International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:8, 2007

A Pairing-based Blind Signature Scheme with Message Recovery

Song Han and Elizabeth Chang

***Abstract*— Blind signatures enable users to obtain valid signatures for a message without revealing its content to the signer. This paper presents a new blind signature scheme, i.e. identity-based blind signature scheme with message recovery. Due to the message recovery property, the new scheme requires less bandwidth than the identity-based blind signatures with similar constructions. The scheme is based on modified Weil/Tate pairings over elliptic curves, and thus requires smaller key sizes for the same level of security compared to previous approaches not utilizing bilinear pairings. Security and efficiency analysis for the scheme is provided in this paper.**

***Keywords*:** Blind Signature, Message Recovery, Pairings, Elliptic Curves, Blindness.

I. Introduction

WITHthe development of electronic commerce, the preservation of the anonymity of users has been an imperative need. Blind signatures are one of the cryptographic tools which can provide such anonymity for users. Therefore, they are one important tool for electronic cash transmission since the way to ensure anonymity goes through the use of e-cash [9], [23]. A blind signature scheme is an interactive protocol which involves two entities, a Bank and a user. It enables a user to obtain a valid signature for a message m from a Bank without her seeing the message. If the Bank sees m and its signature at a later time, she can verify that the signature is genuine but she is unable to link the message-signature pair to a particular instance of the signing protocol which has led to this pair.

The concept of blind signatures was first proposed by Chaum [9] in 1982. It allows to secure electronic payment systems that protect a customer's privacy or anonymity. Therefore, blind signatures can be applied to secure e-coins and secure e-votings. Thereafter, some blind signature schemes were proposed [1], [4], [24].

Nyberg and Rueppel [22] introduced the general signatures with message recovery which has been adopted in the recent IEEE standards [17]. Just as what Nyberg and Rueppel reported, based on the same principles as DSA, a signature scheme can be constructed which achieves message recovery, but cannot be used as the RSA signature scheme for encryption by inter-changing the roles of the private and public transformations. The advantages are obvious: applications without a hash function are possible, smaller bandwidth for signatures of small messages, and direct use in other schemes such as identity-based public key systems or key agreement protocols. Thanks to their motivations, it is interesting to construct an identity-based blind signature scheme with message recovery.

The bilinear pairings [6], especially modified Weil/Tate pairings have been a useful tool for cryptographic protocols since Joux's work [18]. Due to the desirable use of the bilinear pairings in public key cryptography, identity based cryptography has been re-investigated since Shamir proposed the first identity-based cryptosystem [25]. Recently, some identity-based schemes based on pairings have been proposed. Interesting examples include Boneh and Franklin's id-based encryption from the Weil pairing [6], Hess's id-based signatures based on pairings [16], Han et al's committal deniable signatures [14] and undeniable signatures [15], Libert and Quisquater's undeniable signatures based on pairings [21], and Verhel's self-blindable credential certificates from pairings [27].

However, no blind signatures with message recovery based on pairings over elliptic curves has been proposed so far. The advantage of the blind signature schemes with message recovery is obvious in communication which requires the smaller bandwidth for signed messages, when compared with the same constructions except the message recovery. Therefore, it is interesting to construct a blind signature scheme with message recovery based on pairings over elliptic curves. This paper presents a new blind signature which has message recovery and is based on pairings over elliptic curves. As there have been many cryptographic designs that combine the bilinear pairings, we wish to fill the gap between the general blind signatures and the blind signatures with message recovery by utilizing bilinear pairings.

This paper proposes an id-based blind signature scheme with message recovery. The proposed scheme is motivated by the work of [3], [27]. From the perspective of both blind signatures and id-based cryptosystems from the Gap-Diffie-Hellman groups, the new scheme is comparable with [4].

The organization of the rest of the paper is as follows: In the next section, some computational preliminaries are presented. Section 3 provides the definition of blind signatures and id-based blind signatures with message recovery. Section 4 presents the description of the proposed scheme. Analysis of

[0]This work is supported by the Curtin Research Fellowship within the School of Information Systems, Curtin Business School, Curtin University of Technology.

[0]Dr. Song Han is with the School of Information Systems, Curtin Business School, Curtin University of Technology. GPO Box U 1987, Perth WA 6845, Australia. Phone: +61 8 9266 4488. Fax: +61 8 9266 3076. Email: song.han@cbs.curtin.edu.au.

[0]Prof. Elizabeth Chang is with the School of Information Systems, Curtin Business School, Curtin University of Technology. GPO Box U 1987, Perth WA 6845, Australia

the scheme is presented in section 5. Comparison with other blind signature schemes is presented in section 6. The last section concludes this paper.

II. Preliminary

A. Pairings over Elliptic Curves

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

$$y^2 = x^3 + 1. \quad (1)$$

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 the finite field F_{p^2}. Roughly speaking, an elliptic curve is a set of all points Q whose abscissa value and vertical value satisfy Equation (1).

The modified Weil pairing is a bilinear mapping from $G_1 \times G_1$ to G_2,

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

satisfying that the Elliptic Curve Discrete Logarithm (ECDL) problems are difficult in G_1 and the Inversion of Weil pairing (IWP) problems are difficult in G_2. All these requirements are needed in our new scheme and will be stated in the next section.

The modified Weil pairing $e : G_1 \times G_1 \to G_2$ 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-degeneracy: there exists at least one point $P \in G_1$ such that $e(P, P) \neq 1$.

(3) Efficient Computability: there are efficient algorithms to compute the bilinear pairing e.

B. Elliptic Curve Discrete Logarithms

(Elliptic Curve Discrete Logarithm Problem) *Given P as a generator of G_1, and 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) ECDLP Assumption implies there is no probabilistic polynomial time algorithm to solve the Elliptic Curve Discrete Logarithm problem with non-negligible advantage.

C. Inversion of Modified Weil Pairings

(Inversion of Modified Weil Pairings Problem) *Given G_1, G_2 and $e(\cdot, \cdot)$ as above, choose P a generator of G_1, given $e(P, *)$, here $*$ 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 implies that The IWP Assumption is that there is no probabilistic polynomial algorithm to solve the Inversion of Modified Weil Pairings problem with non-negligible advantage.

III. Model of Blind Signatures

The concept of blind signatures was first proposed by Chaum [9] in 1982 in order to deal with the following problem: A user Alice wants to obtain a digital signature on a message chosen by herself from the notary Bob, but Bob should not have any idea which message he signs. If he gets the message and the signature later, it must not be possible that Bob can find a relationship between some blinded and unblinded parameters.

The formal definition of a blind signature scheme is presented below [9], [19].

Blind Signatures A blind signature scheme consists of three algorithms and two parties (the user and the signer). The details are as follows:

(1) (System Key Generation) This is a probabilistic polynomial time algorithm (PPT algorithm). It takes a security parameter k as its input and outputs a pair of public key and private key $\{y, x\}$ for the blind signature scheme, where x is preserved secretly by the signer.

(2) (Generation of Blind Signatures) This is an interactive and probabilistic polynomial time protocol, which is operated by the user and the signer. The user first blinds the message m and obtains a new version m' of m, and then sends it to the signer. The latter utilizes her private key to sign on m' and obtains s', and then sends it to the sender. The sender unblinds it to obtain s which is a blind signature on m.

(3) (Verification of Blind Signatures) This is a deterministic polynomial time algorithm. Given a message m and its alleged blind signature s, anyone who knows the public key y can verify the validity of s. If it is valid, then the algorithm outputs '1'; otherwise outputs '0': $Veri(y, m, s) \equiv$
$\{ 1$, if s is a valid blind signature of m;
0, if s is not a valid blind signature of m.

Blindness We say a blind signature is of blindness if the signer's view (m', s') and the signature-message pair (m, s) are statistically independent. In some papers [9], [23], blindness is also called unlinkability.

A secure blind signature scheme must satisfy the following three requirements:

(1) Correctness: If the user and the signer both comply with the algorithm of blind signature generation, then the blind signature s will be always accepted, i.e.

$$Veri(y, m, s) \equiv 1.$$

(2) Unforgeability of Valid Blind Signatures: it is with respect to the user especially, i.e. the user is not able to forge blind signatures which are accepted by the algorithm of Verification of Blind Signatures.

(3) Blindness: While correctly operating one instance of the blind signature scheme, let the output be (m, s)(i.e. message-signature pair),, and the view of the protocol be $\tilde{v}$. At a later time, the signer is not able to link $\tilde{v}$ to (m, s).

IV. The Proposed Scheme

In this section, we present the proposed blind signature scheme with message recovery.

A. System Initialization

In this blind signature scheme, there is a trusted system authority **SA** which is responsible for the generation of the system parameters. The detailed steps are as follows:

(1) Let p be a sufficient large prime satisfying that: (1)$p \equiv$ 2mod3; (2)$p = 6q - 1$, where q is also a prime. Consider the equation

$$y^2 = x^3 + 1 \tag{2}$$

which defines elliptic curves E/F_p and E/F_{p^2}. G_1 is an additive group of order q of E/F_p, and G_2 a multiplicative group of q of $F^*_{p^2}$. (2) SA chooses a cryptographic hash function as in [7]

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

(3) SA chooses a bilinear pairing, i.e. modified Weil or Tate pairing $e(\cdot,\cdot)$ described as [8]. where:

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

(4) Choose a generator P of G_1 and a random number $a \in Z^*_q$. SA holds a secretly and publishes $P_{pub} = aP$.

(5) Let $f \in \{0,1\}^*$ represent an identifier of the signer, for instance, this identifier may be her email address or library card number, which is the public key in the identity-based blind signatures. In fact, in signing algorithm, $Q_f = H(f)$ which is the corresponding part of public key f will be viewed as the public key of signers. SA computes $SK = aQ_f$ and sends it (as a private key) to the signer. In order to avoid **SA**'s full control on the secret parameters, we can use some threshold secret sharing scheme to participate the **SA**.

(6) Let the message space be $M = Z^*_q$.

Therefore, the system public parameters are:

$$PK = \{P, P_{pub}, Q_f, e(\cdot,\cdot), H\}$$

and the signer's private key is $SK = aQ_f$.

B. Generation of Blind Signatures

This is an interactive probabilistic polynomial time algorithm. The user (Alice) and the signer (Bob) operate this algorithm interactively. Now Alice holds a message $m \in Z^*_q$ secretly. m may contain something important. Alice does not want Bob to know it; On the other hand, she needs the signature on m from Bob. So they do as follows:

(1) The signer Bob chooses $x \in Z^*_q$ randomly and uniformly, and computes $A = xP$. Then Bob sends A to Alice.

(2) The user Alice first chooses α and β randomly and uniformly from Z_q. Then she computes the following two elements:

$$B = e(\alpha P + \beta Q_f, P_{pub}) \cdot m \cdot e(A + P, P_{pub});$$

and

$$\tilde{m} = (B + \beta) \text{mod } q.$$

Afterwards, she sends $\tilde{m}$ to the signer Bob.

(3) After receiving $\tilde{m}$, the signer Bob computes

$$\tilde{S} = xP_{pub} + \tilde{m}SK.$$

Then he sends this value to Alice.

(4) After receiving $\tilde{S}$, Alice will compute $E = \tilde{S} + \alpha P_{pub}$.

(5) At the end of the generation of blind signatures, Bob will output

$$< \tilde{m}, A, \tilde{S} >$$

as the protocol view in this protocol. Alice will output

$$< m, (B, E) >$$

as the blind signature, i.e. (B, E) is the blind signature of message m.

C. Message-Recovery and Signature-Verification

This is a deterministic polynomial time algorithm operated only by the user Alice. Alice will first recover an alleged message m_0; then she will compare it with her original message m. If they are equal, she will accept the blind signature as valid; otherwise, rejects it. The algorithm is as follows: Given a message m and its corresponding alleged blind signature B, E:

(1) The user Alice first computes $F = e(E, P) \in G_1$.

(2) Alice then computes

$$m_0 = \frac{Be(Q_f, P_{pub})^{B \text{mod } q}}{Fe(P, P_{pub})}.$$

(3) Alice checks whether

$$m_0 =^? m(\text{mod } q).$$

If the equality holds, she will accept (B, E) as the valid blind signature of m; otherwise, she will reject it.

V. Security Evaluation and Analysis

This section we will provide the security evaluation and analysis for the proposed blind signature scheme. We will prove that the blind signature scheme with message recovery enjoys the following properties:

(1) Correctness; (2) Blindness; (3) Unforgeability. The third property guarantees that Alice cannot represent Bob to produce valid blind signatures for new messages. In addition, we will discuss the replay attack on the proposed scheme.

A. Correctness

Blind signature with message recovery means that any blind signature produced correctly by the proposed blind signing algorithm will always be accepted by the corresponding message-recovery and signature-verification algorithm. That is, it always holds

$$Veri(m, PK, (B, E)) \equiv 1 \tag{3}$$

if (B, E) is a valid blind signature of m with respect to public key PK.

Theorem 1 The proposed scheme has correctness.

Proof. In fact, if (B, E) is a blind signature produced correctly by the blind signing algorithm, then by the message-recovery and signature-verification algorithm we have:

$F = e(E, P)$
$= e(\tilde{S} + \alpha P_{pub}, P)$
$= e(xP_{pub} + \tilde{m}SK, P)e(\alpha P_{pub}, P)$
$= e(xP_{pub}, P)e(\alpha P_{pub}, P)e(\tilde{m}SK, P)$
$= e(xP, P_{pub})e(Q_f, aP)^{\tilde{m}}e(\alpha P_{pub}, P)$
$= e(A, P_{pub})e(\alpha P, P_{pub})e(Q_f, P_{pub})^{(B+\beta)\text{mod } q}$

Therefore,

$e(E, P)^{-1} \cdot B \cdot e(Q_f, P_{pub})^{B\text{mod } q}$
$= e(-A, P_{pub})e(-\alpha P, P_{pub})e(Q_f, P_{pub})^{-\beta}e(\alpha P + \beta Q_f, P_{pub}) \cdot m \cdot e(A + P, P_{pub})$
$= e(-\alpha P, P_{pub})e(Q_f, P_{pub})^{-\beta}e(\alpha P + \beta Q_f, P_{pub}) \cdot m \cdot e(P, P_{pub})$
$= e(Q_f, P_{pub})^{-\beta} \cdot m \cdot e(\beta Q_f, P_{pub}) \cdot e(P, P_{pub})$
$= m \cdot e(P, P_{pub})$

Therefore,

$m_0 = \frac{Be(Q_f, P_{pub})^{B(\text{mod } q)}}{Fe(P, P_{pub})}$
$= \frac{Be(Q_f, P_{pub})^{B(\text{mod } q)}F^{-1}}{e(P, P_{pub})}$
$= \frac{me(P, P_{pub})}{e(P, P_{pub})}$
$= m\text{mod } q$

Therefore, the correctness is proved.

B. Blindness

Blindness is one important property of the proposed blind signature scheme with message recovery. In fact, blindness means that the signer cannot figure out what's the value of the message he signs blindly during the process of the scheme. Therefore, blindness realizes the anonymity for the underlying protocol, especially for the user of the protocol. In the following, we will prove the new scheme has the blindness (i.e.unlinkability).

Theorem 2 The proposed scheme is of the blindness.

Proof. In order to prove the blindness of the scheme, we show that given any view *V* and any valid message-signature pair $(m, (B, E))$ with $B \in G_2$ and $E \in G_1$, there exists a unique pair of blinding factors α and β. Because the user chooses the blinding factors α and β at random, the blindness of the proposed scheme follows.

If the blind signature (B, E) of a message m has been generated during an instance of the scheme with view *V* consisting of $\tilde{m}$, $A = xP$, $x \in Z_q^*$, and $\tilde{S} = xP_{pub} + \tilde{m}SK$, then the following equation must hold for blinding factors α and β:

$$\tilde{m} = (B + \beta)\text{mod } q, \tag{4}$$

$$B = e(\alpha P + \beta Q_f, P_{pub}) \cdot m \cdot e(A + P, P_{pub}), \tag{5}$$

$$E = \tilde{S} + \alpha P_{pub}. \tag{6}$$

Because $\tilde{m}$, α and β are relatively prime to q, the blinding factors β and α can be uniquely determined by the first and third equation respectively:

$$\beta = (\tilde{m} + ((-B)\text{mod } q))(\text{mod } q) \tag{7}$$

$$\alpha = (\log_{P_{pub}}(E + (-\tilde{S})))(\text{mod } q) \tag{8}$$

The above formula of α is the elliptic curve discrete logarithm of $(E + (-\tilde{S})) \in G_1$ with respect to the base P_{pub}. In fact, we use $\alpha P_{pub} = E + (-\tilde{S})$ replacing α in the proof.

By substituting $\tilde{S} = xP_{pub} + \tilde{m}SK$, we obtain:
$e(P_{pub}, P)^{\alpha} \times e(Q_f, P_{pub})^{\beta} \times e(xP_{pub}, P)$
$= e(\alpha P_{pub}, P) \times e(\beta Q_f, P_{pub}) \times e(xP_{pub}, P)$
$= e(E + (-((B + \beta)SK)), P) \times e(\beta Q_f, P_{pub})$
$= (e(E + (-((B)SK)), P))\text{mod } q$

Therefore, we have:

$B = e(P_{pub}, P)^{\alpha} \times e(Q_f, P_{pub})^{\beta} \times e(xP_{pub}, P) \times m \times e(P_{pub}, P)$
$= e(E + (-((B)SK)), P) \times m \times e(P_{pub}, P).$

By using the verification equation in section 4.3, we have:

$m_0 = \frac{B \times e(Q_f, P_{pub})^{B\text{mod } q}}{e(E, P) \times e(P, P_{pub})}$
$= \frac{e(E+(-((B)SK)), P) \times m \times e(P_{pub}, P)e(Q_f, P_{pub})^{B\text{mod } q}}{e(E, P)}$
$= \frac{e(E, P) \times m \times e(Q_f, P_{pub})^{B\text{mod } q}}{e(SK, P)^{B\text{mod } q} \times e(E, P)}$
$= m(\text{mod } q)$

where $e(E, P) \neq 0(\text{mod } p)$, and $e(P_{pub}, P) \neq 0(\text{mod } p)$.

Therefore, there exists a unique pair of blinding factors α and β for any view *V* and any valid message-signature pair $(m, (B, E))$ with $B \in G_2$ and $E \in G_1$. Because the user chooses the blinding factors α and β at random, the blindness of the proposed scheme follows.

C. Unforgeability

Why do we discuss the unforgeability with respect to the user? Because the user can obtain more useful information about the underlying blind signature scheme than any other adversary party (except **SA**). So in the following it is assumed that we can construct an algorithm which will use the user as a subroutine to attack the proposed scheme. In the end, here comes a contradiction between the prerequisite of the theorem and our proof assumption.

Theorem 3 (The *Unforgeability*) The proposed blind signature scheme with message recovery has the unforgeability with respect to the user under the difficulty of the underlying Inversion of Modified Weil Pairings problems and the Elliptic Curve Discrete Logarithm problems.

Proof.

Here we will use the reduction to absurdity during the proof. We first construct a probabilistic polynomial time algorithm

and use **W** to denote this algorithm. We then use **W** to solve the Inversion of Modified Weil Pairings problem. Therefore, a contradiction will be concluded.

W is admitted to use the user as a subroutine, as well as making queries to the message signing simulator(i.e. PPT algorithm) of the proposed scheme. At the same time, the following requirements need to be satisfied:

Suppose the user has a random transcript:

$$LIST_{SENDER}.$$

On it there store all the data transmitted between the user and signer during the process of interaction of the blind signature scheme. All these data include the data the user receives from the message signing simulator, as well as all the data computed and randomly chosen by the sender herself.

We also let the message signing simulator have a random transcript:

$$LIST_{SIGNER}.$$

On it there store all the data transmitted between the message signing simulator and the user during the process of interaction of the blind signature scheme. All these data include the data the message signing simulator receives from the user, as well as all the data computed and secretly chosen by the sender herself.

For the above two random transcripts, the probabilistic polynomial time algorithm **W** is able to borrow some data from them. That is to say, **W** can fully access to $LIST_{SENDER}$ and obtain the data from it. At the same time, **W** is able to only limitedly access to $LIST_{SIGNER}$ and obtain a little data limitedly but not fully.

In order to complete the proof, we can assume **W** is able to forge valid blind signature which can be accepted by the Message-Recovery and Signature-Verification algorithm of the scheme. Without loss of generality, we may assume **W** has constructed two different valid blind signatures for a message m:

$$(B_1, E_1) \text{and } (B_2, E_2) \tag{9}$$

Since they are valid blind signatures, it is admitted to assume

$$E_1 = \tilde{S_1} + \alpha_1 P_{pub},$$
$$E_2 = \tilde{S_2} + \alpha_2 P_{pub},$$
$$\tilde{S_1} = \tilde{m_1} SK + xP_{pub},$$
$$\tilde{S_2} = \tilde{m_2} SK + xP_{pub},$$

where $x \in Z_q$ is a random element which **W** obtains from the message signing simulator. And α_1 and α_2 are two elements from Z_q^* chosen by the user. $\tilde{m_1}$ and $\tilde{m_2}$ are computed by the user. All these 4 elements exist in $LIST_{SENDER}$. Therefore, **W** is able to access to them. Thus,

$$E_1 - E_2$$
$$= (\tilde{S_1} - \tilde{S_2}) + (\alpha_1 - \alpha_2) P_{pub}$$
$$= (\tilde{m_1} - \tilde{m_2}) SK + (\alpha_1 - \alpha_2) P_{pub}.$$

Therefore,

$$(\tilde{m_1} - \tilde{m_2}) SK = (E_1 - E_2) - (\alpha_1 - \alpha_2) P_{pub},$$

Therefore,

$$SK = (\tilde{m_1} - \tilde{m_2})^{-1} ((E_1 - E_2) - (\alpha_1 - \alpha_2) P_{pub}).$$

Consequently, according to (or by) the System Initialization algorithm of the blind signature scheme, we can solve a solution $X = SK$ to the following equation:

$$e(X, P) = y \text{ where } X \text{ is an unknown element.} \tag{10}$$

where y is the already known value $e(Q_f, P_{pub})$. It is easy to see that this contradicts the difficulty of Inversion of Modified Weil Pairing problems. Therefore, the theorem is concluded.

VI. Efficiency Analysis

In this section we will analyze the proposed scheme from the computational and communication point of view.

In the blind signature generation of the new scheme the signer needs to compute three scalar multiplications in G_1, while the user needs to compute three scalar multiplications in G_1, two pairing evaluation (In fact, the two evaluation can be computed by one pairing evaluation). In the message-recovery and verification, the user needs to compute one pairing evaluation (the other two can be precomputed in case of packing verifications), one exponentiation in G_2.

From the point of communication cost, the new scheme does not need to transmit the signed message together with its corresponding blind signatures, while [4] does need.

At the same time, some computational techniques in [8], [10], [7], [26], [13] can be utilized when the proposed scheme is implemented for practical uses.

VII. Conclusion

This paper has presented a new blind signature scheme, i.e. identity-based blind signatures with message recovery. This new scheme needs smaller bandwidth in contrast to previous identity-based blind signatures. On the other hand, this new scheme is based on modified Weil or Tate pairings over elliptic curves. Therefore, it has smaller key sizes in the same level of security comparing with previous blind signatures which were not based on pairings.

Acknowledgment

The authors would present theirs thanks to the anonymous reviewers of the International Program Committee within this international conference.

REFERENCES

[1] M.Abe & E.Fujisaki, *How to date blind signatures.* Advances in Cryptology-Asiacrypt 1996, LNCS 1163, pp.244-251. 1996.

[2] G. Ateniese & B. de Medeiros, *Efficient group signatures without trapdoors.* 246-268 Advances in Cryptology-Asiacrypt 2003, LNCS 2894, pp.246-268, 2003.

[3] G. Ateniese & B. de Medeiros, *A provably secure Nybery-Rueppel siganture variant with applications.* Cryptology ePrint Archive, Report 2004/093.

[4] A. Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme.* Practice and Theory in Public Key Cryptography- PKC'2003, LNCS 2567, Springer-Verlag, Pp.31-46, 2003.

[5] D. Boneh & X. Boyen, *Short signatures without random oracles.* Proceedings of EUROCRYPT 2004, LNCS 3027, pp.56-73, 2004.

[6] D.Boneh & M.Franklin, *Identity-based encryption from the Weil pairing,* Proceedings of CRYPTO 2001, Springer-verlag, LNCS 2139, 213-229, 2001.

[7] S.L.Barreto & Y.Kim, *Fast hashing onto elliptic curves over fields of characteristic-3,* Cryptology ePrint Archive, Report 2001/098.

[8] 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, pp.354-368, 2002.

[9] D.Chaum, *Blind signatures for untraceable payments.* Advances in Cryptology-Crypto 1982, Plenum, NY, pp.199-203, 1983.

[10] K.Eisentraeger, K.Lauter & P.L.Montgomery, *An efficient procedure to double and add points on an elliptic curve,* Cryptology ePrint Archive, Report 2002/112.

[11] G. Frey, M. Müller, & H. Rück, *The Tate pairing and the Discrete Logarithm applied to elliptic curve cryptosystems,* IEEE Transactions on Information Theory 45(5), 1717-1719, 1999.

[12] P. Horster, M. Michels & H. Petersen, *Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications.* Advances in Cryptology- Asiacrypt 1994, Springer-Verlag, LNCS 917, pp.224-237, 1995.

[13] S. D. Galbraith, K. Harrison, & D. Soldera, *Implementing the Tate pairing,* Algorithmic Number Theory Symposium-ANTS-V, Springer-Verlag, LNCS 2369, 324-337, 2002.

[14] S. Han & Liu, W.Q., 2004, Committal Deniable Signatures over Elliptic Curves. Proceedings of the 23rd IEEE International Performance Computing and Communication Conference, pp. 833-840, Phoenix, Arizona, USA, IEEE Press, 2004.

[15] S. Han, Yeung, K.Y. & Wang, J. 2003, Identity-based Confirmer Signatures from Pairings over Elliptic Curves. Proceedings of ACM Electronics Commerce 2003, pp. 262-263, 2003.

[16] 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.

[17] Standard speciafications for public key cryptography. IEEE P1363-2000, 2000.

[18] A.Joux, *A one-round protocol for tripartite Diffie-Hellman,* Algorithm Number Theory Symposium - ANTS-IV, Springer-Verlag, LNCS 1838, 385-394, 2000.

[19] A.Juels, M.Luby, R.Ostrovsky, *Security of blind digital signatures (Extended Abstract).* Advances in Cryptology-Crypto 1997, Springer-Verlag, LNCS 1294, pp.150-164, 1997.

[20] B. Libert & Jean-Jacques Quisquater, *New identity based signcryption schemes from pairings,* Proceedings of IEEE Information Theory Workshop 2003, 2003.

[21] B.Libert & Jean-Jacques Quisquater, *Identity based undeniable signatures.* Topics in Cryptology- CT-RSA 2004, LNCS 2964, pp.112-125, 2004.

[22] K. Nyberg & Rainer A. Rueppel, *A new signature scheme based on the DSA giving message recovery.* Proceedings of ACM Conference on Computer and Communications Security 1993, ACM Press, pp.58-61, 1993.

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

[24] D. Pointcheval & J.Stern, *Provably secure blind signature schemes.* Advances in Cryptology-Asiacrypt 1992, Springer-Verlag, LNCS 1163, pp.252-265, 1992.

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

[26] 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.

[27] Eric R. Verheul, *Self-blindable credential certificates from the Weil pairing.* Advances in Cryptology - Asiacrypt 2001, Springer-verlag, LNCS 2248, pp.533-551, 2001.