WEB ENGINEERING AND APPLICATIONS
Editors: J. Mishra and P. K. J. Mohapatra

Published by Narosa Publishing House, New Delhi, India

A NOVEL ECDLP-BASED BLIND SIGNATURE SCHEME WITH AN ILLUSTRATION

Debasish Jena, Sanjay Kumar Jena, Banshidhar Majhi, and Saroj Kumar Panigrahy

Department of Computer Science & Engineering
National Institute of Technology Rourkela, 769 008, India
debasishjena@hotmail.com, skjena@nitrkl.ac.in, bmajhi@nitrkl.ac.in, skp.nitrkl@gmail.com

ABSTRACT

Blind signature allows a requester to obtain signature from a signer on any document in such a way that, the authority learns nothing about the message that is being signed. Due to the blindness and untraceability properties of Blind Signature Scheme, it can be used in cryptographic applications such as web based e-voting, digital cash etc. In this paper, a novel blind signature scheme based on Elliptic Curve Discrete Logarithm Problem has been proposed. The model has been explained using a customer-and-bank example and the proof of correctness has been made.

KEYWORDS: *Blind Signature, Elliptic Curve, Digital Signature, RSA.*

1. INTRODUCTION

With growing importance of sender privacy in various schemes such as digital cash, e-voting protocol, blind signature schemes are gaining momentum. Blind signature is a form of digital signature in which the signer doesn't have authority over the message which is sent by a requester, and also a third party can verify the signature without knowing the secrets of both the parties (requester & signer) that are involved in signature. In such a scenario, the services need to be authenticated and secure. Non-repudiation is one of the vital aspects where the requester and the service providers can be prohibited of denying the action made on the transaction made between them. Signature scheme is the most widely used mechanism for this purpose. But in some applications like e-voting, e-cash etc., the requester needs to get the authentication in the message from the signer without really exposing the message content to the signer [2, 3]. For the aforesaid purpose, Blind Signature Scheme (BSS) was introduced by David Chaum in 1982 [4], where the content of a message is blinded before signature and sent to the signer. The signer signs on the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer's public key. This procedure can be well explained with an example taken from the familiar world of paper documents. The paper analogue of a blind signature can be implemented with carbon-paper-lined envelopes. Putting a signature on the outside of such an envelope leaves a carbon copy of the signature on a slip of paper within the envelope [4]. Any BSS must satisfy the following properties [4, 5, 15]:

- ***Correctness*****:** the correctness of the signature of a message signed through the signature scheme can be checked by anyone using the signer's public key.

- ***Authenticity*:** a valid signature implies that the signer deliberately signed the associated message.
- ***Unforgeability*:** only the signer can give a valid signature for the associated message.
- ***Non-reusability*:** the signature of a document can not be used on another document.
- ***Non-repudiation*:** the signer can not deny having signed a document that has valid signature.
- ***Integrity*:** ensure the contents have not been modified.
- ***Blindness*:** the content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.
- ***Untraceability*:** the signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

BSS suggested by Camenisch et al. [1] is based on Discrete Logarithm Problem. Harn [7] has proved that this scheme does not satisfy the untraceability property. Similarly, another BSS suggested by Mohammed et al. [13] is based on ElGamal. Hwang et al. [8] has proved that this scheme does not satisfy the correctness property. In this scheme, when the requester obtained the blinded signature from the signer, he/she could not unblind it to acquire the desired signature. In this paper, we propose a new untraceable BSS based on Elliptic Curve Discrete Logarithm Problem (ECDLP). The proposed scheme is based on a variation of the ElGamal signature scheme which satisfies all the properties of BSS.

The organization of this paper is as follows. In the Section 2, the concept of Blind signature based on RSA is discussed. Basic concept of elliptic curve (EC) is discussed in Section 3. In Section 4, discussion on Elliptic Curve Digital Signature Algorithm (ECDSA) based on variation of ElGamal signature scheme has been made and subsequently, the proposed scheme is elaborated using an illustration of customer-and-bank example. The validity of the proposed BSS has been proved in section 5. Finally, Section 6 describes the concluding remarks.

2. BLIND SIGNATURE BASED ON RSA

Let us consider standard RSA public key cryptosystems, in which the public key is denoted as a pair (e, n) and the private key is denoted as a number d. Here, the modulus n is a product of two large (secret) primes p, q and the private key d is the multiplicative inverse of e modulo $(p-1)(q-1)$. For the security of the RSA system it is assumed that both p and q are sufficiently large (e.g., > 200 digit numbers), such that it is infeasible to find either the factorization of n or the private key d, given only the public key (e, n). Let a requester sends a message $m \in [0, n]$ to be signed by a signer using Chaum's BSS using RSA [2]. The different phases are explained below in detail.

2.1. Blinding Phase

The requester picks a blinding factor r, which is a random integer between 0 and n, and computes the value:

$$m' = m\, r^e \bmod n \qquad \ldots (1)$$

The requester sends m' to the signer. The m' is the message to be signed by the signer as in case of general signature without knowing the original message m.

2.2. Signing Phase

The signer signs the message m' using his/her private key d as below:

$$s' = m'^{d} \bmod n \quad \ldots (2)$$

The signer returns s' to the requester as the blind signature.

2.3. Extraction Phase

The requester after receiving the s', he/she extracts the signature s as follows:

$$s = s'/r \bmod n = m^{d} \bmod n \quad \ldots (3)$$

$[\because s' = (m')^{d} \bmod n = (mr^{e})^{d} \bmod n = m^{d} r^{ed} \bmod n]$

So the requester finds the actual signature of m as (m, s) which satisfies the Eqn. 3. Figure 1 depicts the Chaum's BSS in terms of message communicated between the requester and the signer.

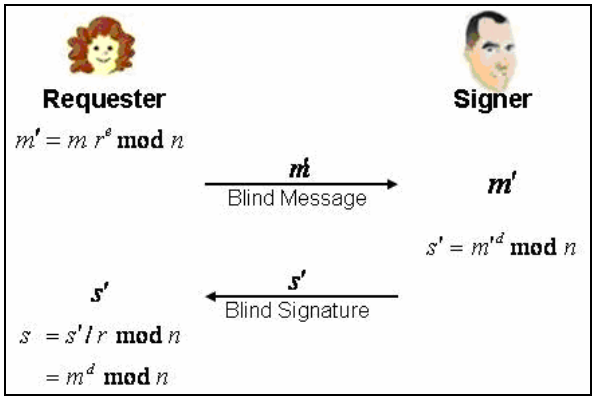

Figure 1. Chaum's Blind Signature Scheme based on RSA

3. ELLIPTIC CURVE OVER FINITE FIELD

The use of Elliptic Curve Cryptography (ECC) was initially suggested by Neal Koblitz [10] and Victor S. Miller [12] and after that many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite fields have some advantages. One is the much smaller key size as compared to other cryptosystems like RSA or Diffie-Hellman, since: (a) only exponential-time attack is known so far if the curve is carefully chosen [9], and (b) elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithms are broken. ECC is also more computationally efficient than the first-generation public key systems such as RSA or Diffie-Hellman [6].

3.1. Elliptic Curve Groups over F_q

A non-super singular Elliptic curve E over F_q can be written as:

$$E: \quad y^2 \bmod q = (x^3 + ax + b) \bmod q \qquad \ldots (4)$$

where $(4a^3 + 27b) \bmod q \neq 0$.

The points $P = (x, y)$ where $x, y \in F_q$. $P(x, y)$ that satisfy the Eqn. 4 together with a "point of infinity" denoted by O form an abelian group $(E, +, O)$ whose identity element is O.

3.1.1. Adding Distinct Points P *and* Q

The negative of the point $P = (x_1, y_1)$ is the point $-P = (x_1, -y_1)$. If $P(x_p, y_p)$ and $Q(x_q, y_q)$ are two distinct points such that P is not $-Q$, then

$$P + Q = R \qquad \ldots (5)$$

where $R = (x_r, y_r)$.

$\therefore s = (y_p - y_q)/(x_p - x_q) \bmod q$ where $s.$ is the slope of the line passing through P and Q.

$x_r = (s^2 - x_p - x_q) \bmod q$ and $y_r = (-y_p + s(x_p - x_r)) \bmod q$.

3.1.2. Doubling the Point P

Provided that y_p is not 0,

$$2P = R(x_r, y_r) \qquad \ldots (6)$$

$\therefore s = ((3x_p^2 + a)/(2y_p)) \bmod q$

$x_r = (s^2 - 2x_p) \bmod q$ and $y_r = (-y_p + s(x_p - x_r)) \bmod q$

The elliptic curve discrete logarithm problem is defined as follows [14].

Definition 1: Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

4. PROPOSED UNTRACEABLE BLIND SIGNATURE

In this section, firstly the variation of ElGamal digital signature and its subsequent extension using ECDLP has been discussed. Subsequently we shall propose a novel efficient and low computation blind signature based on ECDLP with an illustration of customer-and-bank example.

4.1. Digital Signature Using ECDLP

The proposed ECDSA is a variant of ElGamal Digital Signature [11]. The EC variant provides smaller key sizes for similar security level. Initially the curve domain parameters (q, FR, a, b, G, n, h) must be agreed upon by both the signer and the receiver, where q is the field order, FR is the field representation for F_q, G is the generator group, n is a large prime, and h is the division of N, the order of $E(F_q)$) to n. Here The signer must have a key pair suitable for elliptic curve cryptography, consisting of a private key d_B (a randomly selected integer in the interval $[1, n-1]$) and a public key Q where $Q = d_B G$. When the signer wants to send a signed message m to the receiver, he/she must generate a digital signature (r, s) as follows:

Select k randomly between $[1, n-1]$ and generate R, r, and s as:

$$R = kG \quad \ldots (7)$$

where $R = (x_R, y_R)$

$r = x_R \bmod n$ and $r != 0$

$s = md_B - kr \bmod n$ and $s != 0$

After receiving (r, s) from the signer, the receiver can verify the correctness of the signature on the message by using following equation:

$$mQ = sG + rR \quad \ldots (8)$$

4.1.1. Correctness

The verifier only verifies the pair (r, s) and message m by using the Eqn. 8. The correctness of the Eqn. 8 is as follows:

$s = md_B - kr$

$\Rightarrow md_B = s + kr$

$\Rightarrow md_B G = sG + rkG$

$\Rightarrow mQ = sG + rR$

4.2. Blind Signature Based on ECDLP

In the proposed scheme the requester requests signature from the signer and the signer issues blind signature to the requester without knowing the content of the message. The protocol consists of following five phases:

(a) Initialization phase
(b) Requesting phase
(c) Signing phase
(d) Extraction phase
(e) Verification phase

In the initialization phase, the system's parameter is defined, and the signer publishes the necessary information and sends partially blind signature to the requester. To obtain a signature, the requester submits an encrypted version (blinds the message) of the message to the signer in the requesting phase. In the signing phase, the signer computes the blind signature of the message, and then sends the result back to the requester. In the extraction phase, the requester extracts the signature from the result received in the extraction phase. Lastly, anyone can verify the legitimacy of the digital signature in the verifying phase. The underlying principles of the new BSS are explained using a customer-and-bank example where the customer (the requester) needs a document to be signed by the bank (the signer) without disclosing contents of the document. The different phases of the signature scheme are explained below.

4.2.1. Initialization Phase

Initially Bank should do the following. Let (q, FR, a, b, G, n, h) are the curve parameters, d_B and Q are respectively, private and public keys of the signer, where $Q = d_B G$. The bank randomly chooses $\tilde{k}_1, \tilde{k}_2$, l_1 and l_2 and calculates $\tilde{r}_1$ and $\tilde{r}_2$ as follows.

$$\begin{aligned} \tilde{R}_1 &= \tilde{k}_1 G \\ \tilde{R}_2 &= \tilde{k}_2 G \end{aligned} \quad \ldots (9)$$

where, $\tilde{R}_1 = (\tilde{x}_{r_1}, \tilde{y}_{r_1})$ and $\tilde{R}_2 = (\tilde{x}_{r_2}, \tilde{y}_{r_2})$

$\tilde{r}_1 = \tilde{x}_{r_1} \bmod n$ and $\tilde{r}_1 != 0$

$\tilde{r}_2 = \tilde{x}_{r_2} \bmod n$ and $\tilde{r}_2 != 0$

The Bank sends $(\tilde{R}_1, \tilde{R}_2, l_1, l_2)$ to customer.

4.2.2 Requesting Phase

After receiving $(\tilde{R}_1, \tilde{R}_2, l_1, l_2)$, the customer should request for signature by computing the values as follows. The customer randomly selects four integers a, b, w and z such that w is relatively prime to z i.e., $\gcd(w, z) = 1$. According to Extended Eculid's algorithm there exist two integers e and d such that $ew + dz = 1$ [16]. The signer's secret values are (e, w, d, z, a, b). The customer computes R_1 and R_2 as,

$$\begin{aligned} R_1 &= \tilde{R}_1 w a l_1, \quad R_1 = (x_{r_1}, y_{r_1}) \\ R_2 &= \tilde{R}_2 z b l_2, \quad R_2 = (x_{r_2}, y_{r_2}) \end{aligned} \quad \ldots (10)$$

where, $r_1 = x_{r_1} \bmod n$ and $r_2 = x_{r_2} \bmod n$

After calculating r_1 and r_2 the customer blinds the message m as follows:

$$\tilde{m}_1 = em\tilde{r}_1 r_1^{-1} r_2^{-1} a^{-1} \bmod n$$
$$\tilde{m}_2 = em\tilde{r}_2 r_1^{-1} r_2^{-1} b^{-1} \bmod n \quad \ldots (11)$$

The customer sends the blind messages $\tilde{m}_1$ and $\tilde{m}_2$ to Bank for signature.

4.2.3. Signing Phase

In this phase, the Bank computes blind signature $\tilde{s}_1$ and $\tilde{s}_2$ by using received blind messages $\tilde{m}_1$ and $\tilde{m}_2$ as follows.

$$\tilde{s}_1 = d_B \tilde{m}_1 - \tilde{r}_1\, \tilde{k}_1\, l_1 \bmod n$$
$$\tilde{s}_2 = d_B \tilde{m}_2 - \tilde{r}_2\, \tilde{k}_2\, l_2 \bmod n \quad \ldots (12)$$

Then the Bank sends the blind signatures $\tilde{s}_1$ and $\tilde{s}_2$ to the requester.

4.2.4. Extraction Phase

Customer should do the followings to recover the real signature s after receiving the blinded signature $\tilde{s}$ from the Bank. After receiving the blind signatures $\tilde{s}_1$ and $\tilde{s}_2$, the customer extracts the actual signature as follows.

$$s_1 = \tilde{s}_1 \tilde{r}_1^{-1} r_1 r_2\, wa \bmod n$$
$$s_2 = \tilde{s}_2 \tilde{r}_2^{-1} r_1 r_2\, zb \bmod n \quad \ldots (13)$$

$$s = s_1 + s_2, \qquad R = R_1 + R_2, \qquad r = (r_1\ r_2) \bmod n \quad \ldots (14)$$

The pair (r, s) is the valid digital signature of message m.

4.2.5. Verification Phase

Any one can verify the legitimacy of the digital signature (R, r, s) of message m by using Eqn. 8. The proposed scheme is diagrammatically shown in Figure 2.

5. PROOF OF PROPERTIES OF THE PROPOSED SCHEME

In this section we discuss the correctness and some of the important properties of our proposed blind signature scheme.

5.1. Correctness

The correctness of our scheme can be easily verified as follows. The verifier has only digital signature (R, r, s) of message m for verification. The signer computes the s by adding s_1 and s_2.

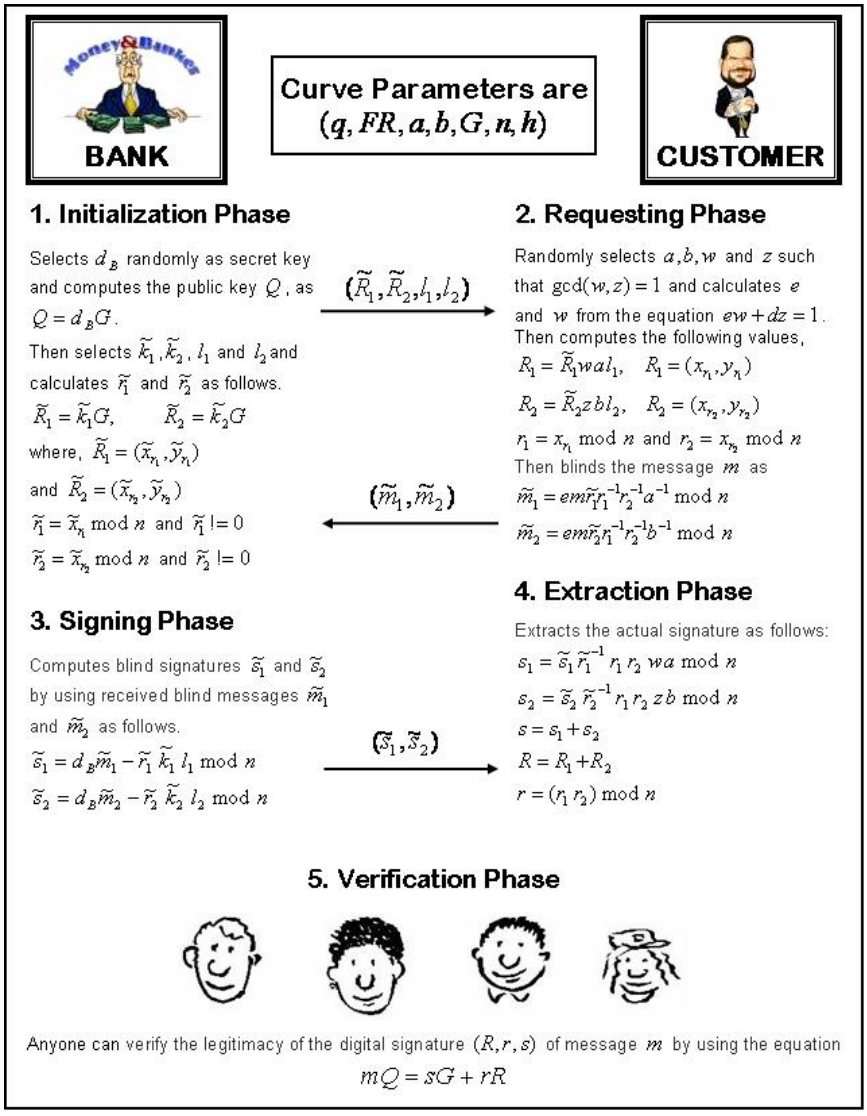

Figure 2. New Blind Signature Scheme based on ECDLP

$$
\begin{aligned}
s &= s_1 + s_2 \\
&= \tilde{s}_1 \tilde{r}_1^{-1} r_1 r_2 wa + \tilde{s}_2 \tilde{r}_2^{-1} r_1 r_2 zb \\
&= \left(d_B \tilde{m}_1 - \tilde{r}_1 \tilde{k}_1 l_1\right) \tilde{r}_1^{-1} r_1 r_2 wa + \left(d_B \tilde{m}_2 - \tilde{r}_2 \tilde{k}_2 l_2\right) \tilde{r}_2^{-1} r_2 zb \\
&= \left(d_B \left(em\tilde{r}_1 r_1^{-1} r_2^{-1} a^{-1}\right) - \tilde{r}\tilde{k}_1 l_1\right) \tilde{r}_1^{-1} r_1 r_2 wa + \left(d_B \left(dm\tilde{r}_2 r_1^{-1} r_2^{-1} b^{-1}\right) - \tilde{r}_2 \tilde{k}_2 l_2\right) \tilde{r}_2^{-1} r_1 r_2 zb
\end{aligned}
$$

$$= d_B emw - \tilde{k}_1 l_1 r_1 r_2 wa + d_B dzm - \tilde{k}_2 l_2 r_1 r_z zb$$
$$= d_B m(ew + dz) - r_1 r_2 (\tilde{k}_1 l_1 wa + \tilde{k}_2 l_2 zb)$$
$$= d_B m - r(\tilde{k}_1 l_1 wa + \tilde{k}_2 l_2 zb) \qquad [\because ew + dz = 1 \text{ and } r = r_1 r_2]$$

Finally,

$$s = d_B m - r(\tilde{k}_1 l_1 wa + \tilde{k}_2 l_2 zb) \qquad \ldots (15)$$

Now multiplying both sides of the Eqn. 15 by generator G we have,

$$sG = d_B mG - r(\tilde{k}_1 l_1 wa + \tilde{k}_2 l_2 zb)G$$
$$\Rightarrow sG = mQ - r(\tilde{k}_1 l_1 waG + \tilde{k}_2 l_2 zbG)$$
$$\Rightarrow sG = mQ - r(R_1 + R_2)$$
$$\Rightarrow sG = mQ - rR$$
$$\Rightarrow mQ = sG + rR$$

5.2. Blindness

As the requester randomly selects six blinding factors $(e_x, w_x, d_x, z_x, a_x, b_x)$ to compute the blind message $(\tilde{m}_1, \tilde{m}_2)$, so from the blind messages $(\tilde{m}_1, \tilde{m}_2)$, the signer can not compute the original message as it is based on ECDLP.

5.3. Untraceability

The signer cannot link the signature to the message as the signer only has the information, i.e., $(\tilde{m}_{1x}, \tilde{m}_{2x}, \tilde{r}_{1x}, \tilde{r}_{2x}, \tilde{k}_{1x}, \tilde{k}_{2x}, \tilde{s}_{1x}, \tilde{s}_{2x}, l_{1x}, l_{2x})$ for all blinded messages, where $x = 1,2,\cdots,n$. If the requester reveals the signatures of a message and its signature, i.e., (m_x, r_x, s_x, R_x) to public, from this information the signer can only compute two values $\tilde{e}_x \tilde{a}_x^{-1}$ and $\tilde{d}_x \tilde{b}_x^{-1}$, corresponding to each information stored $(\tilde{m}_{1x}, \tilde{m}_{2x}, \tilde{r}_{1x}, \tilde{r}_{2x}, \tilde{k}_{1x}, \tilde{k}_{2x}, \tilde{s}_{1x}, \tilde{s}_{2x}, l_{1x}, l_{2x})$ where,

$\tilde{e}_x \tilde{a}_x^{-1} = \tilde{m}_{1x} m_x^{-1} \tilde{r}_{1x}^{-1} \tilde{r}_x \bmod q$ and $\tilde{d}_x \tilde{b}_x^{-1} = \tilde{m}_{2x} m_x^{-1} \tilde{r}_{2x}^{-1} \tilde{r}_x \bmod q$.

Therefore, without the knowledge of the secret information $(e_x, w_x, d_x, z_x, a_x, b_x)$ of the requester, anyone cannot trace the blind signature.

6. CONCLUSION

This paper suggests a secure and efficient blind signature scheme based on the ECDLP. The scheme has been proved to be correct, blind and untraceable. As the scheme is based on ECDLP, it achieves the same security with fewer bits key as compared to RSA. In addition, it has low-computation

requirements. It can also be applied to applications like e-voting systems and untraceable digital cash where anonymity of the signer is a requirement.

REFERENCES

[1] Camenisch J., Piveteau J., and Stadler M., *Blind signatures based on discrete logarithm problem*, in Advancesin Cryptology, EUROCRYPT'94, pp. 428–432, Lecture Notes in Computer Science, 950, 1994.

[2] Chaum D., *Blind Signature Systems*, U.S. Patent 4,759,063, 19 Jul 1988.

[3 Chaum D., *Blind signatures for untraceable payments,* Advances in cryptology, CRYPTO'82, Lect. Notes Computer Science, (Springer-Verlag, 1998), pp. 199-203.

[4] Chaum D., Fiat A. and Naor M., *Untraceable electronic cash*, Advances in cryptology, CRYPTO'RX, Lect. Notes Computer Science, (Springer-Verlag, 1990), pp. 319-327.

[5] Fan Chun-I, Chen W.K., and Yeh Y. S., *Randomization enhanced Chaum's blind signature scheme*, Computer Communications, vol. 23, pp. 1677–1680, 2000.

[6] Hankerson Darrel, Menzes Alferd, Vanstone Scott, *Guide to Elliptic Curve Cryptography,* Springer, 2003.

[7] Harn L., *Cryptanalysis of the blind signatures based on the discrete logarithm problem*, IEEE Letters, pp. 1136–1137, 1995.

[8] Hwang Min-Shiang and Lai Yuan-Liang Tang Yan-Chi, *Comment on A Blind Signature Scheme Based On ElGamal Signature*, Technical Report CYUT-IM-TR-2001-010, CYUT, Aug. 2001.

[9] Koblitz N., *CM-Curves with Good Cryptographic Properties*, Proceeding of Crypto'91,1992.

[10] Koblitz N., *Elliptic Curve Cryptosystems*, Mathematics of Computation ,48, pp.203-209, 1987.

[11] Menezes A., Oorschot P. van, and Vanstone S., *Handbook of Applied Cryptography*, CRC Press, 1996.

[12] Miller V., *Uses of Elliptic Curve in Cryptography*, Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences,218, Springer – Verlag, 1986, pp.417-426.

[13] Mohammed E., Emarah A. E., and El-Shennawy K., *A blind signatures scheme based on ElGamal signature*, in IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, pp. 51–53, 2000.

[14] Popesu C., *A Secure Key Agreement Protocol Using Elliptic Curves*, International Journal of Computers and Applications, Vol 27, 2005.

[15] Shao Z., *Improved user efficient blind signatures*, Electronics Letters, vol. 36, no. 16, pp. 1372–1374, 2000.

[16] Stinson Doug, *Cryptography Theory and Practice*, Second Edition, CRC Press, Inc, 2002.