An ID-Based Short Group Signature Scheme

Xiangguo Cheng
School of Information Engineering, Qingdao University, Qingdao 266071, China
Email: chengxg@qdu.edu.cn

Shaojie Zhou
College of Measure-Control Technology and Communication Engineering,
Harbin University of Science and Technology, Harbin, 150040, China
Email: zhengl@qdu.edu.cn

Lifeng Guo
School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China
Email: lfguo@sxu.edu.cn

Jia Yu and Huiran Ma
School of Information Engineering, Qingdao University, Qingdao 266071, China
Email: {qduyujia, shangxian.yue2008}@163.com

***Abstract*—A new ID-based group signature scheme, in which group managers and group members are all ID-based, is presented in this paper. Our scheme is obtained by using a new way to the construction of group signature schemes and based on an ID-based signature scheme from bilinear pairing. Due to the nice and simple constructive method and the sound properties of bilinear pairing, it is shown that the proposed scheme is very simple and practical and has the advantages of concurrent join, immediate revocation, easy tracing and short signature length. The security analysis is also under the formal security notion of an ID-based group signature scheme.**

***Index Terms*—ID-Based Signature, Group Signature, Short Signature, Bilinear Pairing, Anonymity**

I. INTRODUCTION

A group signature scheme, introduced by Chaum and van Heyst [1], allows group members to anonymously sign messages on behalf of the group. In the case of a later dispute, the tracing manager can open a signature and identify the original signer. Group signatures have many applications where user anonymity is required such as anonymous credential systems [2], identity escrow [3], voting and bidding [4], and electronic cash systems [5]. The motivation for an ID-based cryptosystem, originally proposed by Shamir [6], is to authenticate messages without the need of exchanging public keys. A major advantage of an ID-based signature is that it allows one to sign a message in such a way that any user can verify the signature using the signer's identifier information such as email address instead of using his/her digital certificate. An ID-based group signature is a combination of these two concepts. Many group signature schemes [2-4, 7-19] have been proposed so far. Some of them [16-19] are ID-based. The scheme in [16] is inefficient since the length of group public keys and signatures linearly grew with group size and its anonymity is not guaranteed [25]. A novel ID-based group signature scheme is presented in [17]. Unfortunately, it is universally forgeable [26] and not coalition-resistant [27]. The scheme in [18] is not practical since a new pair of certificate is required for each signature. Furthermore, all of them are not truly ID-based group signature scheme in the strict sense since they have ID-based key pairs for group members only. The scheme proposed in [19] is the first truly ID-based group signature scheme, in which group managers and group members are all ID-based. However, it is not practical.

Different from the traditional way, Cheng *et al.* [24] provided a new method to the construction of group signature schemes. They show us a nice and practical way for converting a general signature scheme such as RSA, DSA into a group signature scheme. Using this method, based on an ID-based signature scheme from bilinear pairings given by Hess [20], we put forward a group signature scheme where group managers and group members are all ID-based. Due to the nice constructive method and the sound properties of bilinear pairing, it is shown that our scheme is practical, efficient and has short signature length. The security analysis is also under the formal security notion of an ID-based dynamic group signature scheme.

This paper is organized as follows. The model and security requirements of an ID-based group signature scheme are present in Section 2. We propose a new ID-based group signature scheme and analyze its security in Section 3. The Performance Evaluation of our scheme is

Manuscript received Mar 17, 2012; revised Aug 16, 2012; accepted Sep 7, 2012.
Corresponding author: Xiangguo Cheng

doi:10.4304/jsw.8.3.554-559

shown in Section 4 and the last section is a conclusion of our paper.

II. Model of ID-Based Group Signatures

We use the model of ID-based group signatures given in [19]. It is in fact an ID-based version of the formal model for dynamic group signatures [14]. We give a briefly description here and refer the readers to [14, 19] for more details.

A. Participants and Procedures

An ID-based group signature scheme consists of a trusted Private Key Generator (PKG) for the producing of private keys of group managers and users, an Issuer Authority (IA) for the joining of users, an Open Authority (OA) for the opening of signatures and some users that may become group members. The scheme is specified as a tuple $(Setup, Gkg, Ukg, Join, Iss, Gsig, Gvf, Open, Judge)$ of polynomial time algorithms which are defined as follows.

- *Setup*: Run by PKG, on inputs a security parameter κ, and outputs CP, a set of common parameters, and the master public-private key pair (pk_m, sk_m).
- *Gkg*: Run by PKG, on inputs κ, CP, (pk_m, sk_m), the identities ID_I and ID_O of IA and OA, and outputs the secret keys sk_I and sk_O of IA and OA, respectively.
- *Ukg*: Run by PKG, on inputs κ, CP, (pk_m, sk_m), the identity ID_i of user i, and outputs the secret key sk_i of user i.
- *Join*, *Iss*, *Gsig*, *Gvf*, *Open* and *Judge* are all similar to that in [14].

B. Security Notions

We use the security notions of *Correctness*, *Anonymity*, *Traceability*, *Non-frameability* from [19]. They are only a slight modification of [14] for ID-based. These notions are formulated via some experiments in which the capabilities of an adversary are modeled by providing it access to some oracles. Readers are referred to [14, 19] for these experiments and oracles. Here is only a briefly description of these notions.

- *Correctness*: *Correctness* requires that, on the one hand, signatures generated by honest group members must be accepted by *Gvf* algorithm; on the other hand, the *Open* algorithm must be able to correctly identify the original signer from a signature generated by an honest group member.
- *Anonymity*: *Anonymity* requires that anyone except OA finds it hard to recover the identity of the original signer from the group signatures.
- *Traceability*: *Traceability* requires that the adversary be unable to generate signatures that OA cannot open, or signatures that OA can open while cannot produce a correct proof.
- *Non-frameability*: *Non-frameability* requires that the adversary be unable to create a correct proof that a group member produced a certain valid signature unless this user really did generate this signature.

III. New ID-Based Group Signature

A. Preliminaries

Let $(G_1, +)$ and $(G_2, \cdot)$ denote cyclic groups of prime order q and P a generator of G_1. The identity element of G_1 and G_2 is denoted as O and 1, respectively. Assume that the DL problem in both G_1 and G_2 is hard.

A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ satisfying the following conditions:

- **Bilinear:** $e(mQ, nR) = e(Q, R)^{mn}$ for any $m, n \in \mathbf{Z}_q^*$ and $Q, R \in G_1$.
- **Non-degenerate**: There exists $Q, R \in G_1$ such that $e(Q, R) \neq 1$, that is $e(P, P) \neq 1$ since $G_1 = \langle P \rangle$ is cyclic.
- **Computable**: There exists an efficient algorithm for computing $e(Q, R)$ for any $Q, R \in G_1$.

The following two problems in G_1 are often considered.

- **CDH problem**: Given $Q, mQ, nQ \in G_1$ for unknown $m, n \in \mathbf{Z}_q^*$, to compute $mnQ \in G_1$.
- **DDH problem**: Given $Q, mQ, nQ, lQ \in G_1$ for unknown $m, n, l \in \mathbf{Z}_q^*$, decide whether $l \equiv mn \pmod q$.

Both the CDH and DDH problems are generally considered to be hard in G_1. However, the DDH problem becomes easy with the help of bilinear pairing since $l \equiv mn \pmod q$ if and only if $e(mQ, nQ) = e(Q, lQ)$.

B. Hess's ID-based signature scheme

We use the ID-based signature scheme given by Hess [20] as a base scheme to construct our group signature scheme. We first give a review of this scheme. Note that it has been proven to be unforgeable against chosen message attack in the random oracle model assuming that the CDH problem is intractable.

- *Setup*: Run by PKG to generate its master key and all the necessary common parameters of the system.
  - Choose a group $G_1 = < P >$ of prime order $q \geq 2^\kappa$, where κ is a security parameter. Specify the bilinear pairing $e: G_1 \times G_1 \to G_2$.
  - Picks $s \in_R \mathbf{Z}_q^*$ and computes $P_{pub} = sP$.
  - Chooses two hash functions $H_1: \{0,1\}^* \to G_1^*$, where $G_1^* = G_1 \setminus \{O\}$ and $H_2: \{0,1\}^* \times G_2 \to \mathbf{Z}_q^*$.
  - Publishes $CP = \{G_1, G_2, q, P, P_{pub}, e, H_1, H_2\}$, the set of system common parameters. The master public-private key pair is set to be $(pk_m, sk_m) = (P_{pub}, s)$.
- *Extract*: Given an ID, the identity of a user. PKG computes $Q_{ID} = H_1(ID)$ and $D_{ID} = sQ_{ID}$. The private key match to ID is D_{ID}.
- *Sign*: To sign a message *M*, a signer, whose identity is ID, needs to do the following work.
  - Chooses $k \in_R \mathbf{Z}_q^*$.
  - Computes $K = kP$ and $r = e(K, P) = e(P, P)^k$.
  - Computes $v = H_2(M, r)$ and $U = vD_{ID} + K$.

— Outputs a signature $\sigma = (U, v)$.

- *Verify*: Any one can verify a signature σ on some message *M* using the signer's identity ID.
  — Computes $r = e(U, P)e(Q_{ID}, -P_{pub})^{v}$.
  — Accepts the signature if and only if $v = \mathrm{H}_2(M, r)$.

C. Proposed Scheme

The new ID-based group signature scheme is described as follows.

- *Setup*: Similar to the *Setup* algorithm in subsection B.
- *Gkg*: Given ID_I, the identity of IA, PKG computes $Q_I = \mathrm{H}_1(ID_I)$, $D_I = sQ_I$. The private key of IA match to ID_I is set to be $sk_I = D_I$.
- *Ukg*: Given ID_i, the identity of user *i*, PKG computes $Q_i = \mathrm{H}_1(ID_i)$, $D_i = sQ_i$. The private key of user *i* match to ID_i is set to be $sk_i = D_i$.
- *Join*, *Iss*: To realize the join of user *i*, IA, OA and user *i* cooperate to do as follows.
  — user *i* sends ID_i to IA.
  — IA chooses $X_i \in_R \mathrm{G}_1$, computes $Y_i = D_I - X_i$, and sends X_i to user *i* and (Y_i, ID_i) to OA, respectively.
  — OA adds (Y_i, ID_i) to L_1, the list of group members.

After this protocol, user *i* becomes a group member and his group membership secret key is $gsk_i = X_i$.

- *Gsig*: To generate a signature on some message *M*, user *i* cooperates with OA to do as follows.
  — User *i* chooses $k_{i_1} \in_R \mathbf{Z}_q^*$, computes $K_{i_1} = k_{i_1} P$ and sends (ID_i, K_{i_1}, M) to OA.
  — OA first checks whether ID_i is in L_1 or not. If not, it refuses to provide signing help; If yes, it chooses $k_{i_2} \in_R \mathbf{Z}_q^*$, computes $K_{i_2} = k_{i_2} P$, $K_i = K_{i_1} + K_{i_2}$, $r_i = e(K_i, P)$ and $v_i = \mathrm{H}_2(M, r_i)$. It sends v_i back to user *i*.
  — User *i* computes $U_{i_1} = v_i(X_i + D_i) + K_{i_1}$ and sends it back to OA.
  — OA computes $R_i = k_{i_2} P_{pub}$, $U_{i_2} = v_i(Y_i + R_i) + K_{i_2}$, $U_i = U_{i_1} + U_{i_2}$ and $S_i = Q_i + K_{i_2}$, where $Q_i = \mathrm{H}_1(ID_i)$. It stores (ID_i, k_{i_2}, M) in L_2, the list of signing information, and sets the group signature on *M* to be $\sigma_i = (U_i, S_i, v_i)$.
- *Gvf*: Anyone can verify the signature σ_i on message *M* using the group identity ID_I.
  — Computes $r_i = e(U_i, P)e(Q_I + S_i, -P_{pub})^{v_i}$.
  — Accepts the signature if and only if $v_i = \mathrm{H}_2(M, r_i)$.
- *Open*: To open a group signature $\sigma_i = (U_i, S_i, v_i)$ on *M*, OA can easily identify the original signer ID_i from the list (ID_i, k_{i_2}, M) stored in L_2.
- *Judge*: To show a group signature $\sigma_i = (U_i, S_i, v_i)$ on *M* is indeed generated by user *i*, OA computes $R_i = k_{i_2} P_{pub}$, $U_i' = v_i R_i$ and $U_i'' = U_i - U_i'$. Noted that (U_i'', v_i) is a multi-signature under ID_I and ID_i, which can be only generated by user *i* collaborating with OA.

D. Security Analysis

Theorem 1. The proposed scheme has the security property of *correctness*.

Proof. We first prove correctness of the signature. Given a signature $\sigma_i = (U_i, S_i, v_i)$ on some message *M* generated by member *i*, note that

$$\begin{aligned} U_i &= U_{i_1} + U_{i_2} \\ &= (v_i(X_i + D_i) + K_{i_1}) + (v_i(Y_i + R_i) + K_{i_2}) \\ &= v_i(D_I + D_i + R_i) + K_i \\ e(U_i, P) &= e(v_i(D_I + D_i + R_i) + K_i, P) \\ &= e(v_i s(Q_I + Q_i + K_{i_2}), P) \cdot e(K_i, P) \\ &= e(Q_I + S_i, P_{pub})^{v_i} \cdot e(K_i, P) \\ e(U_i, P) &\cdot e(Q_I + S_i, -P_{pub})^{v_i} \\ &= e(Q_I + S_i, P_{pub})^{v_i} \cdot e(K_i, P) \cdot e(Q_I + S_i, P_{pub})^{-v_i} \\ &= e(K_i, P) = r_i \end{aligned}$$

That is to say, a valid group signature can be accepted by the *Gvf* algorithm.

To prove that a signature $\sigma_i = (U_i, S_i, v_i)$ on *M* is indeed generated by user *i*, OA provides a proof (U_i'', v_i). Note that

$$\begin{aligned} U_i'' &= U_i - U_i' = U_{i_1} + U_{i_2} - U_i' \\ &= v_i(D_I + D_i + R_i) + K_i - v_i R_i \\ &= v_i(D_I + D_i) + K_i \\ e(U_i'', P) &= e(v_i(D_I + D_i) + K_i, P) \\ &= e(v_i s(Q_I + Q_i), P) \cdot e(K_i, P) \\ &= e(Q_I + Q_i, P_{pub})^{v_i} \cdot e(K_i, P) \\ e(U_i'', P) &\cdot e(Q_I + Q_i, -P_{pub})^{v_i} \\ &= e(Q_I + Q_i, P_{pub})^{v_i} \cdot e(K_i, P) \cdot e(Q_I + Q_i, P_{pub})^{-v_i} \\ &= e(K_i, P) = r_i \end{aligned}$$

Therefore, (U_i'', v_i) is a valid multi-signature on *M* under ID_I and ID_i. Note that only user *i* can cooperate with OA to generate this signature.

Theorem 2. Our scheme has the security property of *anonymity* with the assumption that the CDH problem in G_1 is hard.

Proof. Assumed that $\sigma_i = (U_i, S_i, v_i)$ is a signature on *M* given by member *i*. From the generation of σ_i, we know that $v_i = \mathrm{H}_2(M, r_i)$, where $r_i = e(K_i, P) = e(P, P)^{k_{i_1} + k_{i_2}}$, $U_i = v_i(D_I + D_i + R_i) + (k_{i_1} + k_{i_2})P$ and $S_i = Q_i + K_{i_2}$, where $K_{i_2} = k_{i_2} P$. Note that r_i is a random element in G_2 and $K_{i_2} = k_{i_2} P$ a random element in G_1 since k_{i_1} and k_{i_2} are both randomly chosen from $\mathbf{Z}_q^*$. Furthermore, U_i and S_i are both random elements in G_1 and v_i a random element in $\mathbf{Z}_q^*$. Thus we can find no information of signer *i* just from σ_i. That is, all signatures are indistinguishable.

The following is an anonymity analysis of our scheme under the formal model [19].

In the formal model, an adversary A, who wants to break the anonymity, has the power to get the private key and the group membership secret key of any group member and the private key of IA. It also has the power to add group members by running the *Join* protocol and revoke some group members by asking OA not to provide these members signing help. It is additionally given the access to *Open* oracle on signatures of its choice.

A chooses two honest group members at its will, i_0 and i_1. It also has the power to provide any message M. A is given a signature $\sigma_{i_b} = (U_{i_b}, S_{i_b}, v_{i_b})$ on M generated by i_b, where b is chosen randomly from $\{0,1\}$. The goal of A is to guess who is the original signer, i_0 or i_1.

The following discussion shows that, if A wins the game, it is also able to solve an instance of CDH problem in G_1.

Note that A knows D_{i_b} and D_I, the private key of member i_b and IA, respectively. It chooses $t_1, t_2 \in_R \mathbf{Z}_q^*$, and computes $T_1 = t_1 P$, $T_2 = t_2 P$, $R_1 = t_1 P_{pub}$, $R_2 = t_2 P_{pub}$, $U_1 = v_{i_b}(D_I + D_{i_b} + R_1)$, $U_2 = v_{i_b}(D_I + D_{i_b} + R_2)$, $U'_{i_b} = U_{i_b} - U_1$, $U''_{i_b} = U_{i_b} - U_2$.

Given $P_{pub} = sP$ and $v_{i_b}(T_2 - T_1) = tP$, note that

$$e(U_1, P) = e(v_{i_b}(D_I + D_{i_b} + R_1), P) = e((Q_I + Q_{i_b} + T_1), P_{pub})^{v_{i_b}},$$

$$e(U_2, P) = e(v_{i_b}(D_I + D_{i_b} + R_2), P) = e((Q_I + Q_{i_b} + T_2), P_{pub})^{v_{i_b}}$$

$$\begin{aligned} e(U'_{i_b}, P) &= e(U_{i_b} - U_1, P) = e(U_{i_b}, P) \cdot e(U_1, P)^{-1} \\ &= r_{i_b} \cdot e(Q_I + S_{i_b}, P_{pub})^{v_{i_b}} \cdot (e((Q_I + Q_{i_b} + T_1), P_{pub})^{v_{i_b}})^{-1} \\ &= r_{i_b} \cdot e(Q_I + S_{i_b}, P_{pub})^{v_{i_b}} \cdot e(-(Q_I + Q_{i_b} + T_1), P_{pub})^{v_{i_b}} \\ &= r_{i_b} \cdot e(S_{i_b} - Q_{i_b} - T_1, P_{pub})^{v_{i_b}} \end{aligned}$$

where $r_{i_b} = e(U_{i_b}, P) e(Q_I + S_{i_b}, -P_{pub})^{v_{i_b}}$. Similarly, $e(U''_{i_b}, P) = r_{i_b} \cdot e(S_{i_b} - Q_{i_b} - T_2, P_{pub})^{v_{i_b}}$. Hence we have

$$\begin{aligned} e(U'_{i_b} - U''_{i_b}, P) &= e(U'_{i_b}, P) e(U''_{i_b}, P)^{-1} \\ &= r_{i_b} \cdot e(S_{i_b} - Q_{i_b} - T_1, P_{pub})^{v_{i_b}} \cdot r_{i_b}^{-1} \cdot e(S_{i_b} - Q_{i_b} - T_2, P_{pub})^{-v_{i_b}} \\ &= e(P_{pub}, v_{i_b}(T_2 - T_1)) = e(sP, tP) = e(stP, P) \end{aligned}$$

Due to the non-degeneracy of bilinear pairing, we have $U'_{i_b} - U''_{i_b} = stP$. That is to say, A has solved an instance of CDH problem in G_1. This is contradict to the fact that the CDH problem in G_1 is intractable. Thus our scheme has the security property of anonymity.

Theorem 3. Our scheme has the security property of *traceability* with the assumption that the CDH problem in G_1 is intractable.

Proof. To prove the security property of traceability of our scheme in the formal model, we give an adversary A the capability of adding or revoking group members and the capability of obtaining both the private key and the group membership secret key of any group member. A is additionally given the access to *Gsig* and *Open* oracles. However, IA and OA here must be assumed to be honest.

Group signatures here are generated by group members cooperating with OA. The identity of the signer has been stored in L_2 by OA at the time it provided him signing help. Thus the traceability here means that *an adversary cannot generate a valid group signature without the help of OA.*

If A can forge a signature $\varepsilon = (U, v)$ on some message M under ID_I. Note that we have given A the capability of breaking all the group members. It can therefore forge signatures of member i. Let $Q_i = \mathrm{H}_1(ID_i)$, $U_i = vD_i$. It is apparent that $\sigma = (U + U_i, Q_i, v)$ is a valid group signature on M that OA cannot open. However, we have assumed that IA is honest and cannot be broken. [20] tells us that none except IA is able to generate such a signature if the CDH problem in G_1 is intractable. Signatures under ID_I here are in fact $(2,2)$ threshold signatures produced by group members and OA. It is shown in [23] that, even if group members are corrupted, the signatures are still unforgeable since the private share of OA is unknown to the adversary.

The above discussion tells us that our group signature is traceable if the CDH problem in G_1 is intractable.

Theorem 4. Our scheme has the security property of *non-frameability* if the CDH problem in G_1 is intractable.

Proof. To prove the non-frameability of our scheme, we give an adversary A very strong attack capabilities, including the capability to corrupt IA and OA, which means that A is not only given the private key of IA, but also allowed to access to the storage list of OA. A is also given the capability of adding or revoking group members. The only unknown of A is the private keys of the honest group members.

The non-frameability in our scheme means that *an adversary cannot generate a valid group signature on behalf of an honest group member*.

Given a signature $\sigma_i = (U_i, S_i, v_i)$ on some message M generated by an honest member i, where

$$\begin{aligned} U_i &= U_{i_1} + U_{i_2} \\ &= (v_i(X_i + D_i) + K_{i_1}) + (v_i(Y_i + R_i) + K_{i_2}) \\ &= v_i D_I + (v_i D_i + K_{i_1}) + (v_i R_i + K_{i_2}) \\ &= \Pi_1 + \Pi_2 + \Pi_3, \end{aligned}$$

The adversary A can easily generate Π_1 and Π_3 since it has corrupted IA and OA. However, Π_2 is a signature on M under identity ID_i. It has been shown in [20] that such a signature is unforgeable if CDH problem in G_1 is intractable. Therefore, none except user i can collaborate with OA to generate a valid group signature that OA can trace back to i. That is to say, our scheme has the security property of *non-frameability*.

V. COMPARISON

Compared with previous group signature schemes, our scheme not only is truly ID-based (that is, IA , OA and

group members are all ID-based), but also has some additional functions described as follows.

- **Concurrent join, fast revocation and easy tracing**. It is very easy in our scheme to join a group for a user and to revoke the membership of a member for the manager. Joining of users can be done concurrently at any time. The group membership of a member can be immediately revoked at any time if OA does not provide him signing help. To trace a signature, OA needs only store the identity of the signer at the time it provides him signing help.
- **Trapdoor-free**. Our scheme satisfies the property of trapdoor-free. Trapdoor-free means that none of the parties in the system including the group manager needs to know the trapdoor. The system trapdoor is only used during the initialization to generate system parameters. The advantage of this property is that the same trapdoor information can be used to initiate different groups. There are only two trapdoor-free group signature schemes [3, 8] so far.
- **Signature length**. We compare the signature length of our scheme with that of BBS scheme [6] and NS scheme[8].BBS scheme is the shortest group signature scheme so far and NS scheme is an efficient trapdoor-free group signature scheme. They are both from bilinear pairing. Assumed that all of these schemes are implemented using elliptic curves over a finite field $\mathbf{Z}_q$, where q is about a 170-bit prime, G_1 is a subgroup of an elliptic curve group over $\mathbf{Z}_q$, elements in G_1 are 171-bit strings. G_2 is a subgroup of $\mathbf{Z}_q$, whose size is about 2^{1020}. A possible choice for these parameters can be found in [14,15]. A signature in BBS scheme comprises six elements of $\mathbf{Z}_q$ and three elements of G_1. A signature in NS scheme comprises 8 elements of $\mathbf{Z}_q$ and 10 elements of G_1. In contrast, the signature in our scheme comprises only three elements of G_1. The signature length in our scheme is approximately one third and one sixth of that in BBS scheme and NS scheme, respectively. The result is summarized in Table I.

TABLE I.

COMPARISON OF SIGNATURE LENGTH(BITS)

Schemes	BBS Scheme	NS Scheme	Our Scheme
Signature Length	1533	3070	513

- **Computational complexity**. We also estimate the computational cost of our scheme and that of BBS scheme and NS scheme by the number of scalar multiplications and element additions in G_1, and the number of pairing operations required for *Gsig* and *Gvf*, since these are the most costly computations. We summarize the result in Tabe II, where "# SMul", "# EAdd" and "# Pairing" are abbreviations of "the number of scalar multiplications in G_1", "the number of element additions in G_1" and "the number of pairing operations", respectively.

TABLE II.

COMPARISON OF COMPUTATIONAL COST(*Gsig* / *Gvf*)

Schemes	# SMul	# EAdd	# Pairing
BBS Scheme	9/8	3/4	0/2
NS Scheme	11/8	5/5	0/3
Our Scheme	8/1	6/2	0/2

- **Disadvantages**. One disadvantage of our scheme is that OA must be online to help group members to generate group signatures. Any group member can collaborate with OA to reveal D_M, the private key of IA. Furthermore, Some storage Lists (L_1 and L_2) are also controlled by OA. Therefore, OA must be fully trusted in our scheme.

VI. CONCLUSIONS

By using a new method, we have constructed a truly ID-based group signature scheme, in which IA, OA and group members are all ID-based. It has the advantages of concurrent join, fast revocation, easy tracing, short length of signature and trapdoor-free. A drawback of our scheme is that OA must be online and the signature is finished by a cooperation of OA with group members.

ACKNOWLEDGMENT

This work was supported by grants from HUAWEI, the National Natural Science Foundation of China (No. 61272425 and No. 61202365), Ministry of Education Humanities and Social Science Foundation of China (No. 11YJCZH039), and the Shandong Province Natural Science Foundation of China (No. ZR2010FQ019).

REFERENCES

[1] D.Chaum,E.van Heyst,"Group signatures,"*Proc. Eurocrypt 1991*, LNCS 547, Springer-Verlag, 1991, 257-265.
[2] G. Ateniese, B. de Medeiros, "Efficient group signatures without trapdoors," *Proc. Asiacrypt 2003*, LNCS 2894, Springer-Verlag, 2003, 246-268.
[3] S. Kim, S. Park, D. Won, "Convertible group signatures," *Proc. Asiacrypt 1996*, LNCS 1163, Springer-Verlag, 1996, 311-321.
[4] G.Ateniese, J.Camenisch, M.Joye, G.Tsudik, "A practical and provably secure coalition-resistant group signature scheme," *Proc. Crypto 2000*, LNCS 1880, Springer-Verlag, 2000, 255-270.
[5] M.Michels."Comments on some group signature schemes." *TR-96-3-D*, Department of Computer Science, University of Technology, Chemnitz-Zwickau, Nov. 1996.
[6] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proc. Crypto 1984*, LNCS 196, Springer-Verlag, 1984, 47-53.
[7] J. Camenisch, M. Stadler, "Efficient and generalized group signatures," *Proc. Eurocrypt 1997*, LNCS 1233, Springer-Verlag, 1997, 465-479.
[8] L. Chen, T. P. Pedersen, "New group signature schemes," *Proc. Eurocrypt 1994*, LNCS 950, Springer-Verlag, 1994, 171-181.
[9] J. Camenisch, M. Stadler, "Efficient group signature schemes for large groups," *Proc. Crypto 1997*, LNCS 1296, Springer-Verlag, 1997, 410-424.

[10] J. Camenisch, M. Michels, "A group signature scheme with improved efficiency," *Proc. Asiacrypt 1998*, LNCS 1514, Springer-Verlag, 1998, 160-174.
[11] J. Camenisch, M. Michels, "Separability and efficiency for generic group signature schemes," *Proc. Crypto 1999*, LNCS 1666, Springer-Verlag, 1999, 413-430.
[12] M. Bellare, D. Micciancio, B. Warinschi, "Foundations of group signatures:formal definitions,simplified requirement, and a construction based on general assumptions," *Proc. Eurocrypt 2003*,LNCS 2656, Springer-Verlag, 2003, 614-629.
[13] D.Boneh, X.Boyen, H.Shacham, "Short group signatures," *Proc. Crypto 2004*, LNCS 3152, Springer-Verlag, 2004, 41-55.
[14] M. Bellare, H. Shi, C. Zhang, "Foundations of group signatures: the case of dynamic groups," *Proc.CT-RSA 2005*, LNCS 3376, Springer-Verlag, 2005, 136-153.
[15] L. Nguyen, R. Safavi-Naini, "Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings," *Proc. Asiacrypt 2004*, LNCS 3329, Springer-Verlag, 2004, 372-386.
[16] S. Park, S. Kim, D. Won, "ID-based group signature," *Electronics Letters*, 33 (19), 1998, 1616-1617.
[17] Y. Tseng, J. Jan, "A novel ID-based group signature," *Proc. International computer symposium, workshop on cryptology and information security*, 1998, 159-164.
[18] X.Chen,F.Zhang,K.Kim, "A new ID-based group signature scheme from bilinear pairings," *Cryptology ePrint Archive*, Report 2002/184, 2002, http://eprint.iacr. org.
[19] V. K. Wei, T. H. Yuen, F. Zhang, "Group signature where group manager, members and open authority are identity-based," *Proc. Information Security and Privacy (ACISP 2005)*, LNCS 3574, Springer-Verlag, 2005, 468-480.
[20] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *Proc. of SAC 2002*, LNCS 2595, Springer-Verlag, 2002, 310-324.
[21] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," *Proc. Asiacrypt 2001*, LNCS 2248, Springer- Verlag, 2001, 514-532,.
[22] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing," *Proc. Crypto 2001*, LNCS 2139, Springer-Verlag, 2001, 213-229.
[23] J. Baek, Y. Zheng, "Identity based threshold signature scheme from the bilinear pairings," *Proceedings of the International Conference on Information Technology: Coding and Computing*, IEEE Computer Society Press, 2004, 124-128.
[24] X. Cheng, C. Yang, J. Yu, "A New Approach to Group Signature Schemes," *Journal of Computers*,6(4),Academy Publisher, 2011, 812-817.
[25] W. Mao, C. H. Lim, "Cryptanalysis in prime order subgroup of Z_n ," *Proc. Asiacrypt 1998*, LNCS 1514, Springer-Verlag, 1998, 214-226.
[26] M. Joye, S. Kim, N. Lee, "Cryptanalysis of two group signature schemes," *Proc. Information Security 1999*, LNCS 1729, Springer-Verlag, 1999, 271-275.
[27] M. Joye, "On the difficulty coalition-resistance in group signature schemes," *Technique Report*, LCIS-99-6B, 1999.