# Comparison of Scalar Multiplication Methods by Using Proposed Blind Signature Scheme

Aye Aye Thu, KhinThanMya
*University of Computer Studies (Yangon)*
*suchiq13@gmail.com, khinthanmya@gmail.com*

## Abstract

*Today blind signatures scheme are important techniques and can be used in many e-commerce services, such as electronic voting and cash payment system.Privacy is one of the basic rights for individuals and institutions that need to preserve their confidentiality.The performance of blind signature scheme is based on operation of scalar multiplication method. In this paper, we present the comparison of multiplication methods such asbinary double and adds, ternary expansion, Montgomery ladder and non-adjacent algorithm. The security of proposed blind signature scheme is based on solving the problem of elliptic curve discrete logarithm problem (ECDLP) and it can satisfy the requirements blind signature.The proposed scheme desired to reduce time consuming problem by using efficient multiplication method.Althoughmontgomery ladder algorithm is more efficient than the other algorithms, double and add algorithm is more compatible with the proposed system.*

***Keywords:*** BDS, DLP, ECC, ECDLP, E-commerce, Electronic voting system

## 1. Introduction

Nowadays people can accomplish their daily tasks, such as banking tractions, without leaving their homes by using Internet. People always do shopping through internet, which has increased the growing rate of the e-commerce. Now, the challenge is appeared and it is needed to improve the security and anonymity of the people in dangerous environment. So, we use the concept of blind Digital Signature (BDS) presented in.

Blind Signature is a form of digital signature in which the message is blinded before it is signed, in order to allow the requester to get a signature without giving the signer any information about the actual message or the resulting signature. Several blind signature schemes are proposed in the literature.

Elliptic Curve Cryptosystem (ECC) is accepted to be a secure and efficient public-key cryptosystem. In this paper, we would like to focus on the security of ECC relying upon the difficulty of solving the discrete logarithm problem.

One the most important operations for all applications of elliptic curves are scalar multiplication. This term refers to the operation of multiplying an integer by a point on an elliptic curve. Often the integer multiplied by the point is very large, so it is being able to do this efficiently is very important. Their multiplication techniques are not similar to the normal multiplication. So, it is needed to choose the suitable scalar multiplication for their purposes.

The objective of this paper is to propose blind signature scheme based on ECDLP by applying the strength of the ECC. It can fulfill the requirements of blind signature scheme like correctness, blindness, unforgeability and intraceability. This system will provide comparison of scalar multiplication method by using proposed blind signature scheme. Most of the blind signature scheme can be speed up by using effective scalar multiplication method. In this paper, we produce an efficient scalar multiplication method by applying on proposed blind signature scheme. It is intend to improve the performance of voting system or other applications.

The structure of the paper is as follows: Section 2 discusses the concept of elliptic curve cryptosystem, blind Signature Scheme, point multiplication method and also explains an overview of previous approaches on blind signature scheme. In Section 3, propose blind signature is presented. Section 4 provides security analysis of the system. The performance of this scheme is examined in Section 5. Finally, conclusions and future work are presented in Section 6.

## 2. Elliptic Curve Cryptosystem (ECC)

Elliptic curve Cryptography is based on a special type of elliptic curve which is of the form.

$$y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3$$

ECC makes the existing cryptosystems more secured and more efficient as these cryptosystems have smaller public-key certificates, smaller system parameters, faster implementations and other factors such as lower power consumptions etc. ECC is an

asymmetric key cryptography. Each user has a pair of keys (a secret private key and a public key. The secret key is a random number whereas public key is a point on the curve obtained by multiplying the private key with the base point G of the curve. Domain parameters of ECC include the base point G, the curve parameters a and b, along with some other constants [6].

Elliptic Curve on a prime field E ($F_p$) is

$y^2 \bmod p = x^3+ax+b \bmod p$

Where $4a^3+27b^2 \neq 0$

$G=(x_G, y_G)$ is a base point on E ($F_p$).Main operation in ECC is Point Multiplication. Point Multiplication is achieved by two basic curve operations. They are point addition and point doubling [9,11]:

(i) Point Addition

Adding two points J and K to obtain another point L i.e., L = J+K.

$$x_L = m^2 - x_J - x_K$$

$$y_L = m(x_J - x_L) - y_J$$

Where slope $m = (y_K - y_J)/(x_K - x_J)$

(ii) Point Doubling

Adding a point J to itself to obtain another point L i.e. L =2J.

$$x_L = m^2 - 2x_J$$

$$y_L = m(x_J - x_L) - y_J$$

Where slope $m = (3x_J^2 + a)/2y_J$

Example: If d = 23; then, (using Double and Add Algorithm)

dP = 23*J= 2(2(2(2J) + J) + J) + J

## 2.1. Elliptic Curve Discrete Logarithm Problem (ECDLP)

The classical or general DLP (discrete logarithm problem) is the following:

If $b=a^k \pmod p$, where p is prime and k is any random integer. DLP is the problem to find k. Similarly, ECDLP is the discrete log problem for elliptic curves.

i.e. kP=Q, where P,Q are points on the curve $E_p(a,b)$ and k is an integer such that Q lies on the curve. ECDLP is the problem of finding k knowing P and Q.

## 2.2. Blind Signature

The concept of blind signature scheme was first by introduced by Chaum in 1982. Blind signature is a kind of digital signatures. The main differences between the digital signature and the blind signature are shown [2, 3].

(1) In the blind signature scheme, the content of the message should be blind to the signer.

(2)When the public knows the message-signature pair, the signer should not be able to trace the message-signature pair.

A blind signature scheme involves basically a group of requesters and a signer as describe in (Figure1). Each requester obtains a valid signature from the signer after sending an encrypted message to him. The signer only signs the message without any idea of the contents of the message i.e. if does not decrypt it. Later, the signer can verify the authenticity of the signature whenever he/ she come across the message-signature pair. Moreover, anyone can use the signer's public key to verify whether the signature is authentic or not.

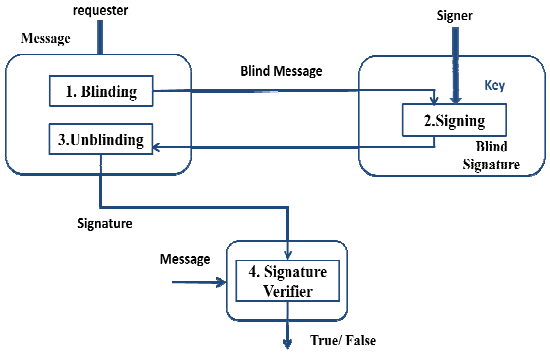



**Figure 1. Flow of blind signature**

### 2.2.1. Short Illustration of Blind Signature

Blind signature schemes consist of four phases. They are blinding, signing, unblinding and verification phases.

**Blinding Phase**

The sender chooses a random number called a blind factor to blind his message such that the signer will not be able to view the contents of the message.

**Signing Phase**

When the signer gets the blinded message, he encrypts the blinded message using his private key and then sends back the blind signature to the sender.

**Unblinding Phase**

The sender uses the blind factor to recover the signer's digital signature from the blinded message.

**Verification Phase**

Anyone can use the signer's public keys to verify whether the signature is authentic or not.

## 2.3. Point Multiplication Algorithms

In elliptic curve cryptosystem, main operations such as key agreement, signature generation, signing and verification involve scalar multiplication. The speed of scalar multiplication plays an important role

in the efficiency of whole system. Fast multiplication is very essential in some environments such as constrained devices, central servers, where large number of key agreements, signature generations, and verification occurs.

### 2.3.1. Scalar Multiplication Method on Elliptic Curve

**Table 1.Binary Double-Add Algorithm**

Scalar Multiplication kP

- Double and add $P \in E$, $k= (k_{n-1}.....k_0)_2$, $k_{n-1} =1$

1. $Q \rightarrow P$
2. From i= n-2 down to 0
3. $Q \rightarrow 2Q$ ECDBL
4. If $k_i = 1$ then $Q \rightarrow Q+P$ ECADD
5. Return Q

**Table 2.Ternary Expansion Algorithm**

INPUT : $k= (k_{t-1},....,k_1 k_0)_3$, Point P
OUTPUT : k*P

1. Point $Q = \infty$
2. For i from 0 to t-1 do
   a. If $k_i = 1$ then $Q \rightarrow Q+P$
   b. If $k_1=2$ then $Q \rightarrow Q+ 2P$
   c. $P \rightarrow 3P$
3. Return Q

**Table 3.Montgomery ladder Algorithm**

INPUT : $P \in E$ and $k= (k_{n-1},...,k_1 k_0)_2$,
OUTPUT : $[k]P \in E$

1. $P_0 \rightarrow P$
2. $P_1 \rightarrow [2]P$
3. For i $\rightarrow$ n-2 to 0 do
   // $k_i$ = either 0 or 1 and $k_i = 1- k_i$
4. $P_{ki} \rightarrow P_0 + P_1$
5. $P_{ki} \rightarrow [2] P_{ki}$
6. return $P_0$

**Table 4.Non-Adjacent Form Algorithm**

INPUT : NAF of a Positive integer k and p
OUTPUT : kP

1. $R \leftarrow P$
2. For i= i-2 to 0 do
2.1 $R \leftarrow 2R$
2.2 if $k_i = 1$ then $R \leftarrow R+P$
2.3 if $k_i = -1$ then $R \leftarrow R-P$
2.4 $i \leftarrow i-1$
3.Return R

The first algorithm implemented was the commercially well-known Binary Double-Add algorithm as shown in (Table 1). There are other efficient methods for point multiplication such as Ternary expansion algorithm, Montgomery ladder algorithm and Non-adjacent form algorithm as shown in (Table 2, 3 and 4).

## 2.4. Related Works

Blind Signature scheme was implemented using many of the cryptographic algorithms. BDS was first proposed using RSA algorithm which was proposed by Rivest, Shamir and Adleman [10] in 1977 which gives the problem of factoring big primes.

Fuh-GwoJeng et.al. , in [4] proposed so far are based on one of the following problem: integer factorization problem, discrete logarithm problem, and quadratic residues. Lee et.al.declared none of the schemes is able to meet the two fundamental properties above.

In 2005, Camenisch and al. [8] proposed a novel blind signature scheme based on the discrete Logarithm problem. But it fails the untraceability. AbhijitSaml and AnimeshChhotaray [1] proposed novel blind signature based upon ECDLP that it does not satisfy computational overhead problem.

The core operation of elliptic curve cryptosystems is the scalar multiplication on elliptic curves. There are numerous investigations of fast and regular multiplication on elliptic curve over large prime filed or binary field [7]. Several scalar multiplication methods have been proposedtoday.However, there is needed to implement efficient multiplication method toincrease the time complexity for blind signature scheme.The advantages of the proposed system solved the problem of time complexity and computation cost by using effective scalar multiplication method.

## 3. The Proposed Blind Signature Scheme

The proposed BDS scheme was derived from a variation of the ECDSA (Elliptic Curve Digital Signature Algorithm).Moreover, the scheme is based on solving the difficulty of elliptic curve discrete logarithm problem.The proposed BDS system contains five phases. They are

1. Initialization
2. Blinding
3. Signing
4. Unblinding and
5. Verifying

In the proposed scheme, used the elliptic curves over the $F_p$ prime field, which has been suggested by National Institute of Science and Technology (NIST) [12].Elliptic curve domain parameters over $F_p$ are defined as follow:

$$T= (p, F_p, a, b, G, n, h) \quad (1)$$

P is an integer specifying the $F_p$ finite field; $a,b \in F_p$ are integers specifying the elliptic curve $E(F_p)$ defined by

$$E(F_p) : y^2=x^3 + ax + b \pmod p \quad (2)$$

Where $G= (x_G, y_G)$ is a base point on $E(F_p)$, n is primenumber defining the order of G, andh s an integer defining the cofactor: $h=\#E(F_p)/n$. The system consists of three participants: They are requester, signer and verifier. The signer declares the necessary information in the initialization step. The requester submits a blinded version of the message to the signer to get the signature of a message at the blinding phase. The signer signs the blinded message and sends the result back to the requester at the signing phase. The requester extracts the signature in the unblinding phase. Finally, thevalidity of the signature is verified. The details of these phases are described below.

### *1. Initialization Phase*

The signer defines the elliptic curve domain parameters T, defined as in (1). Then, for each request, an integer k is randomly selected by the elliptic curve point R' is calculated.

$$R' = kG = (x_1, y_1) \quad (3)$$

$$r' = x_1 \pmod n \quad (4)$$

The Signer checks ($r' \neq 0$),

Otherwise signer selects another k randomly and repeats till his find r ′.If the result is true; the signer sends the elliptic curve point R′ to the requester.

### *2. Blinding phase*

To blind the message m, the requester needs the elliptic curve domain parameters T of the signer. And then the requester calculates r′ by choosing x coordinate of elliptic curve point R′.

$$R'=(x_1, y_1)$$

$$r'= x_1 \bmod n$$

The requester randomly chooses integer *v* and

$$\text{Compute } R=v^{-1}R' =(x_0, y_0) \quad (5)$$

$$r=x_0 \bmod n$$

Then calculate r from the elliptic curve point R.Requester generates the blinded message m and sends it back to the signer for signing operation:

$$m'= H(m) r^{-1}r'v \pmod n \quad (6)$$

Where H is the Hash function and we use SHA-1 [2] algorithm as the hash function.

### 3. *Signing Phase*

The signer receives the blinded message *m′*from the requester; he generates the blind signature *s* by following steps.

1. Signer randomly chooses integer *d* in the range (1, n-1)
2. Then calculates elliptic curve point
   $$Q = dG=(x_Q, y_Q) \quad (7)$$
3. Signer check (k, m) already exists in database?
4. If exist, go to the initialization step and re-select k.
5. Otherwise, compute

$$s= dm' + kr' \pmod n \quad (8)$$

Next, he sends the message-signature pair (m′, s ) pair back to the requester.

### *4. Unblinding Phase*

When the requester receives the blind signature *s* from the signer, the unblinding operation is needed to obtain the digital signature *s′* on message m.

$$s'=sv^{-1}r^{r-1}r \pmod n \quad (9)$$

The requester needed to verify the blind signature and message are intended to him.

### *5. Verifying Phase*

Digital signature of *(s′, R)* on the message m can verify by examining the correctness of the equation

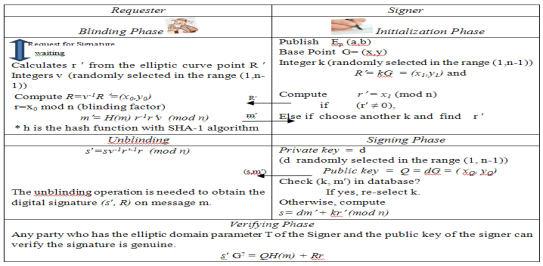
$$s' G^{?} = QH(m) + Rr \quad (10)$$

Table 5defines the notations used in this paper and Table 6illustrate the flow of the proposed blind signature.

**Table 5.Notation and System parameters**

| | |
|---|---|
| T | Elliptic curve domain parameter |
| a,b | Coefficient defining the elliptic curve |
| m | Message |
| G | Base point |
| n | Order of G, a prime number |
| h | Hash value |
| m′ | Blinded message |
| s | Blind signature |
| s′ | Signature |
| r′ | x coordinate of *R′* |
| r | x coordinate of R |
| R, *R′* | Points on Elliptic Curve |
| d | Private key of the Signer |

**Table 6.The Flow of the Proposed Blind Signature**




## 4. Security Analysis

This section examines the properties of blind signature to fulfill security requirements. The security of the proposed method is based on the difficulty of the ECDLP.

### *1. Proof of Blindness*

We used $r^{-1}$, $v^{-1}$ and v in the blind phase. The signer can never find $r^{-1}$, $v^{-1}$ and v so blind property is correctly achieved. Blindness is the first importantproperty in a blind signature. The requester calculates (5) and generates m′ defined in (6). Hence, the signer cannot know the message m.

### 2. *Proof of Unlinkability*

The signer will keep a set of records (k, R′, *m′*, s) for each blind signature requested. When the message m and its signature (*s′*, R) are revealed to the public.

The revealed message-signature pair (m, *s′*, R)

$s'G = QH(m) + Rr$

The signer tries to check the correctness of equation to trace the blind signature. The signer needs to have the blind factor (r, v, $v^{-1}$, $r^{-1}$) in addition to the values of points R,R′. However, he only has the following information for calculation (k, R′, *m′*, s, m, *s′*, R).And there are only three equations including the blind factor defined in (5), (6) and (9).There is no way for the signer to trace the blind signature by checking the correctness of equation from (10).

### 3. *Proof of Correctness*

The correctness of our scheme can be easily verified as follows Table 7. The verifier has only digital signature (r, R, s′) of message m for verification definedin (10).

**Table 7.Correctness Proof of the Proposed Scheme**

| | |
|---|---|
| $s'G$ | $= QH(m) + Rr$ |
| $s'G - Rr$ | $= QH(m)$ |
| $sv^{-1}r'^{-1}rG - Rr$ | $= QH(m)$ |
| $[dm' + kr'] v^{-1}r'^{-1}rG - Rr$ | $= QH(m)$ |
| $[dm'v^{-1}r'^{-1}rG + kr'v^{-1}r'^{-1}rG] - Rr$ | $= QH(m)$ |
| $[d[H(m)r^{-1}r'v]v^{-1}r'^{-1}rG] + [kr'v^{-1}r'^{-1}rG] - Rr$ | $= QH(m)$ |
| $[dH(m)G] + [kv^{-1}rG] - Rr$ | $= QH(m)$ |
| *(Substitute kG=R′ and Q=dG)* | |
| $QH(m) + R'v^{-1}r - Rr$ | $= QH(m)$ |
| *(Substitute R= R′v⁻¹)* | |
| $QH(m) + Rr - Rr$ | $= QH(m)$ |
| $QH(m)$ | $= QH(m)$ |

### 4. *Proof of Unforgeability*

No one can forge ($m_1'$, $R_1$, $s_1'$ ) because the elliptic curve discrete logarithm is difficult to solve. We assume three situations as follows.

$$As_1'G \stackrel{?}{=} QH(m) + R_1r_1$$

*Situation1*: If attacker tried to fake $m_1'$, $R_1$ he/she cannot obtain $s_1'$becausethey don't know $s_1'$ .

*Situation2*: If attacker gets $s_1'$ and $m_1'$ he/she cannot obtain $R_1$.

*Situation3*: If attacker tries to fake $s_1'$, $R_1$ he/she cannot obtain $m_1'$. It is also an elliptic curve discrete logarithm problem and difficult to solve. The privacy of the user is correctly protected and the signer is not able to derive the link between a signature and the corresponding instance of signing protocol which produced that signature. By providing the security requirements of ECDLP, the proposed scheme achieved efficiency in all operation.The proposed scheme applied in electronic voting system as case study shown in (Figure 2).Electronic voting (E-Voting) is an emerging social application of cryptographic protocols.

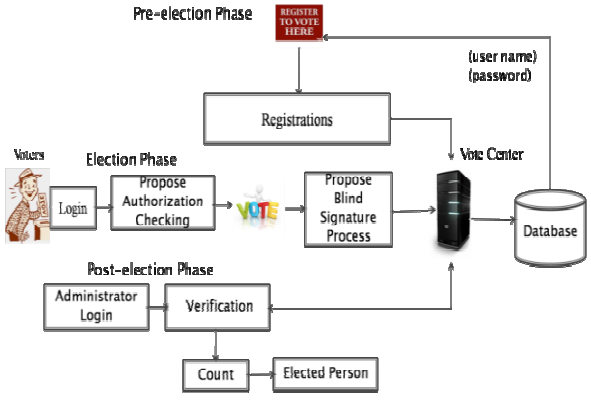



**Figure 2. Overview Architecture of E-Voting System**

## 5. Performance Evaluation

The following notations are used to estimate the time complexity. Any digital signature is compared on the basics of number of operations rather on the basics of time complexity from (4).

$T_{MUL}$ : the time required for the modular multiplication.

$T_{EXP}$ : the time required for the modular exponentiation.

$T_{INV}$ : the time required for the modular inversion.

$T_{ECMUL}$: the time required for the multiplication of as scalar and an elliptic curve point.

$T_{ECADD}$: the time required for the addition of two points over an elliptic curve.

The time complexity of the various operations units in terms of time complexity of a modular multiplication is shown in Table 8(5).

**Table 8.Unit Conversion of Various Operations In Terms of $T_{MUL}$**

| Time complexity of an operation Unit | Time complexity in terms of Multiplication |
|---|---|
| $T_{EXP}$ | 240 $T_{MUL}$ |
| $T_{EC-MUL}$ | 29$T_{MUL}$ |
| $T_{EC-ADD}$ | 0.12$T_{MUL}$ |
| $T_{ADD}$ | negligible |
| $T_{INV}$ | 0.073 $T_{MUL}$ |

The following table 9 compares our scheme with two other schemes. The required computational cost for all schemes has been estimated by accumulating execution times of all the required operations.

**Table 9.Required Time Complexity in Unit of $T_{mul}$**

| Schemes | Time Complexity | Rough Estimation |
|---|---|---|
| Fuh-GwoJeng&Tzer-Long (4) | $8T_{EC-MUL}$ + $3T_{MUL}$+2 $T_{EC-ADD}$ +$3T_{ADD}$ | 232.312 $T_{MUL}$ |
| AbhijitSal&AnimeshChhotaray [1] | $8T_{EC-MUL}$+$2T_{MUL}$+$8T_{EC-ADD}$ +2 $T_{INV}$ | 407.106 $T_{MUL}$ |
| Proposed Scheme with Double and Add algorithm | $6T_{EC-MUL}$+8 $T_{MUL}$+ $T_{EC-ADD}$ +3 $T_{INV}$ | 182.339 $T_{MUL}$ |

**Table 9.Comparison of Scalar Multiplication Methods**

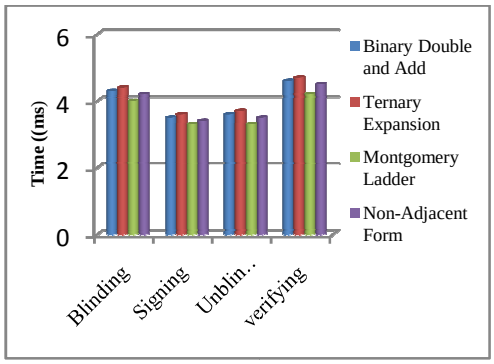



**Table 10.Comparison of Blind Signature Schemes**

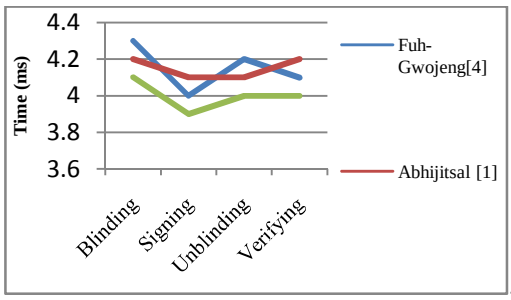



Table 10 shows the comparison of scalar multiplication methods. Montgomery ladder algorithm is slightly efficient than the others.

When we embed the various point multiplication method to my scheme, double and add algorithm with the proposed scheme is more efficient than the other schemes as shown in Table 10.

## 6. Conclusion

This system has proposed the efficient blind signature based on the ECDLP. It achieves the same security with fewer bits key and low computation requirements compared to other system.Moreover, it may satisfy the requirements of a blind signature scheme.And then the proposed scheme will reduce the time complexity with efficient scalar multiplication method.It can also be applied to electronic commerce applications, such as e-voting or e-payment.

## References


[1] AbhijitSamal and AnimeshChhotaray, “A novel blind signature based upon ECDLP”,Degree.thesis, Department of Computer Science and Engineering, Orissia, Japan, 2010.

[2] D.Chaum,“Blind Signatures for untraceable payments”, Advances in Cryptology-Crypto’82, pp.199-203,1982.

[3] D.L.Chaum, “Blind Signature systems”, US Patent 4759063,1988.

[4] Fuh-GwoJeng, Tzer-Long Chen, Tzer-ShyongCh-en, “ A blind Signature Scheme based on Elliptic Curve Cryptosystem”, 2009 Fifth International Joint Conference on INC, IMS, and IDC.

[5] Fuwen Liu, “A Tutorial on Elliptic Curve Cryptography,” Brandenburg Technical University of Cottbus, Computer NetworkingGroup, 2004.

[6] F.G.JengT.S.Chen, T.L.Chen, “A blind signatures scheme based on elliptic curve cryptosystem”. *Journal of Networks*, 5:921, 927, August 2010.

[7] I. F. Blake, G. Seroussi, and N. P. Smart. “*Advance in elliptic curve cryptography*”. Cambridge University Press,2005.

[8] Jan L.Camenisch, jean-Marc Piveteau, and Markus A. Stadler, “Blind Signatures based on the Discrete Logarithm Problem,” *In Advances in Cryptography EUROCRYPT 94, volume 950 of Lecture Notes in Computer Science*, pages 428-432, 1994.

[9] KefahRabah.“Theoryandimplementationofellipticcurvecryptography”.*Journal of applied sciences*,5:604633,2005.

[10] RivestR.ShamirA, and Adleman L. “A method for obtaining digital signatures and public key cryptosystems”. *Communication of the ACM*. February, 1978.

[11] RobLambert.“Understandingellipticcurvecryptography”. Director of New Technology,Certicom.

[12] “SEC 1: Elliptic Curve Cryptography”, Standards from Efficient Cryptography Group, available at*: http://www.secg.org/*, cited in October, 2011.