International Journal of Modern Science and Technology *Vol. 1, No. 8, November 2016. Page 269-275.*
http://www.ijmst.co/ ***ISSN: 2456-0235*.**

Review Article

Elliptic Curve and Associate Cryptosystem

S. Revathi, A. R. Rishivarman

Department of Mathematics, Theivanai Ammal College for Women (Autonomous)
Villupuram - 605 401. Tamilnadu, India.

*Corresponding author's e-mail: rishivarmanar@gmail.com

Abstract

Elliptic curve is a study of points on two-variable polynomials of degree three. With curve defined over a finite field, this set of points are acted by an addition operation forms a finite group structure. Encryption and decryption transform a point into another point in the same set. Besides providing conceptual understanding, discussions are targeting the issues of security and efficiency of elliptic curve cryptosystem. Cryptography is an evolving field that research into discreet mathematical equation that is representable by computer algorithm for providing message confidentiality. The scheme has been widely used by nation-states, corporate and individual who seek privacy for data in storage and during transmission. This paper provides a ground up survey on elliptic curve cryptography. The present paper serves as a basis to understand the fundamental concept behind this cryptosystem. Moreover, we also highlight subareas of research within the scope of elliptic curve cryptosystem.

Keywords: Elliptic Curve Cryptography; Finite field; Addition; Multiplication.

Introduction

Public key cryptosystems are constructed by relying on the hardness of mathematical problem. RSA based on Integer Factorization Problem and DH based on the Discrete Logarithm Problem [1]. The main problem of conventional Public key Cryptosystems is that the Key size has to be sufficiently large in order to meet the high level security requirement, resulting in lower speed and consumption of more bandwidth [2].

Elliptic curves have a rich and beautiful history, having been studied by mathematicians for over a hundred years. They have been deployed in diverse areas like: Number theory (proving Fermat`s Last Theorem) in 1995 [3], modern physics: String theory (The notion of a point-like particle is replaced by a curve-like string.), Elliptic Curve Cryptography (An efficient public key cryptographic system) [4]. In 1985, Neal Koblitz [5] and Victor Miller [6] independently proposed using elliptic curves to design public key cryptographic systems. In the late 1990`s, ECC was standardized by a number of organizations such as ANSI [7-9], ISO [10,11], NIST [12,13] and it started receiving commercial acceptance. Nowadays, it is mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks.There is a trend that conventional public key cryptographic systems are gradually replaced with ECC systems.

In Sep'2000 Bailey and Christof Paar [14] showed efficient arithmetic in finite field extensions with application in elliptic curve cryptography. An elliptic curve coprocessor based on the Montgomery algorithm for curve multiplication can be implemented using generic coprocessor architecture [15]. In February, 2005, the NSA announced that it had decided on a strategy of adopting elliptic curve cryptography as part of a US government standard in securing sensitive-but-unclassified information. The NSA recommended group of algorithms called Suite B, including Elliptic-Curve Menezes-Qu-Vanstone and Elliptic-Curve Diffie-Hellman for key agreement, and the Elliptic Curve Digital Signature Algorithm for digital signatures. The suite also included AES.

In 2010 [16] Brian King provided a deterministic method that guarantees,the map of a message to an elliptic curve point can be made without any modification. In 1988 Koblitz suggested for the first time the generalization of EC to curves of higher genus namely hyper elliptic curves (HEC) [17]. Since then HEC has

Received: 02.11.2016; Received after Revision: 06.11.2016; Accepted: 08.11.2016; Published: 23.11.2016

been analyzed and implemented in software [18,19] and hardware [20,21] both.

Representations of Elliptic curve

Various forms of elliptic curve has been explored as,

Weierstrass curve

An elliptic curve E over a field K is defined by an equation (Weierstrass equation)

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where $a_1, a_2, a_3, a_4, a_5, a_6 \in K$ and $\Delta \neq 0$ where Δ is the discriminant of E and is defined as follows:

$$\Delta = -d_2{}^2 d_8 - 8d_4{}^3 - 27d_6^2 + 9_2 d_4 d_6 \quad (2)$$

$d_2 = a_1{}^2 + 4a_2$, $d_2 = a_2 + a_1a_3$

$d_6 = a_3{}^2 + 4a_6$,

$d_8 = a_1{}^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3{}^2 - a_4{}^2$

If both the coordinate of the point $P \in E$ or $P = \infty$ (the point at infinity, infinity, or zero element. The set of points on E is:

$$E(L) = \{(x,y) \in L \times L: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \quad (3)$$

Hessian curve

This curve [22] was suggested for application in elliptic curve cryptography because arithmetic in this curve representation is faster and needs less memory than arithmetic in standard Weierstrass form.

Edwards curve

This curve was introduced in 2007 by Edward [23] and in Bernstein and Lange [24] pointed out several advantages of the Edwards form in comparison to the more well known weierstrass form.

Twists of curve

In mathematics an elliptic curve *E* over a field *K* has its quadratic twist, that is another elliptic curve which is isomorphic to *E* over an algebric of *K*. In particular, an isomorphism between elliptic curves is an isogeny of degree 1,that is an invertible isogeny. Some curves have higher order twists such as cubic and quartic twists. The curve and its twists have the same j-invariant and is shown in [25]. Twisted Hessian curve [26] represents a generalization of Hessian curve. It was introduced in elliptic curve cryptography to speed up the addition and doubling formulas and to have strongly unified arithmetic. Twisted Edward curves [27] are plane models of elliptic curve, a generalisation of Edward curves introduced by Bernstein (2007).

Jacobian curve

It [28] is used in cryptography instead of the Weierstrass form because it can provide a defense against simple and differential power analysis style (SPA) attacks and also faster arithmetic compared to the Weierstrass curve.

Montgomery curve

This curve was introduced by Peter L Montomery [29], and it has been used since 1987 for certain computations, and in particular in different cryptography applications.

Mathematical Background

Definition 1

A general equation of degree three polynomial with two variables can be defined as

$$(x,y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 + c_4x^2 + c_5xy + c_6y^2 + c_7x + c_8y + c_9 \quad (4)$$

where the coefficient c_i belong to any field *K*.

Definition 2

A point *P* in $C(K)$ is non-singular if and only if the partial derivatives of f with respect to *x* and with respect to *y* are not both zero at the point *P*.

Definition 3

Let two non-singular cubic curves C_1 and C_2 defined over K be given by Weierstrass equations

$$C_1: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$C_2: y + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2a^2 + \bar{a}_4x + \bar{a}_6 \quad (5)$$

C_1 and C_2 are said to be isomorphic over $\bar{K}$ if there exist $u, r, s, t \in K$ with u invertible, such that the function is defined by the change of variables

$$(x,y) \to (u^2x + r, u^3y + u^2sx + t)$$

which transforms equation C_1 into C_2.

Definition 4

An elliptic curve E is a non-singular cubic curve, a rational solution to $f(x,y) = 0$ over K. The set of points is given by

$$E(Q) = \{(a,b) \in Q \times Q \mid f(a,b) = 0\} \cup \{O\} \quad (6)$$

where O is the rational point at infinity.

Definition 5

Let E/Q be an elliptic curve with integer coefficients. Under a reduction modulo q, if E/F_q is a non-singular curve, then E is said to have a good reduction at q. Otherwise, E has bad reduction at q.

Definition 6

Given a point $P \in E(F_q)$ and an integer $k \in Z$, a scalar multiplication on ECC is defined as adding point P to itself k times such that

$$kP = P + P + \cdots + P, K\ times \quad (7)$$

and $-kP = k(-P)$.

Definition 7

An endomorphism φ of E/F_q given by a rational function, is defined by $\varphi: E(F_{q^m}) \to E(F_{q^m})P \to (r_1(P), r_2(P))$

Where r_1 and r_2 are rational function on E and

$$\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2) \quad (8)$$

for all $P, P_1, P_2 \in E(F_{q^m})$.

Group Structure

Closure

Aline through any two non-singular points (probably the same) on a non-singular curve will always intersect the curve at a third point.

Commutativity

Let L_1 be a line through P and Q and extend to a third intersection to produce PQ. Extending from Q to P would produce the same line and the same point of intersection. To get a point $P+Q$, extend a second line L_2 from O and PQ or QP, to produce a third intersection $O(PQ)$ or $O(QP)$ for either case. Hence $P + Q = O(PQ) = O(QP) = Q + P$.

Identity

Consider two points P and O. Extending L_1 through P and O produces PO. Extending L_2 through O and PO results in $L_2 = L_1$ and the third intersection would be P. Hence $P + O = O(PO) = P$.

Inverse

Consider two points P and O.Extend L_1 through a tangent point at O to produce OO such that $O + O = O(OO)O$. Let L_2 be a line through A and OO with the third intersection $P(OO)$ and call it M. On L_2, consider $P + M$ to produce $O(OO)$ on L_1 which again yield the third point O at the tangent. Remember tangent is considered as having two points.

Hence

$O + O = O(OO) = O.P + M = O(OO) = O, \Rightarrow M = -P$.

Associativity

The proof for this property is lengthy. Only the simplified version will be laid here. Consider three points P, Q and C. Let L_1 be a line through P and Q to produce PQ, so $P = Q = O(PQ)$ will be on L_2. Let L_3 be a line through Q and R to produce QR, so $Q + R = O(QR)$ will be on L_4. Now, let L_5 be the line through $(P + Q)$ and R. Hence $(P + Q) + R$ is $O((P + Q)R)$ with line L_6. Also, let L_7 be the line through P and $(Q + R)$. Hence $P + (Q + R)$ is $O(P(Q + R))$ with a line L_8. Geometrically, the two lines L_7 and L_8 are the same, which conclude the proof.

Now, let us consider an algebraic formulation of the well-defined point arithmetic. For simplicity, consider

$$y^2 = x^3 + ax + b \quad (9)$$

Over K where char$(K) \neq 2,3$

Let $P = (x_0, y_0) \in E(Q)$. A line through x_0 parallels to y-axis meets a line at infinity at O and meets E at another point P'. Following the composition law for inversion, this point is actually $-P$ with its y-coordinate a reflection of y_0 at x-axis. Therefore, $-P = (x_0, y_0)$.

Let

$P = (x_0, y_0), Q = (x_1, y_1), R = (x_2, y_2) \in E(Q)$

for which $P, Q \neq O$. Allow $P + Q = R$ and consider the following cases separately.

If $x_0, \neq x_1$ then

$$x_2 = m^2 - x_0 - x_1, y_2 = m(x_0 - x_2) - y_0 \quad (10)$$

where the slope, $m = \frac{y_1 - y_0}{x_1 - x_0}$.

If $x_0 = x_1$ but $y_0 \neq y_1$ then $P + Q = R = O$.

If $P = Q$ and $y_1 \neq 0$ then

$$x_2 = m^2 - 2x_0, y_2 = m(x_0 - x_2) - y_0 \quad (11)$$

where the slope $m = \frac{3{x_1}^2 + a}{2y_1}$.

If $P = Q$ and $y_1 = 0$, then $P + Q = R = O$. Moreover, $P + Q = P$ and $O + O = O$.

The first two cases deal with adding two different points on the curve and this operation is known as point addition. Meanwhile, the last two cases involves doubling a point and this operation is known as point doubling. Hasse's theorem on elliptic curves [30] bounds the number of points on an elliptic curve over a finite field above and below. If $\#E(F_q)$ is the number of points on the elliptic curve E over a finite field with q elements, then Helmut Hasse's result states that

$$q+1-2\sqrt{q} \le \#E(F_q) \le q+1+2\sqrt{q} \quad (12)$$

Field theory

The mathematical concepts necessary to understand and implement the arithmetic operations on an elliptic curve over a finite field(Galois field) [31]. Abstractly a finite field consists of a finite set of objects called field elements together with the description of two operations - addition and multiplication - that can be performed on pairs of field elements. These operations must possess certain properties. The finite field containing q elements is denoted by F_q. Generally two types of finite fields F_q are used-finite fields F_q with $q=p$, p an odd prime which are called prime finite fields, and finite fields $F_2{}^m$ with $q=2^m$ for some $m>=1$ which are called characteristic two finite fields.

Finite field F_p

The elements of F_p should be represented by the set of integers: $\{0,1,2,\ldots,p-1\}$ with operations as follows: If $a,b \in F_p$

Addition: then $a+b=r$ in F_p, where r $\in [0..p-1]$ is the remainder.

Multiplication: then $a.b=s$ in Fp where $s \in [0..p-1]$ is the remainder

Additive inverse

Then the additive inverse $(-a)$ of a in F_p is the unique solution to the equation $a+x \equiv 0$ (mod p). (13)

Multiplicative inverse

$a \neq 0$, then the multiplicative inverse a^{-1} of a in F_p is the unique solution to the equation $a,x \equiv 1$ (mod p).

The prime finite fields F_p used should have:

$log_2 p \in \{112,128;,,160;,192,;224;,256,;384,521\}$.

This restriction is designed to facilitate interoperability in terms of computation and communication since p is aligned with word size.

The Finite Field $F_2{}^m$

The finite field $F_2{}^m$ is the characteristic 2 finite field containing 2^m elements. Here the elements of $F_2{}^m$ should be represented by the set of binary polynomials of degree $m-1$ or less:

$$\{a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0: a_1 \in \{0;1\}\} \quad (14)$$

with addition and multiplication defined in terms of an irreducible binary polynomial $f(x)$ of degree m, known as the reduction polynomial, as follows: If

$$a=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_{0,}\ b=b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_0 \in F_{2,} \quad (15)$$

Addition: then $a+b=r$ in $F_2{}^m$, where $r=r_{m-1}x^{m-1}+r_{m-2}x^{m-2}+\ldots\ldots+a_0$ with $r_i \equiv a_i+b_i (mod\ 2)$. 15(a)

Multiplication: then $a:b=s$ in $F_2{}^m$, where $s=s_{m-1}x^{m-1}+sr_{m-2}x^{m-2}+\ldots\ldots\ldots+s_0$ 15(b)

is the remainder when the polynomial $a.b$ is divided by $f(x)$ with all coefficient arithmetic performed modulo 2.

In this representation of $F_2{}^m$, the additive identity or zero element is the polynomial 0, and the multiplicative identity is the polynomial 1. Additive inverses and multiplicative inverses in $F_2{}^m$ can be calculated efficiently using the extended Euclidean algorithm. Division and subtraction are defined in terms of additive and multiplicative inverses. Here the characteristic two finite fields $F_2{}^m$ used should have:

$m \in \{113,131,163,193,233,239,283,409,571\}$

Elliptic curve domain parameters

Two types of elliptic curve domain parameters may be used: elliptic curve domain parameters over F_p and elliptic curve domain parameters over $F_2{}^m$. Domain parameters for Elliptic curve are specified in [32]. ECC uses modular arithmetic or polynomial arithmetic for its operations depending on the field chosen.

Parameters over F_p

The domain parameters [33] for Elliptic curve over F_p are p,a,b,G,n and h, where p is the prime number defined for finite field F_p, a and b are the parameters defining the curve y^2 mod $p=x^3+ax+b$ mod p, G is the generator point (X_G,Y_G),n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and $n-1$,h, is the cofactor where $h=\#\frac{E(F_p)}{n}$,$\#E(F_p)$ is the number of points on an elliptic curve.

Parameters over $F_2{}^m$

The domain parameters for elliptic curve over $F_2{}^m$ are m, $f(x),a,b,G,n$ and h ,where m is an integer defined for finite field $F_2{}^m$. The elements of the finite field $F_2{}^m$ are integers of length at most m bits, f(x) is the irreducible polynomial of degree m used for elliptic curve operations ,a and b are the parameters defining the curve $y + xy = x^3 + ax^2 + b$ (16)

$G$is the generator point (X_G, Y_G), a point on the elliptic curve chosen for cryptographic operations , n is the order of the elliptic curve [34]. The scalar for point multiplication is chosen as a number between 0 and $n-1$,h is the cofactor, $h = \#E(F_2{}^m)/n$,$\#E(F_2{}^m)$ is the number of points on an elliptic curve [35].

Implementation

ECC can be implemented in software and hardware [36]. Software ECC implementation provide moderate speed, higher power consumption and also have very limited physical security w.r.t key storage, whereas hardware implementation improves performance in terms of flexibility. Also hardware implementation provides greater security since they cannot be easily modified or read by an outside attacker. An approach to combine the advantages of software and hardware in new paradigm of computation referred as reconfigurable computing [37].

Implementation issues in ECC

The most time consuming operation in ECC cryptographic schemes is the scalar multiplication (kP). Efficient hardware and software implementation of scalar multiplication have been the main research topic on ECC in recent years. [37] Shows elliptic curve scalar multiplication according to three layers. Upper layer shows different algorithm to perform the multiplication. In middle layer there are several combinations for finite field representation and coordinate system. The lower level is about finite field operation and arithmetic. An efficient implementation of ECC over binary Galois field in normal and polynomial bases has been proposed by Ester and Henies [38].

Elliptic curve cryptography communication

1. Alice negotiates with Bob on the choice of elliptic curve E over the finite field F_q and its order o.

2. Alice selects a private key K_i such that $0 < K_i < o$. She calculate the corresponding public key $K_u = K_i P$. Alice sends K_u to Bob.

3. Bob selects a random number r such that $1 < r < o$. He encrypts the message $M \in E(F_q)$ using K_u to obtain $C_1 = rP$and $C_2 = M + rK_u$.Bob sends C_1 and C_2 back to Alice.

4. Alice decrypts the message using her K_i such that $K_i C_1 = K_i(rP) = r(K_i P) = rK_p$.

The original message M is acquired through $M = C_2 - rK_p + rK_p$.

Conclusion

The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA yet using shorter keys. Implementing ECC with the combination of software and hardware is advantages as it provides flexibility and good performance. Mathematicians believe that not enough research has been done in ECDLP. Although ECC is a promising candidate for public key cryptosystem, its security has not been completely evaluated. This is now a deep and popular area of research. Also it has been found that hyperelliptic curves of higher genus are potentially insecure from a cryptographic point of view yet the researchers are trying to prove it better than ECC.

Acknowledgements

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

Conflict of interest

Authors declare there are no conflicts of interest.

References

[1] Mohamed MA. A Survey on Elliptic Curves Cryptography. *Applied Mathematical Science*. 2014;8(154):7665-7691.

[2] Kumar A, Lala K, Kumar A. VHDL Implementation using Elliptic Curve Point Multiplication. *International Journal of Advanced Research in Computer and Communication Engineering*. 2012;1(6)392-398.

[3] Faltings G, Taylor R, Wiles A. The Proof of Fermat's Last Theorem. *Notices of the American Mathematical Society*. 1995;42(7):743-746.

[4] Lavanya M, Natarajan V. Improved Elliptic Curve Arithmetic Over GF(P) Using

Different Projective Coordinate System. *Applied Mathematics Science.* 2015;9(45):2235-2243.

[5] Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation.* 1987;48: 2003-2009.

[6] Miller V. Use of Elliptic Curves in Cryptography. *Advances in Cryptology.* 1986;218(483):417-426.

[7] ANSI X9.62. Public Key Cryptography for Financial Services Industry: The Curve Digital Signature Algorithm, 1999.

[8] ANSI X9.62, Public Key Cryptography for The Financial Services Industry: The Elliptic curve key Agreement and Key Transport Protocols. 2000.

[9] Hemnath Ravindra, Jalaja S. ASIC Architectures for Implementing ECC Arithmetic over Finite Fields. *International Journals of Science and Research.* 2015;4(6):2319-7064.

[10] ISO IEC 14888, Information Technology Security Techniques-Digital Signatures. Appendix part 3. Certificate based Mechanism. 1998.

[11] ISO IEC15946, Information Security Technology-Cryptography Techniques based on Elliptic Curve. 1999.

[12] Digital Signature standard. FIPS Publication. 2000:186-192.

[13] Mishal N, Singh RK. A Study on Finite Field Multiplication Over GF(2m) and its Application on Elliptic Curve Cryptography. *International Journal of Science and Engineering Research*. 2014;5(5):1672-1684.

[14] Bailey D, Christof Paar C. Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography. *Journal of Cryptology.* 2001;14(3):153-176.

[15] Bednara M, Daldrup J, Shokrollahi.et al Tradeoff analysis of pga Based Elliptic Curve Cryptography. Proc. Of the IEEE International Symposium on Circuits and Systems, Scottsdale, Arizona, USA, 2002.

[16] King B. Mapping an Arbitary Message to an Elliptic Curve When Defined over GF (2n). *International Journal of Network Security*. 2009;8(2):169-17.

[17] Koblitz N. A family of Jacobian Suitable for Discrete Log Cryptosystem. *Advances in Cryptology*. 1988;88:94-99.

[18] Uwe Krieger Signature, Diplomaebeit C. University Essen Faahbereich. Mathematics and Informatics. 1997.

[19] Sakai Y, Sakurai K. On The Practical Performance of Hyperelliptic Curve Cryptosystem in Software Implementation. *IEICE Transaction on Fundamental of Electronics, Communication and Computer Sciences*. 2000;E83-A(4):692-703.

[20] Wollinger T. Computer Architecture for Cryptosystems Based on Hyperelliptic Curves. Thesis: Worcester Polytechnique Institute, 2001.

[21] Boston N, Clancy T, Liow Y, Webster J. Genus Two Hyperelliptic Curve Coprocessor. Workshop on Cryptographic Hardware and Embeded System, 2002.

[22] Smart NP. The Hessian form of An Elliptic Curve. Berlin Heidelberg: Springer-Verlag; 2001.

[23] Edwards HM. A Normal form for Elliptic Curves. *Bulletin of the American Mathematical Society,* 2007;44(3):393-422.

[24] Bernstein D, Lange T. Faster Addition and Doubling on Elliptic Curves, 2007.

[25] Gouvea F, Mazur B. The Square Free Sieve and The Rank of Elliptic Curve. *Journal of American Mathematical Society*. 1991;4(1):1-23.

[26] Twisted Hessian Curves Retrieved. Auto-Twisted Hessian.html, 2010.

[27] Daniel J. Bernstein, Marc Joye, Tania Lange et al. Twisted Edward curves, 2008.

[28] Olivier Billet, Marc Joye. The Jacobi Model of An Elliptic Curve and The Side-channel Analysis. Berlin Heidelberg: Springer-Verlag; 2003.

[29] Montgomery PL. Speeding the Pollard and Elliptic Curve Methods of Factorization. *American Mathematical Society.* 1987;48:243-264.

[30] Silverman, Joseph H. The Arithmetic of Elliptic Curves. Gradute Texts in Mathematics. New York. Springer Verlag: 1994.

[31] Standards for Efficient Cryptography, Sec 2. Elliptic Curve Cryptography. Certicom Research. 2000.

[32] Standards for Efficient Cryptography, Sec 2. Recommended Elliptic Curve Domain parameters, Certicom Research. 2010.

[33] Sravana Kumar D, Suneetha CH, Chandrasekhar A. Encryption of Data Using Elliptic Curve Over Finite Fields. *International Journals and Parallel System*. 2012;3(1):301-308.

[34] Gajbhiye S, Sharma M, Dashputre S. A Survey Report on Elliptic Curve Cryptography. *International Journal of Electrical and Computer Engineering*, 2011;1(2):195-201.

[35] Gayoso Martinez V, Hernandez Encinas L, Avila S. A Survey of the Elliptic Curve Integrated Encryption Scheme. *Journal of Computer Science and Engineering*. 2010;2(2):7-13.

[36] Marisa W, Paryasto, Kuspriyante, Sarwan et al. Issues in Elliptic Curve Crypyography Implementation. *International Indonesia Journal*, 2009;1(1):29-33.

[37] Morales-Sandoval M, An Interoperable and Reconfigurable Hardware Architecture for Elliptic Curve Cryptography Thesis: Mexico. National Institute for Astrophysics. Optics and Electronics. 2006.

[38] Mathew Estes, Phillip Hines, Efficient Implementation of an Elliptic Curve Cryptosystems Over Binary Galios Field in Normal and Polynomial Bases. George Massion University. 2006.

****

