A New Blind Identity-Based Signature Scheme with Message Recovery

Hassan Elkamchouchi and Yasmine Abouelseoud*
Faculty of Engineering, Alexandria University, Egypt
email address*: yasmine.abouelseoud@gmail.com

Abstract- **Anonymity of consumers is an essential functionality that should be supported in e-cash systems, locations based services, electronic voting systems as well as digital rights management system. Privacy protection is an important aspect for wider acceptance of consumers of DRM systems. The concept of a blind signature is one possible cryptographic solution, yet it has not received much attention in the identity-based setting. In the identity-based setting, the public key of a user is derived from his identity, thus simplifying certificates management process compared to traditional public key cryptosystems. In this paper, a new blind identity-based signature scheme with message recovery based on bilinear pairings on elliptic curves is presented. The use of bilinear pairings over elliptic curves enables utilizing smaller key sizes, while achieving the same level of security compared to other schemes not utilizing elliptic curves. The scheme achieves computational savings compared to other schemes in literature. The correctness of the proposed scheme is validated and the proof of the blindness property is provided. Performance and other security related issues are also addressed.**

I. INTRODUCTION

The privacy issue of DRM systems [1] is one of the most intensely discussed concerns in public debates by advocates and citizens representatives. Consumer representatives point out that DRM systems have the potential to generate, transmit and store vast quantities of data on personal use of copyrighted works, representing an unprecedented level of monitoring to consumers activities. The key objective of consumer representatives is to achieve legitimate anonymous access DRM systems. In pay-TV applications, an authorized user expects to enjoy watching his favorite shows and sports events without his interests being revealed to outsiders. In tourist location-based mobile services [2], the tourist surely prefers to get advice on places to visit without his privacy being jeopardized. In both cases anonymity may be achieved through the use of anonymous identifiers. Other typical scenarios involving the need for anonymity include e-cash payment systems [3,4,5,6] and electronic voting systems [7].

Blind signatures are one of the cryptographic tools which can provide such anonymity for users. The concept of a blind signature scheme was introduced by Chaum [8], since then many blind signature schemes have been presented in the literature [9,10,11,12]. A blind signature scheme is an interactive protocol allowing Bob to obtain a valid signature for a message *m* from a signer Alice without her seeing the message or its signature. If Alice sees *m* and its signature later, she can verify that the signature is genuine, but she is unable to link the message-signature pair to the particular instance of the signing protocol which had led to this pair. This intuitively corresponds to signing a document with your eyes closed. If you happen to see the document and signature later on, you can indeed verify that the signature is yours, but you will probably have great difficulty in recollecting when or for whom you signed the original document.

At first this concept seems a little strange- why would you want to sign something without seeing it? It turns out, when applied properly, this notion has some nice applications where anonymity is a big issue. The document may be an electronic coin, an electronic ballot, an identifier to enable access to a digital good with intellectual copyright safeguards, etc..

Identity-based cryptosystems are becoming increasingly common those days. In a traditional public key cryptosystem, the association between a user's identity and his public key is obtained through a digital certificate issued by a certifying authority (CA). If Alice wants to send a signed message to Bob, first she obtains a digital certificate for her public key from a CA. Alice then signs a message using her private key and sends the signed message along with her certificate to Bob. Bob first verifies the validity of the certificate by checking the certificate revocation list published by the CA, then he verifies the signature using public key in the certificate.

Identity-based cryptosystems were introduced by Shamir in 1984 [13] to get rid of public key certificates by allowing the user's public key to be the binary sequence corresponding to an information identifying him in a non-ambiguous way (e-mail address, social security number,...). This kind of system allows to avoid trust problems encountered in certificate based public key infrastructures (PKIs): there is no need to bind a public key to its owner's identity since those are one single thing. These systems involve trusted authorities called private key generators (PKGs) whose task is to compute users' private keys from their identity information (users do not generate their key pairs themselves). Several practical identity-based signature schemes (IBS) have been devised since 1984, but a satisfactory identity-based encryption scheme (IBE) only appeared in 2001 [14]. It was devised by Boneh and Franklin and cleverly uses bilinear maps (the Weil or Tate pairing) over supersingular elliptic curves. Since then, many identity-based cryptosystems have been developed based on the bilinear pairings [15]. Just to name a few, we have Hess's identity-based signature [16], Libert and Quisquarter undeniable signatures [17] as well as signcryption schemes in [18] and Verheul's self-blindable credential certificates presented in [19].

In this paper, a new blind signature scheme in the identity-based setting is presented. The scheme is based on the modified Weil pairing over elliptic curves. Moreover, the scheme is simple and the communication overhead during

the blind signature generation phase is relatively low. Furthermore, bandwidth reductions are achieved as the scheme supports message recovery. Thus, there is no need to append the message to the signature for verification purposes. The proposed blind signature scheme is validated and its security is proven under the assumption of the hardness of the computational Diffie-Hellman problem.

The organization of the rest of the paper is as follows. In the next section, the definition of blind signatures is presented. Section 3 presents a protocol for issuing anonymous identifiers to legitimate users of a DRM system. In Section 4, basic terminology used throughout the paper is provided. In Section 5, an identity-based signature scheme with message recovery is presented. Sections 6,7 present the proposed blind signature scheme and its efficiency analysis, respectively. Section 8 provides proofs of security of the proposed scheme. Finally, Section 9 concludes the paper.

II. BLIND SIGNATURE STRUCTURE

The formal definition of a blind signature is presented below.

Blind Signatures: A blind signature scheme [8] consists of three algorithms and two parties (the recipient and the signer). The details are as follows.

1. Setup: This is a probabilistic polynomial time algorithm. It takes a security parameter *k* as its input and outputs a pair of public key *y* and private key *x* for the blind signature scheme.
2. Blind Signature Generation: This is an interactive and probabilistic polynomial time protocol, which is operated by the recipient 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 *m'* and obtains *s'* and sends it to the recipient. The recipient then unblinds it to obtain *s* which is a blind signature on *m*.
3. Verify: This is a deterministic polynomial time algorithm. Given a message *m* and its alleged blind signature *s*, anyone who knows the public key of the signer can verify the validity of *s*. If it is valid, then the algorithm outputs '1'; otherwise outputs '0'.

The blindness property of a signature scheme may be formally defined as follows: A blind signature scheme possesses the *blindness* property, sometimes referred to as unlinkability property, if the signer's view (*m',s'*) and the message-signature pair (*m*,*s*) are statistically independent.

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

1. Correctness: If the recipient and the signer both comply with the algorithm of blind signature generation, then the blind signature *s* will always be accepted.

2. Unforgeability of Valid Blind Signatures: The recipient is not able to forge blind signatures which are accepted by the verification algorithm of blind signatures.

3. Blindness: While correctly operating one instance of the blind signature scheme, let the output be (*m*,*s*) and the view of the protocol $\tilde{v}$. At a later time, the signer is unable to link $\tilde{v}$ to (*m*,*s*).

III. ISSUING ANONYMOUS IDENTIFIERS

Blind signatures present a cryptographic solution to the problem of constructing anonymous access DRM systems. This is achieved through the use of anonymous identifiers, i.e. identifiers that are not linkable to the identities of their owners. In order to issue an anonymous identifier, the legitimate user and the access control system should carry out the following procedure:

1. The access control system should publish a collection of valid identifiers $\{id_1, id_2, \cdots, id_n\}$.
2. The user should prove his identity to the access control system through some identification protocol.
3. The user randomly selects one of the published valid identifiers id_j.
4. The user blinds the chosen identifier id_j and sends the blind version id_j^* to the access control system.
5. The access control system signs id_j^* to obtain s^*, which is then sent to the legitimate user requesting the anonymous identifier.
6. The user unblinds the message-signature pair (id_j^*, s^*) to obtain a valid signature s on the desired identifier id_j.

When the legitimate user later on requests to access the digital good, he presents the pair (id_j, s) to the access control system. The access control system in turn validates its signature on id_j and access is allowed if the validation procedure succeeds, otherwise access is denied.

IV. BASIC DEFINITIONS AND TERMINOLOGY

This section includes the basic terminology used throughout the rest of the paper.

A. Bilinear Pairing

Many efficient identity-based encryption and signature schemes in the literature are based on the use of bilinear pairings, which are briefly defined below [20] .

Consider two groups G_1 (additive) and G_2 (multiplicative) of the same prime order *q*. A bilinear map $e: G_1 \times G_1 \to G_2$ satisfying the following properties is needed.

1- Bilinearity: $\forall\, P,Q \in G_1, \forall\, a,b \in F_q^*$, we have $e(aP,bQ) = e(P,Q)^{ab}$, $e(P+R,Q) = e(P,Q)\, e(R,Q)$.

2- Non-degeneracy: For any point $P \in G_1$, we have $e(P,Q) = 1$ for all $Q \in G_1$ iff $P = \mathrm{O}$

3- Computability: There exists an efficient algorithm to compute $e(P,Q), \forall\, P,Q \in G_1$.

B. Bilinear Pairings over Elliptic Curves

The modified Weil pairing and the Tate pairing [14] are admissible instantiations of bilinear pairings. The modified Weil pairing settings are briefly described below.

Let p be a sufficiently large prime that satisfies: (1) $p \equiv 2 \mod 3$; (2) $p = lq - 1$, where q is also a large prime. Let *E* be the elliptic curve defined by the equation

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

over F_p . Define $E(F_p)$ to be the group of points on *E* defined over F_p . Let $P \in E(F_p)$ be a point of order *q* and let G_1 be the subgroup of points generated by *P*. Set G_2 to be the subgroup of $F^*_{p^2}$ of order *q*. The modified Weil

pairing is thus defined by $e: G_1 \times G_1 \to G_2$ satisfying the conditions of a bilinear pairing.

The advantage of schemes based on bilinear pairings over elliptic curves is that they require smaller key sizes for the same level of security compared to previous approaches not utilizing elliptic curves.

C. Map-to-Point Hash Function

Consider a hash function $H_1: \{0,1\}^* \to G^*_1$. As suggested in [14], it is sufficient to have a hash function $H_1: \{0,1\}^* \to A$ for some set A and an encoding function $L: A \to G^*_1$. In case of using modified Weil pairings, we have that the set A is F_p and the encoding function L is called Map-to-Point.

Again, let p be a prime satisfying $p \equiv 2 \mod 3$ and $p = lq - 1$, where q is also a prime. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$ over F_p. Let G_1 be the subgroup of points on E of order q. Suppose we already have a hash function: $H_1: \{0,1\}^* \to F_p$. Algorithm Map-to-Point works as follows on input $y_0 \in F_p$:

1. Compute $x_0 = (y_0{}^2 - 1)^{1/3} = (y_0{}^2 - 1)^{(2p-1)/3} \in F_p$
2. Let $Q = (x_0, y_0) \in E(F_p)$ and set $Q_{ID} = lQ \in G_1$
3. Output Map-to-Point(y_0) = Q_{ID}

This algorithm is needed in the schemes given below.

D. Security Assumptions

The security of the schemes defined below relies on the hardness of the following problems:

The Computational Diffie-Hellman Problem(CDHP): Given a group G_1 of prime order q, and a generator P of G_1, the CDHP is to compute abP, given (P, aP, bP)

The Bilinear Diffie-Hellman Problem (BDHP): Given two groups G_1 and G_2 of the same prime order q, a bilinear map $e: G_1 \times G_1 \to G_2$ and a generator P of G_1, the BDHP is to compute $e(P,P)^{abc}$, given (P, aP, bP, cP)

V. An Identity-Based Signature Scheme with Message Recovery

The proposed blind signature scheme is a blind version of the following identity-based signature scheme which is an adaptation of Nyberg-Rueppel scheme to the identity-based setting.

The scheme consists of the following four algorithms: (*Setup*, *Extract*, *Sign*, *Verify*).

Setup: The private key generator (PKG) decides on a bilinear pairing $e: G_1 \times G_1 \to G_2$ and P an arbitrary generator of G_1. He then chooses $s \in_R (Z/qZ)^\times$ as his secret key and computes the global public key $P_{pub} = sP$. The PKG also selects a Map-to-Point hash function $H_1: \{0,1\}^* \to G^*_1$. He then publishes the system parameters:

$$params = \langle G_1, G_2, e, P, P_{pub}, H_1 \rangle$$

Extract: Given the public identity information *ID* of a new user, the PKG computes the corresponding secret key as $d_{ID} = sQ_{ID}$, where $Q_{ID} = H_1(ID)$ plays the role of the corresponding public key.

Sign: To sign a message $m \in \{0,1\}^*$ using the secret key d_{ID}, the signer picks a random integer $k \in (Z/qZ)^\times$ and computes:

1. $r = m\, e(P,P)^k$
3. $S = rd_{ID} + kP$

The signature σ is the pair: $\langle r, S \rangle \in G_1 \times (Z/qZ)^\times$

Verify: To verify the signature $\sigma = \langle r, S \rangle$ of an identity *ID* on a message *m* calculate

1. $Q_{ID} = H_1(ID)$
2. $m^* = \dfrac{r\, e(Q_{ID}, P_{pub})^r}{e(S,P)}$
3. Accept the signature if and only if $m = m^*$.

The correctness of the above scheme may be easily validated according to the following arguments.

$$\frac{r\, e(Q_{ID}, P_{pub})^r}{e(S,P)} = \frac{m\, e(P,P)^k\, e(sQ_{ID}, P)^r}{e(kP + rd_{ID}, P)}$$

$$= \frac{m\, e(P,P)^k\, e(rd_{ID}, P)}{e(kP,P)\, e(rd_{ID}, P)} = m$$

In the above scheme, the signing phase requires one pairing operation, namely $e(P,P)$ which could be pre-computed, one exponentiation in G_2, one point addition and two scalar multiplications in G_1. The verification phase requires two pairing operations, one Map-to-Point hash operation and one exponentiation in G_2.

VI. The Proposed Blind Identity-Based Signature Scheme with Message Recovery

In this section, a new blind identity-based signature scheme with message recovery is proposed. Signature schemes with message recovery are of special interest for secure, authenticated message transfer over low-bandwidth channels. There is no need to transmit the message itself along with the signature for verification. This is because only a valid signature could be used to reproduce an illegible message. The PKG runs the setup and extract algorithms as discussed in the previous section. We suggest to set the bilinear pairing to be the modified Weil pairing.

In order to sign a message *m* blindly by a signer whose identity is *ID*, the recipient and signer should follow the scenario given below.

Recipient

Sends a signature request to the signer

Signer

1. Picks a random integer $k \in (Z/qZ)^\times$
2. Computes $X = kP$ and sends it to the recipient

Recipient

3. Picks $\alpha, \beta \in (Z/qZ)^\times$ at random
4. Computes $r = m\, e(\alpha P + \beta X, P)$
5. A blind version of the message $\tilde{m} = r\beta^{-1}$ is sent to the signer.

Signer

6. Computes $\tilde{S} = X + \tilde{m}\, d_{ID}$

Recipient

7. Computes $S = \beta \tilde{S} + \alpha P$

The signature on the message *m* is the pair $\sigma = \langle r, S \rangle$. The verification process is the same as that described in the previous section.

VII. Efficiency of the Proposed Scheme

In the blind signature generation phase of the new scheme, the signer needs to compute two scalar multiplications and one point addition in G_1. The recipient needs to compute three scalar multiplications and two point additions in G_1, one pairing evaluation and one inversion operation in G_2.

In the verification phase, two pairing evaluations (one of which $e(Q_{ID}, P_{pub})$ could be precomputed for frequently communicating parties) and an exponentiation operation in G_2 are required. These requirements are advantageous over those of the scheme proposed in [22].

VIII. Proof of Correctness

In this section the correctness of the proposed scheme is presented, that is, any blind signature $\sigma = \langle r, S \rangle$ on a message *m* correctly produced by the proposed blind signing algorithm will always be accepted by the verification algorithm.

Theorem 1: The pair $\sigma = \langle r, S \rangle$ is a valid signature of the message *m*.

Proof:

The validity of the signature $\sigma = \langle r, S \rangle$ can be easily shown as follows.

$$\frac{r\, e(Q_{ID}, P_{pub})^r}{e(S,P)} = \frac{m\, e(\alpha P + \beta X, P)\, e(rd_{ID}, P)}{e(\beta \tilde{S} + \alpha P, P)}$$

$$= \frac{m\, e(\alpha P + \beta X, P)\, e(rd_{ID}, P)}{e(\beta \tilde{S}, P)\, e(\alpha P, P)}$$

$$= \frac{m\, e(\beta X, P)\, e(rd_{ID}, P)}{e(\beta \tilde{m}\, d_{ID} + \beta X, P)}$$

$$= \frac{m\, e(rd_{ID}, P)}{e(\beta\, \beta^{-1} rd_{ID}, P)} = m$$

IX. Security Analysis

The security analysis of the proposed scheme proceeds in two steps. First, we prove the blindness property of the scheme. This is followed by the proof of unforgeability.

A. Proof of Blindness

Blindness or unlinkability is an important property of the proposed scheme. In order to prove the blindness of the scheme, we show that given any view *V* and any message-signature pair (m, σ), there exists a unique pair of blinding factors α and β. Since the recipient chooses the blinding factors at random, the blindness of the scheme follows.

Theorem 2: The proposed protocol is a blind signature scheme, i.e. possesses the blindness property.

Proof:

If the blind signature $\sigma = \langle r, S \rangle$ of the message *m* has been generated during an execution of the protocol with view *V* consisting of *X*, $\tilde{m} = r\beta^{-1}$ and $\tilde{S} = \tilde{m} d_{ID} + X$, then the following equations must hold for α and β:

$$r = m\, e(\alpha P + \beta X, P) \quad (1)$$

$$\tilde{m} = r\, \beta^{-1} \quad (2)$$

$$S = \beta \tilde{S} + \alpha P \quad (3)$$

Since $\tilde{m}$, α and β are relatively prime to *q*, the blinding factors α and β are uniquely determined by the last two equations.

$$\beta = r\, \tilde{m}^{-1} \mod q$$

$$\alpha = \log_P (S - \beta \tilde{S}) \bmod q$$

The above formula for α involves the elliptic curve discrete logarithm of $(S - \beta \tilde{S}) \in G_1$ with respect to the base *P*. In fact, we can use αP in the rest of the proof instead.

By substituting the values of αP and β in the right hand side of the last equation (1) and using the verification equation

$$m = \frac{r\, e(Q_{ID}, P_{pub})^r}{e(S,P)}$$

as well as $\tilde{S} = X + \tilde{m}\, d_{ID}$ we obtain the following results

$$m\, e(\alpha P + \beta X, P) = \frac{r\, e(Q_{ID}, P_{pub})^r}{e(S,P)}\, e(\alpha P + \beta X, P)$$

$$= \frac{r\, e(rd_{ID}, P)\, e(S - \beta \tilde{S} + \beta X, P)}{e(S,P)}$$

$$= r\, e(rd_{ID}, P)\, e(-\beta \tilde{S} + \beta X, P)$$

$$= r\, e(rd_{ID}, P)\, e(-\beta \tilde{m} d_{ID} - \beta X + \beta X, P)$$

$$= r\, e(rd_{ID}, P)\, e(-\beta \tilde{m} d_{ID}, P)$$

$$= r\, e(rd_{ID}, P)\, e(-r\, \tilde{m}^{-1} \tilde{m} d_{ID}, P)$$

$$= r\, e(d_{ID}, P)^r\, e(d_{ID}, P)^{-r}$$

Thus, the unique solution of the last two equations satisfies the last equation. Since the blinding factors α and β are unique and chosen at random during the protocol, the blindness property of the proposed scheme follows.

B. Proof of Unforgeability

The unforgeability property of the scheme will be discussed with respect to the recipient [23]. This is because the recipient can obtain more useful information about the underlying blind signature scheme than any other adversary.

Theorem 3: The proposed blind signature scheme possesses the unforgeability property with respect to the recipient under the assumption of the hardness of the computational Diffie-Hellman problem.

Proof:

We first assume that we can construct a probabilistic polynomial time algorithm *A* which can create forged signatures of the signer. We then use *A* to solve the computational Diffie-Hellman problem. Therefore, a contradiction is concluded.

Algorithm *A* is admitted to use the recipient as a subroutine, as well as being admitted to make queries to the message signing simulator (a probabilistic time algorithm) of the proposed scheme. Moreover, the following requirements need to be satisfied.

Suppose the recipient has a random transcript $LIST_{RECIPIENT}$. On this list, all the data transmitted between the recipient and the signer during the process of interaction of the blind signature scheme are recorded. All these data include the data the recipient gets from the message signing

simulator as well as the data computed and those randomly chosen by the recipient itself.

Assume also that the message signing simulator has a random transcript $LIST_{SIGNER}$. On this list, we store the data the message signing simulator receives from the recipient as well as the data computed and secretly chosen by the signer itself.

For the above two random transcripts, the probabilistic time algorithm A has full access to $LIST_{RECIPIENT}$ but has only limited access to $LIST_{SIGNER}$.

In order to complete the proof, we can assume that algorithm A is able to forge valid blind signatures which can be accepted by the verification algorithm. Without loss of generality and applying the forking lemma, assume that A has successfully constructed two different valid blind signatures for a message m:

$$\sigma_1 = \langle r_1, S_1 \rangle \quad \text{and} \quad \sigma_2 = \langle r_2, S_2 \rangle$$

Since they are valid blind signatures, it is admissible to assume that

$$S_1 = \beta_1 \tilde{S}_1 + \alpha_1 P$$

$$S_2 = \beta_2 \tilde{S}_2 + \alpha_2 P$$

$$\tilde{S}_1 = X + \tilde{m}_1 \, d_{ID}$$

$$\tilde{S}_2 = X + \tilde{m}_2 \, d_{ID}$$

where X is a random element that A obtains from the message signing simulator. As for α_1 and α_2, these are two elements randomly chosen by the recipient. Finally, $\tilde{m}_1$ and $\tilde{m}_2$ are computed by the recipient. All the four elements α_1, α_2, $\tilde{m}_1$ and $\tilde{m}_2$ exist in $LIST_{RECIPIENT}$, which A has full access to. Thus, we have

$$\begin{aligned} S_1 - S_2 &= (\tilde{S}_1 - \tilde{S}_2) + (\alpha_1 - \alpha_2)\, P \\ &= (\tilde{m}_1 - \tilde{m}_2) d_{ID} + (\alpha_1 - \alpha_2)\, P \end{aligned}$$

Therefore, we arrive at

$$(\tilde{m}_1 - \tilde{m}_2) d_{ID} = (\beta_1 S_1 - \beta_2 S_2) - (\alpha_1 - \alpha_2)\, P$$

Consequently, we can compute d_{ID} as follows

$$d_{ID} = (\tilde{m}_1 - \tilde{m}_2)^{-1} ((\beta_1 S_1 - \beta_2 S_2) - (\alpha_1 - \alpha_2)\, P)$$

Thus, according to the system initialization algorithm of the blind signature, we are able to solve an instance of the CDH problem, namely, given $(P, Q_{ID} = aP, P_{pub} = sP)$ it is possible to compute $d_{ID} = sQ_{ID} = saP$. Therefore, a contradiction is reached and the theorem is concluded.

In other words, in order to solve an instance of the CDH problem, (P, aP, bP), the CDH solver runs the system setup procedure of the blind signature scheme and sets P_{pub} to aP and runs algorithm A, the forger, on an identity whose public key is $Q_{ID} = bP$. If A succeeds in the forgery process, a solution to the CDH problem is achieved.

X. Conclusions

In this paper, a new identity-based blind signature scheme has been proposed. The work is motivated by the importance of blind signatures as a cryptographic primitive essential in protocols that guarantee anonymity of users. This is particularly of interest in DRM systems, electronic cash systems, electronic voting systems and location-based mobile services that are becoming common those days. Anonymous identifiers may be used to protect the privacy of users of DRM systems. Blind signatures present a practical tool for issuing such identifiers. The proposed scheme is a blind signature scheme with message recovery and consequently achieves bandwidth savings. Since the proposed scheme is identity-based, the user's public key is easily extracted from his identification information. This eliminates the certificates for public keys needed in traditional public key cryptosystems.

The correctness of the proposed scheme has been validated. Security proofs for the blindness property and unforgeability have been developed. Performance assessment is also provided.

References

[1] N. Duff et al., "Digital Rights Management and Consumer Acceptability", Technical Report of INDICARE Project, December 2004.

[2] H. Qi, D. Wu and P. Khosla, "A Mechanism for Personal Control over Mobile Location Privacy", Proceedings of IEEE/ACM First International Workshop on Broadband Wireless Services and Applications, BroadWISE 2004.

[3] S. Brands, "Untraceable Cash in Wallets with Observers", In Advances in Cryptology- CRYPTO 1993, Springer-Verlag, LNCS 773, pp. 302-318, 1994.

[4] P. Wayner, "Digital Cash: Commerce on the Net", MIT Academic Press, 1996.

[5] Z. Ramzan, "Group Blind Digital Signatures: Theory and Applications", M.Sc. thesis at the Massachusetts Institute of Technology, 1999.

[6] A. Lysyanskaya and Z. Ramzan, "Group Blind Signatures: A Scalable Solution to Electronic Cash", In Proceedings of the International Conference on Financial Cryptography, 1998.

[7] A. Fujioka, T. Okamoto and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", In Advances in Cryptology- ASIACRYPT 1992, Springer-Verlag, LNCS 718, pp. 244-251, 1992.

[8] D. Chaum, "Blind Signatures for Untraceable Payments", In Advances in Cryptology, CRYPTO 1982, Plenum, NY, pp. 199-203, 1983.

[9] D. Pointcheval and J. Stern, "Provably Secure Blind Signature Schemes", In Advances in Cryptology- ASIACRYPT 1992, Springer-Verlag, LNCS 1163, pp. 252-265, 1992.

[10] D. Pointcheval and J. Stern, "New Blind Signatures Equivalent to Factorization", In Proceedings of the 4th ACM Conference on Computer and Communications Security, pp. 92-99, Zurich, Switzerland, 1997.

[11] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", In G. Brassard (ed.), In Proceedings of CRYPTO 1989, Springer-Verlag, LNCS 435, pp. 239-252, 1990.

[12] T. Okamoto, "Provable, Secure and Practical Identification Schemes and Corresponding Signature Schemes", In Advances in Cryptology- CRYPTO 1992, Springer-Verlag, LNCS 740, pp. 31-53, 1992.

[13] A. Shamir, "Identity-based Cryptosystems and Signatures", In Proceedings of CRYPTO 1984, Springer-Verlag, LNCS 196, pp. 47-53, 1985.

[14] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairings", In Proceedings of CRYPTO 2001, Springer-Verlag, LNCS 2139, 213-229, 2001.

[15] P. Barreto, H. Y. Kim, B. Lynn and M .Scott, "Efficient Algorithms for Pairing-based Cryptosystems", In Advances in Cryptology- CRYPTO 2002, Springer-Verlag, LNCS 2442, pp. 354-368, 2002.

[16] F. Hess, "Efficient Identity-based Signature Schemes based on Pairings", In Selected Areas in Cryptography, SAC 2002, K. Nyberg and H. Heys (eds.), Springer erlag, 310-324, 2003.

[17] B. Libert and J. Quisquater, "Identity-based Undeniable Signatures, In Topics in Cryptology CT-RSA 2004, LNCS 2964, pp. 112-125, 2004.

[18] B. Libert and J. Quisquater, "New Identity-based Signcryption Schemes from Pairings", In Proceedings of the IEEE Information Theory Workshop 2003, 2003.

[19] E. Verheul, "Self-blindable Credential Certificates from the Weil Pairings", In Advances in Cryptology- ASIACRYPT 2001, Springer-Verlag, LNCS 2248, pp. 533-551, 2001.

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

[21] M. Bellare and P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”, In Proceedings of the 1st ACM Computer and Communications Security, pp. 62-73, 1993.
[22] S. Han and E. Chang, “A Pairing-based Blind Signature with Message Recovery”, In International Journal of Information Technology, Vol. 2, No. 4, 2005.
[23] D. Pointcheval and J. Stern, “Security Arguments for Digital Signatures and Blind Signatures”, In Journal of Cryptology 13(3), pp. 361-396, 2000.