A Practical ID-Based 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 ＆Communication Engineering, Harbin University of Science and Technology, Harbin, 150040, China
Email: zhengl@qdu.edu.cn

Jia Yu, Xin Li and Huiran Ma
School of Information Engineering, Qingdao University, Qingdao 266071, China
Email: {qduyujia, tyz-007, shangxian.yue2008}@163.com

***Abstract*—A new ID-based group signature scheme, in which group managers (Membership Manager and Tracing Manager) and group members are all ID-based, is presented in this paper. Due to the nice constructive method of group signature schemes and the sound properties of bilinear pairing, it is shown that our scheme has the advantages of concurrent joining of users, immediate revocation of group members, easy tracing of signature signers and short length of signatures. Furthermore, it is trapdoor-free. The security analysis is under the formal security notion of an ID-based dynamic group signature scheme.**

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

I. Introduction

Group signatures, introduced by Chaum and Heyst [1], allow a group member to anonymously sign a message 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 in which user anonymity is required such as anonymous credential systems [2], identity escrow [3], voting and bidding [4] and electronic cash systems. The motivation for identity (ID)-based signature, originally proposed by Shamir [5], is to authenticate messages without the need of exchanging public keys. An advantage of ID-based signature is that it allows an user to sign a message in such a way that anyone can verify the signature using the signer's identifier information such as email address, instead of using his/her digital certificate. ID-based group signature is a combination of these two concepts. Several ID-based group signature schemes [9-12] have been proposed so far. The scheme in [9] is inefficient since the signature length linearly grew with group size and its anonymity is not guaranteed[18]. A novel ID-based group signature scheme is shown in [10]. It is universally forgeable[19] and not coalition-resistant[20]. The scheme in [11] is not practical since a new pair of certificates is required for each signature. In fact, these group signature schemes are not truly ID-based since they have ID-based key pairs for group members only. The first truly ID-based group signature scheme was presented by Wei *et al.* [12], in which the group managers and group members are all ID-based.

Different from the traditional method, Cheng *et al.* presented a new approach to group signatures in [17]. It shows us a good way for converting a general signature scheme such as RSA and DSA into a group signature scheme. Using this method, based on the ID-based signature scheme from bilinear pairing given by Yi [13], we put forward a truly ID-based group signature scheme. Due to the sound properties of bilinear pairing and the nice constructive method, it is shown that our scheme is efficient and has short signature length. Furthermore, it has the functions of fast joining of any users, immediate revocation of group members, easy tracing of group signatures and trapdoor-free. The security analysis is also under the formal security notion of an ID-based dynamic group signature scheme.

This paper is organized as follows. Section 2 presents the model and security requirements of an ID-based group signature and the new ID-based group signature scheme and its security analysis is given in Section 3. The additional functions and performance evaluation of our scheme is 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 [12]. It is in fact an ID-based version of the formal model for dynamic group signatures [7]. We briefly recall the model here and refer the readers to [7, 12] for more details.

A. Participants and Procedures

An ID-based group signature scheme consists of a trusted Private Key Generator (PKG) for the production

Manuscript received November 6, 2011; revised February 20, 2012.
Corresponding author: Xiangguo Cheng

doi:10.4304/jcp.7.11.2650-2654

of private keys of group managers and users, an authority called a Membership Manager (MM) for the joining of users, an authority called a Tracing Manager (TM) for the tracing 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, takes as input a security parameter λ, and outputs the system parameters SP and the master public-private key pair $(pk_m,\ sk_m)$.
- *Gkg*: Run by PKG, takes as input λ, SP, $(pk_m,\ sk_m)$, the identity ID_M of MM, and outputs the private key sk_M to MM.
- *Ukg*: Run by PKG, takes as input λ, SP, $(pk_m,\ sk_m)$, the identity ID_i of user i, and outputs the private key sk_i to user i.
- *Join*, *Iss*: similar to that in [7].
- *Gsig*: similar to that in [7].
- *Gvf*: similar to that in [7].
- *Open*: similar to that in [7].
- *Judge*: similar to that in [7].

B. Security Notions

We use the security notions of *Correctness*, *Anonymity*, *Traceability*, *Non-frameability* from [12]. They are only a slight modification of [7] for ID-based. These notions are formulated via some experiments, where the capabilities of an adversary are modeled by some oracles. Readers are referred to [12] for these experiments and oracles. Here is only a brief 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 TM 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 TM cannot open, or signatures that TM 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 $(\mathrm{G}_1,+)$ and $(\mathrm{G}_2,\cdot)$ 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.

A bilinear pairing is a map $e:\mathrm{G}_1\times\mathrm{G}_1\rightarrow\mathrm{G}_2$ satisfying the following conditions:

— **Bilinear:** $e(mQ_1,\ nQ_2)=e(Q_1,\ Q_2)^{mn}$ for any $m,\ n\in\mathbf{Z}_q^*$ and $Q_1,\ Q_2\in\mathrm{G}_1$.

— **Non-degenerate**: There exists $Q_1,\ Q_2\in\mathrm{G}_1$ such that $e(Q_1,Q_2)\neq 1$, that is $e(P,P)\neq 1$ since $\mathrm{G}_1=\langle P\rangle$ is cyclic.

— **Computable**: There exists an efficient algorithm for computing $e(Q_1,\ Q_2)$ for any $Q_1,\ Q_2\in\mathrm{G}_1$.

The following two problems in G_1 are often considered.

— **CDH problem**: Given $Q,\ mQ,\ nQ\in\mathrm{G}_1$ for unknown $m,\ n\in\mathbf{Z}_q^*$, to compute $mnQ\in\mathrm{G}_1$.

— **DDH problem**: Given $Q,mQ,nQ,lQ\in\mathrm{G}_1$ for unknown $m,\ n,\ l\in\mathbf{Z}_q^*$, to decide whether $l\equiv mn(\mathrm{mod}\,q)$.

The **CDH** problem is generally considered to be hard in G_1. However, the **DDH** problem in G_1 becomes easy since $l\equiv mn\ (\mathrm{mod}\,q)$ if and only if $e(mQ,nQ)=e(Q,lQ)$.

Chooses two hash functions:

$$\mathrm{H}_1:\{0,1\}^*\times\mathrm{G}_1\rightarrow\mathbf{Z}_q^* \text{ and } \mathrm{H}_2:\{0,1\}^*\rightarrow\mathrm{G}_1^*.$$

All these notations will exist as system parameters of the proposed scheme in this paper. We denote them as a set: $\mathrm{SP}=\{\mathrm{G}_1,\mathrm{G}_2,q,P,e,\mathrm{H}_1,\mathrm{H}_2\}$.

B. Proposed Scheme

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

- *Setup*: Given a security parameter λ, PKG runs the Parameters Generator [14, 15] to obtain the system parameters SP such that $q\geq 2^{\lambda}$. Then it picks $s\in_R\mathbf{Z}_q^*$ and computes $P_{pub}=sP$. The master public-private key pair is set to be $(pk_m,\ sk_m)=(P_{pub},\ s)$.
- *Gkg*: Given an identity ID_M of MM, PKG computes $Q_M=\mathrm{H}_2(ID_M)$, $D_M=sQ_M$. The private key of MM is $sk_M=D_M$.
- *Ukg*: Given ID_i, the identity of user *i*, PKG computes $Q_i=\mathrm{H}_2(ID_i)$, $D_i=sQ_i$. The private key of user i is $sk_i=D_i$.
- *Join*, *Iss*: To realize the join of user *i*, MM, TM and user *i* cooperate to do as follows.
  — user *i* sends ID_i to MM.
  — MM chooses $X_i\in_R\mathrm{G}_1$ and computes $Y_i=D_M-X_i$. It then sends X_i to user *i* and $(Y_i,\ ID_i)$ to TM.
  — TM 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 TM to do as follows.
  — User *i* sends ID_i to TM asking for signing help.
  — TM first checks whether ID_i is in L_1. It refuses to provide signing help if ID_i is not in L_1. Otherwise, it chooses $r_{i_1}\in_R\mathbf{Z}_q^*$, computes $R_{i_1}=r_{i_1}P$ and sends R_{i_1} to user *i*.

— Having received R_{i_1}, user i chooses $r_{i_2} \in_R \mathbf{Z}_q^*$, computes $R_{i_2} = r_{i_2}P$, $R_i = R_{i_1} + R_{i_2}$, $h_i = H_1(M, R_i)$, $\omega_i = r_{i_2}P_{pub} + h_i(X_i + D_i)$, and sends (ω_i, R_i, h_i) to TM.

— After receiving (ω_i, R_i, h_i), TM chooses computes $\eta_i = r_{i_1}P_{pub} + h_iY_i$, $\delta_i = h_ir_{i_1}P_{pub}$, $S_i = \eta_i + \omega_i + \delta_i$ and $V_i = Q_i + R_{i_1}$, where $Q_i = H_2(ID_i)$ and $h_i = H_1(M, R_i)$. TM stores $(ID_i,\ h_i,\ r_{i_1})$ in L_2, the list of tracing information, and sets the signature to be $\sigma_i = (R_i, S_i, V_i)$.

- *Gvf*: Anyone can verify a signature $\sigma_i = (R_i, S_i, V_i)$ on M by the equation $e(P, S_i) = e(P_{pub}, R_i + h_i(Q_M + V_i))$.
- *Open*: To open a signature $\sigma_i = (R_i, S_i, V_i)$ on M, TM computes $h_i = H_1(M, R_i)$. It can easily identify the original signer ID_i from the storage list $(ID_i,\ h_i,\ r_{i_1})$.
- *Judge*: To show that a group signature $\sigma_i = (R_i, S_i, V_i)$ on M is indeed generated by user *i*, TM computes $\delta_i = h_ir_{i_1}P_{pub}$ and $\varepsilon_i = S_i - \delta_i$. Note that ε_i is a multi-signature under ID_M and ID_i, which can be only generated by user *i* collaborating with TM.

C. Security Analysis

Theorem 1. Our scheme satisfies the security property of *correctness*.

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

$$\begin{aligned} S_i &= \eta_i + \omega_i + \delta_i \\ &= (r_{i_1}P_{pub} + h_iY_i) + (r_{i_2}P_{pub} + h_i(X_i + D_i)) + (h_ir_{i_1}P_{pub}) \\ &= (r_{i_1} + r_{i_2})P_{pub} + h_i(D_M + D_i + r_{i_1}P_{pub}) \\ &= (r_{i_1} + r_{i_2})sP + h_is(Q_M + Q_i + R_{i_1}) \\ &= (r_{i_1} + r_{i_2})sP + h_is(Q_M + V_i) \end{aligned}$$

Therefore,

$$\begin{aligned} e(P, S_i) &= e(P, (r_{i_1} + r_{i_2})sP + h_is(Q_M + V_i)) \\ &= e(P_{pub}, R_i + h_i(Q_M + V_i)) \end{aligned}$$

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

To prove that a group signature $\sigma_i = (R_i, S_i, V_i)$ on M is indeed generated by user *i*, TM provides a proof ε_i.

Note that

$$\begin{aligned} e(P, \varepsilon_i) &= e(P, S_i - \delta_i) \\ &= e(P, S_i) \cdot e(P, \delta_i)^{-1} \\ &= e(P_{pub}, R_i + h_i(Q_M + V_i)) \cdot e(P, h_ir_{i_1}P)^{-1} \\ &= e(P_{pub}, R_i + h_i(Q_M + V_i - R_{i_1})) \\ &= e(P_{pub}, R_i + h_i(Q_M + Q_i)) \end{aligned}$$

Therefore, ε_i is a valid multi-signature on M under ID_M and ID_i. Note that only user *i* can cooperate with TM to generate ε_i.

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

Proof. Given a group signature $\sigma_i = (R_i, S_i, V_i)$ on M generated by user i. Note that r_{i_1} and r_{i_2} are randomly chosen from $\mathbf{Z}_q^*$ and h_i is also a random element in $\mathbf{Z}_q^*$. Therefore, $R_{i_1} = r_{i_1}P$, $R_{i_2} = r_{i_2}P$, $\eta_i = r_{i_1}P_{pub} + h_iY_i$, $\delta_i = h_ir_{i_1}P_{pub}$ and $\omega_i = r_{i_2}P_{pub} + h_i(X_i + D_i)$ are all random elements in G_1. Furthermore, $R_i = R_{i_1} + R_{i_2}$, $S_i = \eta_i + \omega_i + \delta_i$ and $V_i = Q_i + R_{i_1}$ are also all random elements in G_1. We can find no information of member i just from $\sigma_i = (R_i, S_i, V_i)$. That is to say, it is anonymous.

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

To break the anonymity of our scheme, an adversary A is given the private key and the group membership secret key of any group member. It also has the power to add group members by running the *Join* protocol and revoke some group members by asking TM not to provide these members signing help. It is additionally given the access to *Open* oracle on signatures of its choice. Proceeding adaptively, A generates some group signatures and open these signatures via the *Open* oracle. Eventually A halts, outputting a message M and two honest group members i_0 and i_1. A is given a signature $\sigma_{i_b} = (R_{i_b}, S_{i_b}, V_{i_b})$ on M generated by i_b, here b is chosen randomly from $\{0,1\}$. The goal of A is to guess who is the signer, i_0 or i_1. In this stage, A can still query the *Open* oracle, but not on the challenge signature. If A wins the game, then the following discussion shows that it is also able to solve an instance of the CDH problem.

Note that A knows the private key D_{i_b} and the group membership secret key X_{i_b} of i_b, It chooses $r'_{i_b} \in_R \mathbf{Z}_q^*$, computes $R'_{i_b} = r'_{i_b}P$, $R''_{i_b} = R_{i_b} - R'_{i_b}$, $S'_{i_b} = r'_{i_b}P_{pub} + h_{i_b}D_{i_b}$ and $T_{i_b} = S_{i_b} - S'_{i_b}$, where $h_{i_b} = H_1(M, R_{i_b})$. Given $P_{pub} = sP$ and $R''_{i_b} + h_{i_b}(Q_M + V_{i_b} - Q_{i_b}) = tP$, in which s and t are unknown numbers in $\mathbf{Z}_q^*$. Note that

$$\begin{aligned} e(P, T_{i_b}) &= e(P, S_{i_b} - S'_{i_b}) = e(P, S_{i_b}) \cdot e(P, S'_{i_b})^{-1} \\ &= e(P_{pub}, R_{i_b} + h_{i_b}(Q_M + V_{i_b})) \cdot e(P_{pub}, R'_{i_b} + h_{i_b}Q_{i_b})^{-1} \\ &= e(P_{pub}, (R_{i_b} - R'_{i_b}) + h_{i_b}(Q_M + V_{i_b} - Q_{i_b})) \\ &= e(P_{pub}, R''_{i_b} + h_{i_b}(Q_M + V_{i_b} - Q_{i_b})) \\ &= e(sP, tP) = e(P, stP) \end{aligned}$$

Due to the non-degeneracy of bilinear pairing, we have $T_{i_b} = stP$. That is to say, A has solved an instance of the 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, 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, MM and TM here must be assumed to be honest.

Group signatures here are generated by group members collaborating with TM. The identity of the signer has been stored by TM 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 TM*.

If an adversary A can forge a signature $\varepsilon = (R, S)$ on some message M under ID_M, where $r \in_R \mathbf{Z}_q^*$, $R = rP$ and $S = rP_{pub} + H_1(M, R)D_M$. Note that we have given A the capability of breaking all members. It can therefore forge signatures of member i. Let $Q_i = \mathrm{H}_2(ID_i)$, $S_i = H_1(M, R)D_i$. It is apparent that $\sigma = (R, S + S_i, Q_i)$ is a valid signature on M that TM cannot open. However, we have assumed that MM is honest and cannot be broken. [13] tells us that anyone except MM is not able to generate such a signature if the CDH problem in G_1 is intractable. A signature under ID_M here is in fact a (2,2) threshold signature produced by a group member and TM. It is shown in [16] that, even if group members are corrupted, the signatures are still unforgeable since the private share of TM is still 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 MM and TM, which means that A is not only given the private key of MM, but also allowed to access to the storage list of TM. 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 $\sigma_i = (R_i, S_i, V_i)$ on some message M generated by an honest group member i, where

$$\begin{aligned} R_i &= R_{i_1} + R_{i_2} = r_{i_1}P + r_{i_2}P, \\ S_i &= \eta_i + \omega_i + \delta_i \\ &= (r_{i_1}P_{pub} + h_iY_i) + (r_{i_2}P_{pub} + h_i(X_i + D_i)) + h_ir_{i_1}P_{pub} \\ &= (r_{i_1}P_{pub} + h_iD_M) + (r_{i_2}P_{pub} + h_iD_i) + h_ir_{i_1}P_{pub} \\ &= \pi_1 + \pi_2 + \pi_3 \end{aligned}$$

and $V_i = Q_i + R_{i_1}$. The adversary A can easily generate π_1 since it knows the private key D_M of MM. π_3 can also be randomly generated by A. However, π_2 is a signature on M under ID_i. It has been shown in [13] that such a signature is unforgeable if CDH problem in G_1 is intractable. Therefore, none except user i can collaborate with TM to generate a valid group signature that TM 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, MM, TM 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 TM does not provide him signing help. To trace a signature, TM 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 $\mathbb{G}_1$ ", "the number of element additions in $\mathbb{G}_1$ " 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 TM must be online to help group members to generate group signatures. Any group member can collaborate with TM to reveal D_M , the private key of MM. Furthermore, Some storage Lists (L_1 and L_2) are also controlled by TM. Therefore, TM 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 MM, TM and group members are all ID-based. It has the advantages of concurrent joining, fast revocation, easy tracing, short length of signature and trapdoor-free. A drawback of our scheme is that TM must be online and the signature is finished under the cooperation of TM and group members.

ACKNOWLEDGMENTS

This work was supported by grants from the National Natural Science Foundation of China (No.60703089 and No. 60973135), Ministry of Education Humanities and Social Science Foundation of China (No. 11YJCZH039), and the Shandong Province Natural Science Foundation of China (No. ZR2010FQ019).

The authors wish to thank the reviewers for their valuable comments.

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] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proc. Crypto 1984*, LNCS 196, Springer-Verlag, 1984, 47-53.

[6] D. Boneh, X. Boyen, H. Shacham, "Short group signatures," *Proc.Crypto 2004*, LNCS 3152, Springer-Verlag, 2004, 41-55.

[7] 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.

[8] 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.

[9] S. Park, S. Kim, D. Won, "ID-based group signature," *Electronics Letters*, 33 (19), 1998, 1616-1617.

[10] Y. Tseng, J. Jan, "A novel ID-based group signature," *Proc. International computer symposium, workshop on cryptology and information security*, 1998, 159-164.

[11] 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.

[12] 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.

[13] X. Yi, "An identity-based signature scheme from the Weil pairing," *IEEE Communications Letters*, 7(2), 2004, 76-78.

[14] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," *Proc. Asiacrypt 2001*, LNCS 2248, Springer-Verlag, 2001, 514-532,.

[15] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing," *Proc. Crypto 2001*, LNCS 2139, Springer-Verlag, 2001, 213-229.

[16] X. Cheng, J. Liu, X. Wang, "An identity-based signature and its threshold version," *Proc. 19th International Conf. on Advanced Information Networking and Applications*, IEEE Computer Society Press, 2005, 973-977.

[17] X. Cheng, C. Yang, J. Yu, "A New Approach to Group Signature Schemes,"*Journal of Computers*, 6(4), Academy Publisher, 2011, 812-817.

[18] W. Mao, C. H. Lim, "Cryptanalysis in prime order subgroup of Z_n ," *Proc. Asiacrypt 1998*, LNCS 1514, Springer-Verlag, 1998, 214-226.

[19] M. Joye, S. Kim, N. Lee, "Cryptanalysis of two group signature schemes," *Proc. Information Security 1999*, LNCS 1729, Springer-Verlag, 1999, 271-275.

[20] M. Joye, "On the difficulty coalition-resistance in group signature schemes," *Technique Report*, LCIS-99-6B, 1999.