An Efficient Identity-based Group Signature Scheme over Elliptic Curves

Song Han[1,2], Jie Wang[2], and Wanquan Liu[1]

[1] Department of Computing, Curtin University of Technology
GPO Box U1987, Perth 6845, Western Australia, Australia
[2] Department of Mathematics, Beijing University
Beijing, 100871, China

[3]

Abstract. Considering such a scenario: Several network policemen consist of a group *NP* in a network; Every one of them can find out what kind of documents are harmful and then sign them. Any user in this network who receives the above documents would check whether a signature exists on the documents and also it is validly signed by the group *NP*. And then, this user can be convinced the document is really harmful. How can we realize (or deploy) the network security of this scenario? A group signature protocol may be a better choice. Group signatures allows every authorized member of a group to sign on behalf of the underlying group. Anyone except the group manager is not able to validate who signs a signature for a document. A new group signature scheme is proposed in this paper. It is an identity-based group signature scheme. This scheme makes use of a bilinear function derived from Weil pairings over elliptic curves. On the other hand, in the underlying composition of group signatures there is no exponentiation computation modulo a large RSA modulus. Thanks to these ingredients of the novel group signatures, the proposed scheme is efficient with respect to signing computation. In addition, this paper comes up with a security proof against adaptive forgeability.

Keywords: Group Signatures, Anonymity, Network Security, Weil Pairings, Security Protocol.

1 Introduction

Group signatures are one of the most important security protocols offered by cryptography. A group signature scheme is a digital signature scheme such that an individual member of a group can generate a signature (for a document), which can be verified by anyone, without revealing her identity; that is to say,

[3] This paper was published in the Proceedings of the European Conference on Universal Multiservice Networks 2004, Springer LNCS 3262.
Corresponding Author: Wanquan Liu
wanquan@cs.curtin.edu.au
Tel: 61-8-92662746; Fax: 61-8-92662819

authorized group member is in possession of anonymity. At the same time, group signatures are of the property that the signer can be identified later in case of disputes by a designated group manager. Moreover, no one including the group manager can misattribute a valid group signature. Therefore, in fact, the group signatures were first proposed in order to solve the following similar practical problem:

The corporation LTD has several computers, that are connected to the local network center of LTD. Every department of LTD only has one printer that is used only by the employees of this department. All these printers are also connected to the local network of LTD. Therefore, before each printing, the printer has to be confirmed that the employee belongs to the designated department. At the same time, the printer cannot display the identity of the employee in order to protect his or her privacy. However, if some printer was used frequently while off duty everyday, the supervisor is able to find out who abused that printer and then give him or her a fine bill.

The concept of group signatures was first introduced by Chaum and E.van Heyst in [5] in 1991. Besides the above applicable example, group signatures are also able to put on the applications: e-cash, bidding, voting, and so on. More generally, group signatures can be used to conceal organizational structures, for instance, when a company or a government agency issues a signed document. Very recently in [2], Ateniese and B. de Medeiros presented a new application concerning group signatures: anonymous E-prescriptions in medical situations. Previous to [8], all the proposed group signature protocols, for instance [5, 7, 11] have the following undesirable properties:

(1) the length of a group signature and (or) the length of group's public key depend linearly on the numbers of the underlying group.

(2) it is necessary to modify at least the public key, while new authorized member joins the group.

While subsequent works on group signature schemes for instance [8, 19, 1, 16, 12] possess the desirable property: the length of a group signature and (or) the size of the group public key are independent of the number of group members.

In traditional group signature signing algorithms the public keys of group members are essentially random bit strings picked from a given set. This leads to a problem of how the public keys are associated with the corresponding physical entities that are meant to be performing the signing computations. The identity-based group signature scheme assumes the existence of a trusted key generation center whose purpose is to give each member a personalized smart card when she first joins the network. The information embedded in this card enables each member to sign the documents she sends and verifies the documents she receives in a totally independent way, regardless of the identities of other members in this group. Previously issued cards do not have to be updated when new group member joins the network.

Recently identity-based cryptographic technique has also been applied to group signature schemes. The concept of identity-based cryptography is due to A.Shamir [14]. Shamir's original motivation was to simplify certificate manage-

ment in e-mail systems. When Alice sends mail to Bob at bob@hotmail.com, she simply encrypts her message using the public key string ' bob@hotmail.com '. There is no need for Alice to obtain Bob's public key certificate. Therefore, an identity-based cryptosystem is a system that allows a publicly known identifier (for instance email address, IP address) to be used as the public parameter or public key of a public/private key pair. In 1997, Park, Kim and Won presented the first identity-based group signature scheme. In 1998, Tseng and Jan proposed another identity-based group signature scheme. Thereafter, Popescu brought forward a modification on [18]. In 2002, Popescu proposed a new identity-based group signature scheme [12], that makes use of the pairings over elliptic curves. However, the scheme in [12] made use of the RSA signatures in group signatures. It is known that at the same security level ECC-521 can be expected to be on average 400 times faster than 15,360-bit RSA [10].

In this paper, a novel identity-based group signature scheme is proposed. It makes use of the bilinear pairings over elliptic curves. The size of the group public key is independent of the size of the underlying group. Also, the length of a group signature is independent of the number of the underlying group. Different from [12], our signing computation does not encompass RSA signatures. Therefore, by [10] the new scheme is expected to be more efficient than [12]. At the same time, a security proof against adaptive forgeability is presented in this paper.

The new group signature scheme proposed in this paper has the following desirable properties:

(1) Provably secure against adaptive forgeability. In [1, 6, 12] etc., there is no formal security proof against adaptive forgeability.

(2) No exponentiation calculations during both the generation and the verification of signatures. Previous to this new scheme, some group signature schemes need to compute exponentiations modulo a large RSA modulus [12]. Therefore, the new scheme is efficient in terms of computation cost.

The rest of this paper is organized as follows. The next section comes up the model: *identity-based group signatures*. In section 3, the paper presents some preliminaries including the bilinear pairings over elliptic curves. Section 4 brings forward the descriptions of the details of our new id-based group signature scheme. Subsequently, the security proofs and analyses are presented in section 5. The performance of the novel scheme is discussed in section 6. Finally in section 7, the paper is concluded.

2 The Model

In this section, the concept of an identity-based group signature scheme are presented as follows. In the following concept, see [9] for the definition of an identity-based digital signature scheme.

Definition 1. (Identity-based Group Signatures) An identity-based group signature scheme is an identity-based digital signature scheme comprised of the following five procedures:

(1) Setup: An algorithm, executed by the group manager, takes a random security parameter l as input and generates from it system parameters and master key. The system parameters are publicly known as the initial group public key; while the master key is only known to the group manager.

(2) Extract: A protocol between the group manager and a user. We assume the communications between the user and the group manager is private and authenticate. At the end of the protocol, the user becomes an authorized member of this group. The member's output is a membership certificate and a membership secret. Here the member's secret contains two parts: one is sent by the group manager, the other is chosen by herself.

(3) Sign: A probabilistic algorithm that on input a group public key, a membership secret, and a message m outputs a group signature of m.

(4) Verify: An algorithm for establishing the validity of an alleged group signature of a message with respect to the group public key.

(5) Reveal: An algorithm that, given a message, a valid group signature on it, a group public key and a group manager's master key, determines the identity of the actual signer.

A secure identity-based group signature scheme must satisfy as all or part of as the properties of:

(1) Correctness: Group signatures produced by a group member using SIGN algorithm must be accepted by VERIFY algorithm.

(2) Unforgeability: Only group members are able to sign messages on behalf of the underlying group.

(3) Anonymity: Given a valid signature of some message, identifying the actual signer is computationally infeasible for everyone but the group manager.

(4) Unlinkability: Deciding whether two different valid signatures were computed by the same group member is computationally hard.

(5) Exculpability: Neither a group member nor the group manager can sign on behalf of other group members.

(6) Traceability: The group manager is always able to open a valid signature and identify the actual signer in case of disputes.

3 Preliminaries

3.1 Notations

This subsection describes some notations used in this paper. Let q be a large prime, and Z_q^* be $Z_q \backslash \{0\}$. Let N be a positive integer. We write Z_N^* for the multiplicative group of integers modulo N. We denote $\varphi(n)$ as the Euler phi function. Let H and H_1 be two cryptographic hash functions: $H : \{0,1\}^* \rightarrow G_1$, and $H_1 : \{0,1\}^* \times G_1 \rightarrow G_1$.

3.2 Pairings over Elliptic Curves

Let p be a sufficiently large prime that satisfies: (a) $p \equiv 2\text{mod}3$; (b) $p = 6q - 1$, where q is also a large prime. Consider respectively the elliptic curves E/F_p and E/F_{p^2} defined by the equation:

$$y^2 = x^3 + 1.$$

Let G_1 be an additive group of points of prime order q on an elliptic curve E/F_p and let G_2 be a multiplicative group of same order q of some finite field F_{p^2}. We assume the existence of a bilinear map, the modified Weil pairing,

$$e : G_1 \times G_1 \to G_2$$

such that the Elliptic Curve Discrete Logarithm (ECDL) problems are difficult in G_1 and the Computational Diffi-Hellman (CDH) problems and the Inversion of Weil pairing (IWP) problem are difficult in G_2.

The modified Weil pairings $e : G_1 \times G_1 \to G_2$ has the following properties:

(1) Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for every pair $P, Q \in G_1$ and for any $a, b \in Z_p$.

(2) Non-degenerate: there exists at least one point $P \in G_1$ such that $e(P, P) \neq 1$.

(3) Efficient Computable: there are efficient algorithms to compute the bilinear pairings e.

3.3 Elliptic Curve Discrete Logarithms

Definition 2. (Elliptic Curve Discrete Logarithm Problem) Given G_1 as above, choose P a generator from G_1, given xP, where x is an unknown random element of Z_q^*, the Elliptic Curve Discrete Logarithm (ECDL) problem is to find x.

(ECDLP Assumption) Given xP and a generator P in G_1 with unknown $x \in Z_q^*$. There is no probabilistic polynomial algorithm to solve the Elliptic Curve Discrete Logarithm problem with non-negligible advantage.

3.4 Inversion of Modified Weil Pairings

Definition 3. (Inversion of Modified Weil Pairings Problem) Given G_1, G_2 and $e(\cdot, \cdot)$ as above, choose P a generator from G_1, given $e(P, *)$, where $*$ is an unknown point of G_1, the Inversion of Modified Weil Pairings (IWP) problem is to find $Q \in G_1$ such that

$$e(P, Q) = e(P, *).$$

(IWP Assumption) Given G_1, G_2 and $e(\cdot, \cdot)$ as above, choose P a generator from G_1, given $e(P, *)$, where $*$ is an unknown point of G_1. There is no probabilistic polynomial algorithm to solve the Inversion of Modified Weil Pairings problem with non-negligible advantage.

4 New Identity-based Group Signature Scheme

In this section the detailing description of the new group signature scheme is presented.

4.1 SETUP

This is a system generation algorithm. The group manager(GM) executes the following procedures:

(1) Choose p, q, G_1, G_2 defined in subsection 3.2.

(2) Choose two cryptographic hash functions:

$$H : \{0,1\}^* \mapsto G_1,$$

$$H_1 : \{0,1\}^* \times G_1 \mapsto G_1.$$

(3) Construct a bilinear function defined in subsection 3.2:

$$e : G_1 \times G_1 \longmapsto G_2.$$

(4) Select a generator element $P \in G_1$, therefore $e(P,P)$ is a generator element of G_2.

(5) Select an integer a from Z_q^* as the secret key of GM; Set $P_{pub} = aP$ as the public key of this group.

(6) Let a string $f \in \{0,1\}^*$ denoting an identifier (e.g. email address or IP address) of any group member of this group. GM computes $Q_f = H(f)$ as the public key of this member. It is easy to see we may not confirm the real identity of some group member by her email address or IP address.

(7) Let $\{0,1\}^*$ (a set of strings of any length) be the message space.

Therefore, the group public key of this group is: $PK = \{P, P_{pub}, e(\cdot,\cdot), H, H_1\}$ The master key of GM is $SK = a$.

4.2 Extract

Suppose a new member U_i wants to be an authorized member of this group. GM will communicate with U_i through a secure channel(e.g. secure against tampering, intruding, intercepting):

(1) U_i sends her identifier f_i to GM;

(2) GM computes $sk_i = aQ_{f_i}$, and then sends them to U_i.

(3) U_i regards respectively private value b(secretly chosen by herself) and her identifier f_i as her personal secret key and personal public key. Suppose $bf_i \equiv 1 \mathrm{mod} \varphi(n)$, where n is a product of two lager prime numbers.

(4) U_i and GM simultaneously execute a Schnorr identification protocol (see [15]). Thereafter, U_i obtains a credential t_i which is used to identify the membership of U_i.

(5) GM has a transcriptor: $trans = \{< f_i, t_i > \mid \text{for every authorized group member } U_{f_i}\}$.

This transcriptor is held only by GM.

(6) At the end of the communication, U_i becomes an authorized group member of this group. Her credential is t_i; her personal secret key is $\{b, sk_i\}$; and her personal public key is f_i. All these information are stored in a smart card held privately by U_i.

4.3 SIGN

This is a generation algorithm of group signatures. Suppose U_{f_i} is an authorized member of this group. Given a message $m \in M$, she performs the following algorithm:

(1) chooses randomly and uniformly x from Z_q^*, and sets $A = xP$.

(2) computes $B = x^{-1}sk_i + H_1(m, A)b$, where x^{-1} is the inversion of x in Z_q^*.

Therefore, the group signature on message m is $\{A, B, f_i\}$.

4.4 VERI

This is an algorithm of verification on alleged group signatures. Given a message m and its alleged group signature $\{A, B, f_i\}$, any verifier who holds public key can validate the validity of the group signature by carrying out the followings:

(1) computes $\alpha = e(f_i P_{pub}, Q_{f_i})$;

(2) computes $\beta = e(A, f_i B)$;

(3) computes $\gamma = e(A, H(m, A))$.

At the end of it, the verifier checks the equation:

$$\beta =^{?} \alpha\gamma \tag{1}$$

If the equality holds, then the verifier accepts: $\{A, B, f_i\}$ is a valid group signature on message m; otherwise, rejects it. On the one hand, by the group public key the verifier knows the signature coming from this group; On the other hand, by the personal public key the verifier knows this signature was generated by an authorized member U_{f_i} not by group manager.

4.5 REVEAL

This algorithm is only executed by the group manager GM. Given a message m and its corresponding valid group signature $\{A, B, f_i\}$, the group manager looks up the tanscriptor for the corresponding membership credential t_i. By the Schnorr identification protocol [15] and this group membership credential, the group manager can confirm the real identity of the group member.

5 Security Proofs and Analyses

This section we will come up with the security proofs and analyses of the new id-based group signature scheme. Specially we shall prove that the new id-based is secure against adaptive chosen message attack. On the other hand, some properties in the definition of group signatures will also be analyzed here.

5.1 Correctness

Theorem 1. *Given any message $m \in M$, if an authorized group member honestly computes the corresponding group signature $\{A, B, f_i\}$ on m by SIGN algorithm, then the VERI algorithm always accept it:*

$$VERI(m, \{A, B, f_i\}) \equiv 1. \tag{2}$$

Proof. Suppose $\{A, B, f_i\}$ is a group signature on message m honestly computed by an authorized member through SIGN algorithm, we shall prove it is valid. Therefore, it will always be accepted by VERI algorithm. In fact, $\{A, B, f_i\}$ has the following formula:

$$\{\, A = xPB = x^{-1}sk_i + H_1(m, A)b. \tag{3}$$

Therefore, $\beta = e(A, f_iB)$
$= e(A, f_ix^{-1}sk_i + f_i)bH_1(m, A)$
$= e(xP, f_ix^{-1}sk_i)e(xP, H_1(m, A))$
$= e(P, aQ_{f_i})^{xf_ix^{-1}}e(xP, H_1(m, A))$
$= e(f_iaP, Q_{f_i})e(xP, H_1(m, A))$
$= e(f_iP_{pub}, Q_{f_i})e(A, H_1(m, A))$
$= \alpha\gamma$. Hence, VERI algorithm always accepts the group signature.

5.2 Security against Adaptive Forgeability

Generally speaking, adaptive unforgeability (resp. adaptive forgeability)in group signatures satisfies that: Even if an adversary has oracle (ideal random algorithm) access to the group signing algorithm which provides valid group signatures on messages of the adversary's choice, the adversary cannot (resp. can)create a valid group signature on a message not previously queried.

Theorem 2. *Under the assumption of Elliptic curve Discrete Logarithm and the assumption of Inversion of Weil Pairings, the new id-based group signature scheme is secure against adaptive forgeability.*

Proof. We shall prove that the new id-based group signature scheme is secure against adaptive chosen message attacks.

Suppose **Adv** is a probabilistic polynomial time adversary that will forge valid group signatures to our new id-based group signature scheme.

First it is noted that **Adv** is not able to obtain the personal secret key of any authorized group member by observing the corresponding personal public key Q_{f_i} and the group public key PK. In fact,

(1) Due to the difficulty of Elliptic Curve Discrete Logarithm problems, **Adv** is not able to obtain a by solving $P_{pub} = aP$. Therefore, it is not able to work out $sk_i = aQ_{f_i}$.

(2) Due to the unknown factors of n, **Adv** is not able to figure out b by the relation of $f_ib \equiv 1 \bmod n$.

On the other hand, even though it is adaptive, **Adv** is not able return a valid group signature. In this case, we first assume that **Adv** is able to bring forward valid group signatures, then there will be a contradiction.

Adv would interact with GM, SIGN simulator, and hash oracle. The detailed descriptions of these interactions are as follows:
GM:

(1) **Adv** would choose freely a personal public key f_j of any authorized group member and interact with GM;

(2) GM randomly and uniformly selects $a^{'}$ from Z_q^* and sets $Q_{f_j} = a^{'}P$, $sk_{f_j} = a^{'}P_{pub}$, and then sets $H(f_j) = Q_{f_j}$.
SIGN simulator:

(1) Given any message m chosen by **Adv**, SIGN simulator will return a group signature with respect to f_j;

(2) By use of the results returned by **Adv** interacting with GM, SIGN simulator computes

$$\{A = xP, B = x^{-1}sk_{f_j} + f_j^{-1}H_1(m, A)\},$$

where x is chosen by SIGN simulator from Z_q^*.
HASH ORACLE:

For any message m chosen by **Adv** and the element A returned by SIGN simulator, HASH ORACLE defines $H_1(m, A) = gP$, where $g \in Z_q^*$. (It is known that P is a generator of G_1.)

In fact, we may regard **Adv**, GM, SIGN simulator and HASH ORACLE respectively as some probabilistic polynomial time algorithms. In the course of interacting with GM, SIGN simulator and HASH ORACLE, **Adv** would freely choose some messages and some personal public keys of authorized members. However, there is a limitation on the behavior of **Adv**; that is, as it forges a valid group signature (the corresponding message m_0) , the message m_0 has to be not queried in the course of interactions by **Adv** to obtain its corresponding valid group signature.

By the descriptions of the above three probabilistic polynomial time algorithms, for a new message m (not queried by **Adv**), due to the Theorem 1 in [13], we may with respect to public key f_i make use of the random transcripts of GM and SIGN simulator respectively

$$\sigma \text{ and } \psi$$

as the auxiliary inputs, and then run the probabilistic polynomial time algorithm **Adv** twice. At the same time, we use the different values of hash function $H_1(m, \cdot)$: h_1 and h_2. Therefore, due to the assumption on **Adv**(that is, it is able to output valid group signatures.), we can obtain two different valid group signatures on message m with respect to public key f_i:

$$A_1, B_1, f_i \tag{4}$$

and

$$A_1, B_2, f_i \tag{5}$$

Since we used the different hash values, it is easy to see

$$B_1 \neq B_2.$$

Therefore, due to the verification algorithm $VERI$, by the equation (5.3) we have:

$$e(A_1, f_i B_1) = e(f_i P_{pub}, Q_{f_i})\gamma_1; \tag{6}$$

By the equation (5.4) we have:

$$e(A_1, f_i B_2) = e(f_i P_{pub}, Q_{f_i})\gamma_2. \tag{7}$$

where

$$\gamma_1 = e(A_1, h_1);$$
$$\gamma_2 = e(A_1, h_2).$$

Therefore, we can by use of equation (5.5) and (5.6) respectively arrive at:

$$\frac{e(A_1, f_i B_1)}{e(A_1, f_i B_2)} = \frac{e(f_i P_{pub}, Q_{f_i})\gamma_1}{e(f_i P_{pub}, Q_{f_i})\gamma_2};$$

Hence,

$$e(A_1, f_i(B_1 - B_2)) = \gamma_1 \gamma_2^{-1};$$

By the computations of γ_1 and γ_2, and the randomness of h_1 and h_2, we may understand:

$$\gamma_1 \gamma_2^{-1}$$

is a random element of the finite group G_2.

Therefore, given a point A_1 in the finite group G_1, for any element g in G_2, we may use a probabilistic polynomial time algorithm to find:

$$F = f_i(B_1 - B_2)$$

such that:

$$e(A_1, F) = g.$$

where $g = \gamma_1 \gamma_2^{-1}$. Evidently, that contradicts the assumption of assumption of Inversion of Weil Pairings. Therefore, the theorem concludes.

5.3 Anonymity

In identity-based group signatures, the anonymity means that any user outside of the signing group cannot identify the membership of the original signer even though the user can check the validity of the group signature.

In this subsection, we discuss the anonymity property of the new identity-based group signature scheme. Given a valid group signature

$$\{A, B, f_i\},$$

since the group membership credential t_i is privately held by U_{f_i}, any user is not able to identify the real identification of U_{f_i}. On the other hand, because of the difficulty of elliptic curve discrete logarithm problem, any user is not able to work out t_i by use of the group public key.

5.4 Exculpability

Neither a group member nor the group manager can sign on behalf of other group members. In fact, due to the secure channel between authorized members and the group manager, $sk_i = aQ_{f_i}$ and $cert_i$ are secretly communicated. Additionally, the value b is privately held only by U_{f_i}. Therefore, for any authorized member U_{f_j}, she does not know the personal secret key $\{sk_i, b\}$ of the authorized member U_{f_i}. Hence, U_{f_j} cannot on behalf of U_{f_i} output a group signature A, B, f_i such that

$$e(A, f_i B) = e(f_i P_{pub}, Q_{f_i}) e(A, H_1(m, A)) \tag{8}$$

At the same time, the group manager GM cannot represent or personate U_{f_i} to output valid group signatures. In fact, b is secretly chosen by U_{f_i}. Therefore, due to the difficulty of integer factor problem, GM is not able to work out b from $bf_i \equiv 1 \mathrm{mod} \varphi(n)$.

5.5 Traceability

The group manager is always able to open a valid signature and identify the actual signer in case of disputes. Given a valid group signature $\{A, B, f_i\}$. By the group membership credential t_{f_i} (related to f_i) and the committed property of the Schnorr identification protocol, GM can then identify the real identification of the corresponding authorized group member.

6 Performance

When the new identity-based group signature scheme is put into practice for application, the performance is dominated by the signing algorithm and the verification algorithm. As to the verification algorithm, there are two point multiplications, one modulus multiplication, one hash function evaluation, and two bilinear pairing computations. Moreover, the verification makes use of the bilinearity of the pairings over elliptic curves. As to the signing algorithm, there are three point multiplications and one hash function evaluation. There is no pairing evaluation in the signature generation.

We note that there is no exponentiation (specially RSA exponentiation) calculations during the generation of signatures. Additionally, there is no exponentiation calculations during the verification of signatures. Previous to this new scheme, some group signature schemes need to compute exponentiations modulo a large RSA modulus. Therefore, the new scheme is efficient in terms of computation cost.

The group public key and group signatures are independent of the number of the authorized group members. Therefore, our scheme is suited to large groups. Especially, the new group signatures may be applied in mobile communications while the new scheme is in the setting of elliptic curves.

In order for application, some papers, for instance [4, 17], provide useful tools to deal with pairing evaluation, point multiplication or scalar multiplication, and hash function evaluation in the elliptic curve settings.

7 Conclusion

A novel identity-based group signature scheme is presented. It makes use of the bilinear pairings over elliptic curves. The size of the group public key is independent of the size of the underlying group. Also, the length of a group signature is independent of the number of the underlying group. In addition, the signing computation does not encompass RSA signatures. Therefore, the new scheme is claimed to be efficient. At the same time, the proof of security against adaptive forgeability is presented in this paper.

References

[1] G.Ateniese, J.Camenisch, M.Joye & G.Tsudik, *A pratical and provably secure coalition-resistant group signature scheme,* Advances in Cryptology-CRYPTO 2000, Springer-Verlag, LNCS 1880, 255-270, 2000.

[2] G.Ateniese & B. de Medeiros, *Anonymous E-prescriptions,* ACM Workshop on Privacy in the Electronic Society (WPES02), Sponsored by ACM SIGSAC, Washington DC, USA, 2002.

[4] P.S.L.M.Barreto, H.Y.Kim, B.Lynn & M.Scott, *Efficient algorithms for pairing-based cryptosystems,* Advances in Cryptology-Crypto 2002, Springer-Verlag, LNCS 2442, 354-368, 2002.

[5] D.Chaum & E.Van Heyst, *Group signatures,* EUROCRYPT 1991, LNCS 547, Springer-Verlag, 257–265, 1991.

[6] J.Camenisch & M. Michels, *A group signature scheme with improved efficiency,* Advances in Cryptology-ASIACRYPT 1998, Springer-Verlag, LNCS 1514, 160-174, 1998.

[7] L.Chen & T.P.Pedersen, *New group signature schemes,* Proceedings of EUROCRYPT 1994, Springer-Verlag, LNCS 950, 171-181, 1995.

[8] J.Camenish & M.Stadler, *Efficient group signature schemes for large groups,* Proceedings of CRYPTO 1997, Springer-Verlag, LNCS 1296, 410-424, 1997.

[9] F.Hess, *Efficient identity based signature schemes based on pairings,* K. Nyberg and H. Heys(Eds.), Selected Areas in Cryptography, SAC 2002 , Springer-Verlag, 310-324, 2003.

[10] K.Lauter, *The Advantages of Elliptic Curve Cryptography for wireless security.* IEEE Wireless Communications Magazine, IEEE Press, February 2004.

[11] H.Petersen, *How to convert any digital signature scheme into a group signature scheme,* Security Protocols Workshop 1997, 177-190, 1997.

[12] C. Popescu, *An efficient id-based group signature scheme,* Studia Universitatis Babes-Bolyai, Informatica, Vol. XLVII, November 2, 2002.

[13] D.Pointcheval & J.Stern, *Security arguments for digital signatures and blind signatures,* Journal of Cryptology, Springer-Verlag, 13(3), 361-396, 2000.

[14] A.Shamir, *Identity-based cryptosystems and signatures,* Proceedings of CRYPTO 1984, Springer-verlag, LNCS 196, 47-53, 1985.

[15] C.Schnorr, *Efficient signature generation by smart cards,* Journal of Cryptology, Springer-Verlag, 4(3), 239-252, 1991.

[16] D.Song, *Prcatical forward-secure group signature schemes,* Proceedings of ACM Symposium on Computer and Communication Security. ACM Press, 225-234, 2001.

[17] N.P.Smart & E.J.Westwood, *Point multiplication on ordinary elliptic curves over fields of characteristic three,* Applicable Algebra in Engineering, Communication and Computing, Vol 13, 485-497, 2003.

[18] Y.M.Tseng & J.K. Jan, *A novel id-based group signature scheme,* Proceedings of Workshop on Cryptology and Information Security 1998, Tainan, 159-164, 1998.

[19] C.K.Wu & V.Varadharajan, *Many-to-one cryptographic algorithms and group signatures,* Australian Computer Science Communications, Proceedings of the Twenty Second Australasian Computer Science Conference (ACSC'99), Jenny Edward (Ed.), Springer, 432-444, 1999.