacks under the assumption of CDHP is hard in G_1 and random oracle model..*

Proof. In our systems, the partial signature V is the "real" signature of the user for the message. W can be regarded as a certificate issued by PKG which proves that rP correspondences to ID for a certain period T. We consider the following two cases:

Case 1: Forgery of the Partial Signature

Since PKG is not a trusted party, we consider that an adversary can collude with PKG. For a randomly chosen target user whose identity is ID, the adversary can know the target user's long-term public key rP and secret key S_{ID} from PKG. So, if he can compute V for a message m, he can successfully forge a signature of the user's for the message m. We consider the following game:

Suppose the adversary can query to H_2 adaptively at most k times. Suppose the i-th input of query is (m_i, U) and he gets the corresponding signature V_i, here $1 \leq i \leq k$. Finally, he outputs a new pair (m, V). We say that the adversary wins the game if rP is not queried and $e(V, P) = e(H_2(m, U), rP)$.

If there exists an algorithm $\mathcal{A}_0$ for an adaptively chosen message attack to our scheme with a non-negligible probability, we can construct an algorithm $\mathcal{A}_1$ as follows:

[3] In the CA-based systems, CA also can forge a user's certificate and impersonate the user to communicate with others. However, the user can accuse the dishonest CA because there exist his two different "valid" certificates issued by the same CA. Therefore, CA-based systems reach Girault's trusted level 3.

- choose an integer $u \in \{1, 2, \cdots, k\}$. Define $\mathbf{Sign}(H_2(m_i, U)) = V_i$.
- For $i = 1, 2, \cdots, k$, $\mathcal{A}_1$ responds to $\mathcal{A}_0$'s queries to H_2 and **Sign**, while for $i = u$, $\mathcal{A}_1$ replaces m_u with m.
- $\mathcal{A}_0$ outputs (m_{out}, V_{out}).
- If $m_{out} = m$ and the signature V is valid, $\mathcal{A}_1$ outputs (m, U, V). Otherwise, out *Fail*.

Note that u is randomly chosen, $\mathcal{A}_0$ knows nothing from the queries result. Also, since H_2 is a random oracle, the probability that the output of $\mathcal{A}_0$ is valid without query of $H_2(m, U)$ is negligible. Let $H_2(m, U) = bP$, we obtain $V = rbP$ from P, rP and bP, *i.e.*, we solved CDHP in G_1.

Actually, V can be regarded as the short signature of the message m and $(P, rP, H_2(m_i, U), V)$ is a valid Diffie-Hellman tuple. From the result of [7], we also can deduce that the probability of the adversary can successfully forge a valid partial signature is negligible.

Case 2: Forgery of the "Certificate"

Suppose the adversary chooses a different $r'P$. If he can forge a valid "certificate" which ID correspondence to $r'P$, he can also forge a valid signature of the target user.[4] However, if the adversary can forge a valid "certificate" of PKG, *i.e.*, he can forge a valid signature of Cha-Cheon's ID-based signature scheme on message m. Since Cha-Cheon's ID-based signature scheme is proved to be secure against on existential adaptively chosen message and ID attacks, the success probability of forgery in this case is negligible.

Note that the target user is randomly chosen, we can deduce that our signature scheme is secure against on existential adaptively chosen message and ID attacks under the assumption of CDHP is hard in G_1 and random oracle model. □

5 Proposed ID-based Group Signature Scheme

In this Section, we propose the ID-based group signature scheme. Suppose there exists a hierarchical ID-based system [15]. If the group manager is not a PKG, he then joins the system and becomes a PKG. Therefore we just consider the case that the group manager is a PKG .

[**Setup**]

The system parameters are the same as before. Every user with identity ID who gets his partial private key S_{ID} from the PKG is a "potential" group member.[5] The group public key $\mathcal{Y} = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$. PKG computes a

[4] In this case, PKG will not collude with the adversary, otherwise, the target user can prove the treachery of PKG afterwards.

[5] The users can choose to be the group members immediately or later. Also, there are some users who gets the private key from the PKG just for ordinary signature and they will never to be the "real" group members.

user' private key S_{ID} and sends it to the user via a secure channel. S_{ID} is only used for ordinary signature.

[**Join**]

When a user later wants to be a "real" member of the group, he and PKG perform the **Join** Protocol as follows:

- The user randomly chooses $x_i \in Z_q$ for $i = 1, 2, \cdots, k$. He then sends rx_iP, x_iP, rP, ID and S_{ID} to PKG.
- If $S_{ID} = sH_2(ID||T, rP)$ and $e(rx_iP, P) = e(x_iP, rP)$, PKG sends the user $S_i = sH_2(T, rx_iP)$ for $i = 1, 2, \cdots, k$. Otherwise the protocol is terminated.[6]
- The user's member certificates are (S_i, rx_iP) and his private signing keys are rx_i, here $i = 1, 2, \cdots, k$.
- PKG adds rx_iP, x_iP, rP, ID to the member list.

[**Sign**]

To sign a message m, the user randomly chooses a certain signing key and corresponding member certificate and then computes the following values:

- $U = aH_2(T, rx_iP)$ for randomly chosen integer $a \in Z_q^*$ and certain i.
- $V = rx_iH_2(m, U)$.
- $h = H_1(m, U + V)$.
- $W = (a + h)S_i$.

Then (U, V, W, T, rx_iP) is the signature of the message of m.

[**Verify**]

If T is a valid period, the verifier computes $Q = H_2(T, rx_iP)$, $H_2(m, U)$, $h = H_1(m, U + V)$. He accepts the signature if the following equations hold:

$$e(W, P) = e(U + hQ, P_{pub})$$
$$e(V, P) = e(H_2(m, U), rx_iP)$$

[**Open**]

Given a valid group signature, PKG can easily identify the user from rx_iP. The user cannot deny his signature because PKG can provide a proof that it is indeed the user's signature:

$$e(rx_iP, P) = e(x_iP, rP)$$

[6] PKG needs not to verify $S_{ID} = sH_2(ID||T, rP)$ for the users who become the group members immediately.

$$e(S_{ID}, P) = e(H_2(ID||T, rP), P_{pub})$$

Also, PKG cannot misattribute a signature to frame the user unless he can compute bP given p, aP and rP which satisfies:

$$a \equiv rb \bmod q$$

We define this problem the Reversion of Computation Diffie-Hellman Problem (RCDHP), which is equivalent to CDHP in G_1.

Theorem 2. *RCDHP is equivalent to CDHP in G_1.*

Proof. Given P, aP, bP, suppose we can solve RCDHP in G_1, then we can obtain $b^{-1}P$ from P and bP. Note $a \equiv (ab)b^{-1} \bmod q$, we can compute abP from P, aP and $b^{-1}P$, *i.e.*, we solve CDHP in G_1.

Given P, aP, bP, let $Q = bP$, so $P = b^{-1}Q$. Suppose we can solve CDHP in G_1, so with Q and $b^{-1}Q$ we can get $b^{-2}Q$, *i.e.*, $b^{-1}P$. Then we can obtain $ab^{-1}P$ from P, aP and $b^{-1}P$, *i.e.*, we solve RCDHP in G_1.

□

6 Analysis of Our Systems

6.1 Security

Theorem 3. *If there is an adversary $\mathcal{A}_0$ (without colluding with PKG) can forge a member certificate with time t and a non-negligible probability ϵ, then we can solve CDHP in G_1 at most with time t and a non-negligible probability ϵ.*

Proof. Consider the following game: the adversary $\mathcal{A}_0$ may query H_2 adaptively at most k times. Suppose the i-th input of query is (T, r_iP) and he gets the corresponding certificate S_i, here $1 \leq i \leq k$. Finally, he outputs a new pair (rP, S). $\mathcal{A}_0$ wins the game if rP is not queried and $e(S, P) = e(H_2(T, rP), P_{pub})$.

If $\mathcal{A}_0$ outputs a valid pair (rP, S). Let $H_2(T, rP) = aP$, $P_{pub} = bP$. We solved CDHP in G_1 for $S = abP$.

□

Theorem 4. *The non-interactive protocol underlying the signature schemes is an honest-verifier zero-knowledge proof of knowledge of a member certificate and corresponding identity.*

Proof. The proof that zero-knowledge is trivial. We restrict our attention the proof of knowledge part and we use the technique of [1]. We show that the knowledge extractor can recover the member certificate once it has found two accepting tuples.

Let (U, V, W, T, rx_iP) and (U, V', W', T, rx_iP) be two accepting tuples. Define $h = H_1(m, U + V)$. Because $e(W, P) = e(U + hH_2(T, rx_iP), P_{pub})$, we have

$$W = s(U + hH_2(T, rx_iP))$$

Similarly, we have $W' = s(U + h' H_2(T, rx_iP))$. So, we obtain

$$sH_2(T, rx_iP)) = (h - h')^{-1}(W - W')$$

Note that $e(rx_iP, P) = e(x_iP, rP)$, *i.e.*, rx_iP corresponds to rP and the identity ID. The signer can not deny his signature because his S_{ID} satisfies

$$e(S_{ID}, P) = e(H_2(ID||T, rP), P_{pub})$$

□

Theorem 5. *Our ID-based group signature scheme from bilinear pairings is secure under the assumption of CDHP is hard in the random oracle.*

Proof. We show that our scheme satisfies all the security properties listed in Definition 1.

– *Correctness*: It is trivial.
– *Unforgeability*: Even the "potential" member of the group cannot sign on behalf of the group. Based on the assumption that H_1 and H_2 are random oracles, it can be easily deduced by the theorem 4.
– *Anonymity*: Since x_i is randomly chosen, rx_iP reveals no identity information of the user to anyone except PKG.
– *Unlinkability*: Given rx_iP and rx_jP, it is computationally hard to decide they correspondence the same rP without knowing x_iP and x_jP.
– *Traceability*: PKG can open any valid group signature because he can provide a zero-knowledge proof that the signer indeed produces the signature.
– *Exculpability*: From the theorem 1 we can easily deduce neither the group manager nor a group member can sign messages on behalf of other group members. Also, the group manager or colludes with some group members can not misattribute a valid group signature to frame a certain member since one period T correspondences only one unique rP.
– *Coalition-resistance*: From the theorem 3 and 4 we can deduce that a colluding subset of group members (even if comprised of the whole group) cannot produce a valid signature that the group manager cannot open.

□

6.2 Efficiency

The size of the group public key and the group signatures is independent on the numbers of group members. The algorithms and protocols of the group signatures are efficient. A serious drawback of our scheme is that each signing key can just sign one message, which is same to [10]. However, the user can once apply many membership certificates corresponding to different signing keys, which is similar to the idea of "trustee tokens" [19]. Therefore, the user can use them for further signing without contacting with PKG each time. This idea is also used for secret handshakes agreement protocol [3].

6.3 Comparison with Two Previous Group Signature Schemes

We compare the proposed group signature scheme with previous two schemes. In the table 1, “independent, linear” denotes that the number is is independent or linear in the number of group members.

Properties	*Scheme* [8]	*Scheme* [1]	*Proposed Scheme*
Assumption	*Double* DLP *Root* DLP	*Strong* RSA DDHP	CDHP
Anonymity	*Computationally*	*Computationally*	*Computationally*
Identification	*by GM*	*by GM*	*by* $GM(PKG)$
Inclusion of new members	*Yes*	*Yes*	*Yes*
System	$CA-based$	$CA-based$	$ID-based$
Number of certificate	*One*	*One*	*Many*
Length of group public key	*Fixed*	*Fixed*	*Fixed*
Length of signature	*Fixed*	*Fixed*	*Fixed*
Computation	*Linear*	*Linear*	*Linear*
Communication	*Linear*	*Linear*	*Linear*

Table 1. Comparison with two previous group signature schemes

7 Concluding Remarks

The salient properties of group signature make it attractive for plenty of applications in electronic commerce [20, 26, 27]. In this paper we propose new ID-based systems without distributed PKGs to solve the problem of key escrow. We also propose an ID-based group signature scheme under the new systems from bilinear pairings. The size of the group public key and the length of the signature are independent on the numbers of the group. The security and performance of our scheme depend on our new ID-based system.

It is a drawback that a user should have a new key pair for each message if he wants to sign many message. It is an open problem to design an ID-based group signature scheme from bilinear pairings with one key pair. Recently, Bellare, Micciancio and Warinschi [5] provides theoretical foundations for the group signature primitive. How to design an ID-based signature scheme under such foundation is another open problem.

References

1. G. Ateniese, J. Camenisch, M. Joye, G. Tsudik, *A practical and provably secure coalition-resistant group signature scheme*, Advances in Cryptology-Crypto 2000, LNCS 1880, pp.255-270, Springer-Verlag, 2000.

2. G. Ateniese, G. Tsudik, *Some open issues and new directions in group signatures*, Financial Cryptography 1999, LNCS 1648, pp.196-211, Springer-Verlag, 1999.
3. D. Balfanz, G. Durfee, N. Shankar, D. Smentters, J. Staddon, H. Wong, *Secret handshakes from pairing-based agreements*, Proceeding of the 2003 IEEE Symposiumon Security and Privacy, pp. 180–196, 2003.
4. P. Barreto, H.Y. Kim, B.Lynn, and M.Scott, *Efficient algorithms for pairings-based cryptosystems*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
5. M. Bellare, D. Micciancio and B. Warinschi, *Foundations of group signatures: formal definations, simplified requirements, and a construction based on general assumptions*, Advances in Cryptology-Eurocrypt 2003, LNCS 2656, pp.614-629, Springer-Verlag, 2003.
6. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairings*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
7. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairings*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
8. J. Camenisch, *Efficient and generalized group signatures*, Advances in Cryptology-Eurocrypt 1997, LNCS 1233, pp.465-479, Springer-Verlag, 1997.
9. J. Camenisch and M. Stadler, *Efficient group signatures schemes for large groups*, Advances in Cryptology-Crypto 1997, LNCS 1294, pp.410-424, Springer-Verlag, 1997.
10. C. Castelluccia, *How to convert any ID-based Signature Scheme into a Group Signature Scheme*, Cryptology ePrint Archive, Report 2002/116.
11. J. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Public Key Cryptography-PKC 2003, LNCS 2567, pp.18-30, Springer-Verlag, 2003.
12. D. Chaum and E. van Heijst, *Group signatures*, Advances in Cryptology-Eurocrypt 1991, LNCS 547, pp.257-265, Springer-Verlag, 1991.
13. L. Chen and T. Pedersen, *New group signature schemes*, Advances in Cryptology-Eurocrypt 1994, LNCS 950, pp.171-181, Springer-Verlag, 1994.
14. L. Chen and T. Pedersen, *On the efficiency of group signatures providing information-theoretic anonymityenisch*, Advances in Cryptology-Eurocrypt 1995, LNCS 1233, pp.465-479, Springer-Verlag, 1997.
15. C. Gentry and A. Silverberg, *Hierarchical ID-Based Cryptography*, Advances in Cryptology-Asiacrypt 2002, LNCS 2501, pp.548–566, Springer-Verlag, 2002.
16. F. Hess, *Efficient identity based signature schemes based on pairingss*, Proc. 9th Workshop on Selected Areas in Cryptography – SAC 2002, LNCS 2595, Springer-Verlag, pp.310-324, 2002.
17. M. Joye, *On the difficulty coalition-resistance in group signature schemes (II)*, Technique Report, LCIS-99-6B, 1999.
18. M. Joye, S. Kim and N. Lee, *Cryptanalysis of two group signature schemes*, Information Security 1999, LNCS 1729, pp.271-275, Springer-Verlag, 1999.
19. A. Juels, *Trustee Tokens: simple and practical anonymous digital coin tracing*, Financial Cryptography 1999, LNCS 1648, pp.33-43, Springer-Verlag, 1999.
20. A.Lysyanskays, Z.Ramzan, *Group blind signatures: A scalable solution to electronic cash*, Financial Cryptography 1998, LNCS 1465, pp.184-197, Springer-Verlag, 1998.
21. W. Mao and C.H. Lim, *Cryptanalysis in prime order subgroup of Z_n*, Advances in Cryptology-Asiacrypt 1998, LNCS 1514, pp.214-226, Springer-Verlag, 1998.
22. S. Park, S. Kim and D.Won, *ID-based group signature*, Electronics Letters, 33(19), pp.1616-1617, 1997.

23. H. Petersen, *How to convert any digital signature scheme into a group signaure sheme*, In Security Protocols Workshop 1997, pp.177-190, Springer-Verlag, 1997.
24. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 1984, LNCS 196, pp.47-53, Springer-Verlag, 1984.
25. N.P. Smart, *An identity based authenticated key agreement protocol based on the Weil pairings*, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.
26. K. Sakurai, S. Miyazaki, *An Anonymous Electronic Bidding Protocol Based on New Convertible Group Signature Scheme*, ACISP 2000, LNCS 1841, pp.10-12, Springer-Verlag, 2000.
27. J. Traoré, *Group signatures and their relevance to privacy protecting offline electronic cash systems*, ACISP 1999, LNCS 1587, pp. 228-243, Springer-Verlag, 1999.
28. Y. Tseng and J. Jan, *A novel ID-based group signature*, International computer symposium, workshop on cryptology and information security, pp.159-164, 1998.
29. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, Advances in Cryptology-Asiacrypt 2002, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.