Elliptic Curve Cryptography and Security Protocol

Dr.S.Vasundhara1, A.Sreedhar 2

1. G.Narayanamma Institute of Technlogy&Science(women)

2 . G.Narayanamma Institute of Technlogy&Science(women)

Shaikpet Hyderabad

Abstract: Algebraic curves over binary and finite fields used in the design of public key cryptography. This paper discusses some topics in algebraic curve cryptography namely elliptic curve cryptography with recent developments and different algorithms in Elliptic curve cryptography and also discussed discrete logarithmic problem and security protocol.

Key words: Cryptography Elliptic curves ,Finite fields, Binary fields elliptic curves cryptography

Introduction: The history of cryptography is long and interesting. It had a very considerable turning point when two researchers from Stanford, Whitfield Diffie and Martin Hellman, published the paper "New Directions in Cryptography" in 1976. They preface the new idea of public key cryptography in the paper.

Public-key cryptography and symmetric-key cryptography are two main categories of cryptography. The Well-known public-key cryptography algorithms are RSA (Rivest, et al. 1978), El-Gamal and Elliptic Curve Cryptography. Presently, there are only three problems of public key cryptosystems that are considered to be both secure and effective (Certicom, 2001). Table 1.1 shows these mathematical problems and the cryptosystems that rely on such problems.

	Mathematical problem	Detail	Cryptosystem
1	Integer Factorization problem (IFP)	Given an integer n find its prime factorization	RSA
2	Discrete Logarithm problem(DLS)	Given integer g and h find x' such that $=g^x \bmod n$	Diffie-Hellman(DH)
3	Elliptic curve discrete logarithmic problem(ECDLP)	Given points P and Q on the curve find 'x' such that Q=xP	Diffie-Hellman(DH)

Table 1.1-Mathematical Problem

Providing an equivalent level of security with smaller key size is an advantage of ECC compared to RSA. It is very efficient to implement ECC.ECC[1] obtains lower power consumption, and faster computation. It also gains small memory and bandwidth because of its key size length (Dormale, Bulens and Quisquater 2004), (Huang 2007). Such attributes are mainly fascinating in security applications in which calculative power and integrated circuit space are limited. Wireless devices and smart cards present a good example for the constrained devices with limited resources.

Cryptography companies such as Certicom Corporation have already implemented ECC in their products for some commercial purposes which are RFID and Zigbee. This company has an agreement with NSA on a set of cryptographic algorithms called suite B. This suite uses Elliptic curves and works over the prime field.

2 Cryptography Introduction:

Information security nowadays is a very important subject Governments, commercial businesses, and individuals are all demanding secure information in electronic documents, which is becoming preferred over traditional documents (paper and microfilm, for example). Documents in electronic form require less storage space, its transfer is almost instantaneous, and it is accessible via simplified databases. The ability to make use of information more efficiently has resulted in a rapid increase in the value of information.

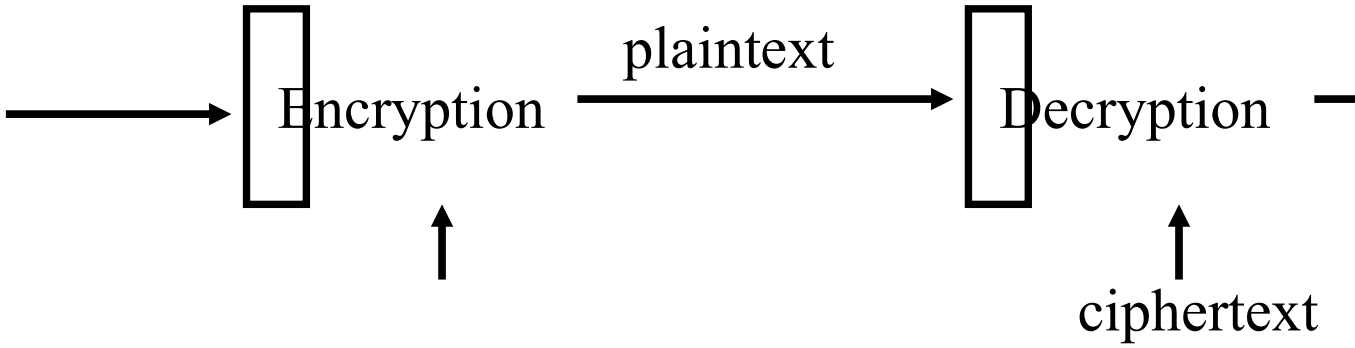
However, information in electronic form faces potentially more damaging security threats. Unlike information printed on paper, information in electronic form can virtually be stolen from a remote location. It is much easier to alter and intercept electronic communication than its paper-based predecessors. Information security is described as the set of measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of disclosure, alteration, substitution, or destruction of the data.

Several measures have been considered to provide these services but no single measure can ensure complete security. Of the various proposed measures, the use of cryptographic systems offers the highest level of security, together with maximum Flexibility. A cryptographic system transforms electronic data into a modified form. The owner of the information in modified form is now assured of its security features. Depending on the security services required, the assurance may be that the data cannot be altered without detection, or it may be that the data is unintelligible to all but authorized parties

According to Koblitz,[3] cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plain text and the disguised message is called the cipher text. The process of converting a plaintext to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Historically much of this study focused on private key cryptosystem where the sender and receiver agreed on private keys for sending messages and receiving messages, and was primarily used for military and diplomatic reasons. However with these cryptosystems, anyone who knew enough to decipher messages could not only ‘break a code” but also determine the enciphering key. Enciphering and deciphering were considered equivalent sciences in a cryptosystem until the 1970 are when Whitefield Diffie and Martin Hellman invented public key cryptography

The goal of cryptography is to achieve the aim of allowing two people to exchange messages using cryptography which are not understood by other people (Wang, et al.). Figure 2.1 provides a sample model of a two-party communication using encryption. In this simple party, an

entity is a person that sends, receives or manipulates data. S*ender* is an entity that legitimately transmits the information. On the other hand, a *receiver* is an entity that is the recipient of information. A *receiver* may be one of the entities that attempt to crush the information security service provided between the sender and receiver. An adversary plays the
role either as the sender or the receiver. The other synonymous names for adversary are attacker, enemy, eavesdropper, opponent and intruder (Jesper2006 be able to read the clear text or change it.



Figuere 2.1

3 Introduction for Elliptic curve cryptography :In 1985 Miller and Koblitz[4] independently presented ECC which based on algebraic structure of Elliptic curve. Currently ECC is the most efficient public key cryptosystem that uses shorter keys while providing the same security level as the RSA. Several researches were conducted on implementing public key cryptography especially ECC in Embedded devices. The use of elliptic curves in cryptography is very inviting because shorter key lengths can be used than in the case of conventional cryptography e.g. RSA

Elliptic curve cryptography has better security with a shorter key length than any other published public-key cryptography method. Elliptic curve cryptosystem with a 173-bit key is considered as secure as RSA using a 1024-bit key and ECC with a 313-bit key is considered as secure as 4096-bit RSA . Elliptic curve cryptography is thus a very attractive alternative, especially in communication systems with limited bandwidth.
Elliptic curves have been studied by mathematicians for more than a century. An extremely rich theory has been developed around them, and in turn they have been the basis of numerous new developments in mathematics. As far as cryptography is concerned, elliptic curves have
been used for factoring and primality proving. The idea of using elliptic curves for public-key cryptosystems is due to Victor Miller
[Miller85] and Neal Koblitz [Koblitz87] in the mid-eighties. As with all cryptosystems, and especially with public-key cryptosystems, it takes years of public evaluation before a reasonable level of confidence in a new system is established. The elliptic curve public-key cryptosystems (ECPKCs) seem to have reached that level now. In the last couple of years, the first commercial

applications have appeared(email security, web security, smart cards, etc.). Before we look at how the ECPKC s work, we will give a short introduction to elliptic curves.

Definition of elliptic curves: Elliptic curves are not ellipses. They are called this because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, an elliptic curve is the set of solutions of an equation of the form

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$ ……(1)

Where the coefficients ai are elements of some field (R, Z or Zp) which satisfy some Simple conditions in order to avoid singularities. Such an equation is said to be Cubic, or of degree 3, because the highest exponent it contains is 3. The Eq.1 is Called Weierstrass *equation*. Also included in the definition of any elliptic curve is a single element denoted O and called *point of infinity* or the *zero point*

An elliptic curve over real numbers may be defined as the set of points (x,y) which satisfy an elliptic curve equation of the form:

$y^2 = x^3 + ax + b$, where x, y, a and b are real numbers.

Each choice of the numbers[5] a and b yields a different elliptic curve. For example, a =1 and b =1 gives the elliptic curve with equation $y^2 = x^3 + x + 1$; the graph of this curve is shown below:

If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2$ is not 0, then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

Figure:

Elliptic Curve (y2 = x3+x +1)

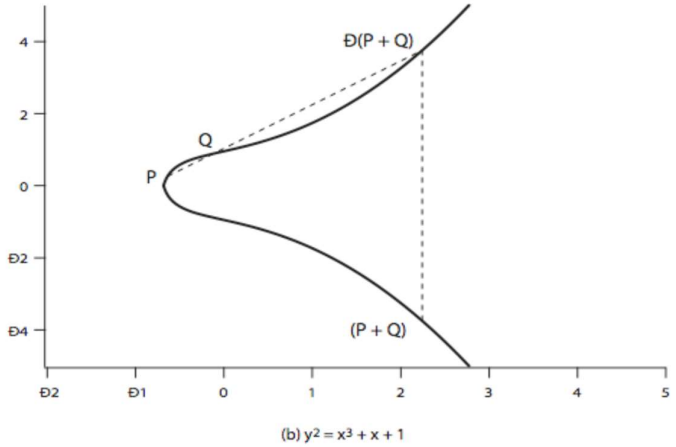
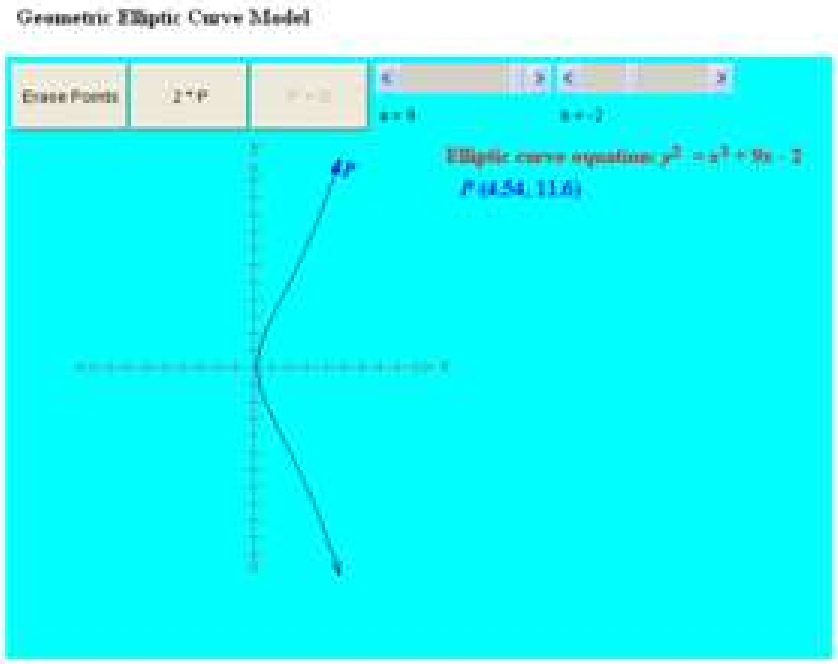


Figure 3. 1

Elliptic curves over real numbers 3.1: $y^2=x^3+ax+b$ with a=9,b=-2.



3.2 Elliptic curves over Finite fields F_P

All elliptic curve operations mentioned earlier are based on real numbers. However, operations over the real numbers are inaccurate and slow, whereas cryptographic operations need to be accurate and fast. Therefore, the curve cryptography can be defined over finite fields to operate EC efficiently and accurately. A finite field is a set of a finite number of elements. Cryptographic applications require fast and precise arithmetic; thus elliptic curve groups over the finite fields of F_p and $F_{2}m$ are used in practice.

Recall that the field Fp uses the numbers from 0 to p - 1, and computations end by taking the remainder on division by p. The number of points on $E(\mathrm{F}\ p)$ is denoted by $\#E(\mathrm{F}\ p)$. The Hasse Theorem states that:

$p+1-2\sqrt{p} \leq \#E(\mathrm{F}\ p) \leq p+1+2\sqrt{p}$.

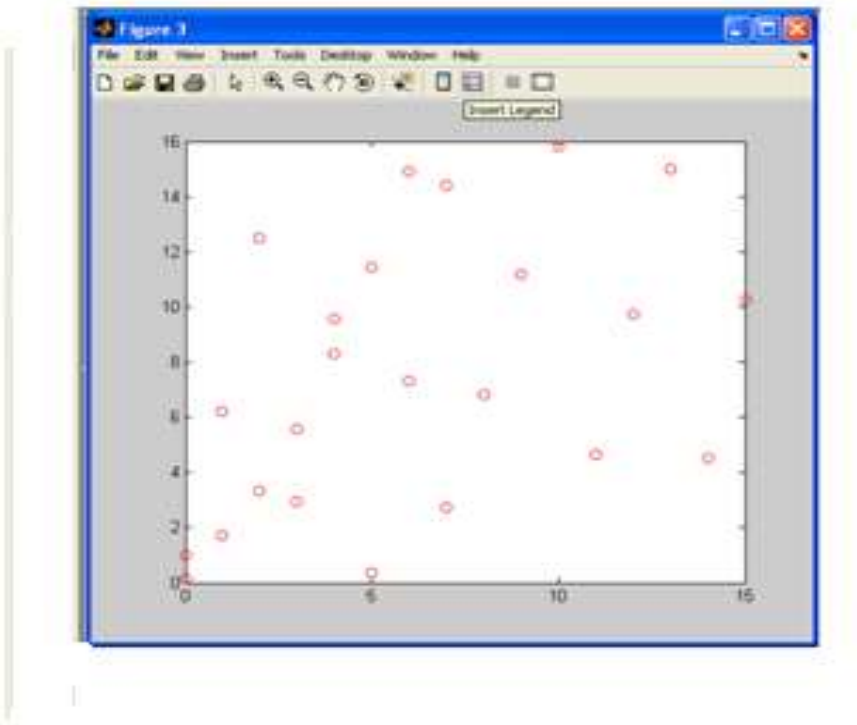


Figure3. 2

Note that there is two points for every x value. Even though the graph seems random, there is still symmetry about y = 11.5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. Over the field of F_{23}, the negative components in the y-values are taken modulo 23, resulting in a positive number as a difference from 23. Here -P = (x_P, (-y_P Mod 23))

3.3 Elliptic curves over binary field over 2^n:

The number of points on $E(F_2^m)$() is denoted by $\#E(F_2^m)$. The Hasse Theorem states that:

$2^m+1-2\sqrt{2^m} \leq \#E(F_2^m) \leq 2^m+1+2\sqrt{2^m}$:

There are finitely many points on a curve over F_2^m .

Elements of the field F_2^m are m-bit strings. The rules for arithmetic in F_2m can be defined by either polynomial representation or by optimal normal basis representation. Since F_2m operates on bit strings, computers can perform arithmetic in this field very efficiently.

An elliptic curve with the underlying [9]field F_2^m is formed by choosing the elements a and b within F_2m (the only condition is that b is not 0). As a result of the field F_2m having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation:

$y^2 + xy = x^3 + ax^2 + b$

The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over F_2m (where x and y are elements of F_2m). An elliptic curve group over F_2m consists of the points on

the corresponding elliptic curve, together with a point at infinity, O. There are finitely many points

on such an elliptic curve.

Example of Elliptic curve over F_2^n:

As a very small example,[6] consider the field F_24, defined by using polynomial representation with the irreducible polynomial $f(x) = x^4 + x + 1$.
The element g = (0010) is a generator for the field . The powers of g are:
$g^0 = (0001)$ $g^1 = (0010)$ $g^2 = (0100)$ $g^3 = (1000)$ $g^4 = (0011)$ $g^5 = (0110)$
$g^6 = (1100)$ $g^7 = (1011)$ $g^8 = (0101)$ $g^9 = (1010)$ $g^{10} = (0111)$ $g^{11} = (1110)$
$g^{12} = (1111)$ $g^{13} =(1101)$ $g^{14} =(1001)$ $g^{15} = (0001)$

In a true cryptographic application, the parameter m must be large enough to preclude the efficient generation of such a table otherwise the cryptosystem can be broken. In today's practice, m = 160 is a suitable choice. The table allows the use of generator notation (g^e) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without reference to the irreducible polynomial
$f(x) = x^4 + x + 1$.
Consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. Here $a = g^4$ and $b = g^0 =1$. The point (g^5, g^3) satisfies this equation overF_2^m :
$y^2 + xy = x^3 + g^4x^2 + 1$

$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$

$g^6 + g^8 = g^{15} + g^{14} + 1$

$(1100) + (0101) = (0001) + (1001) + (0001)$

$(1001) = (1001)$

The fifteen points which satisfy this equation are:

$(1, g^{13})$ (g^3, g^{13}) (g^5, g^{11}) (g^6, g^{14}) (g^9, g^{13}) (g^{10}, g^8) (g^{12}, g^{12})

$(1, g^6)$ (g^3, g^8) (g^5, g^3) (g^6, g^8) (g^9, g^{10}) (g^{10}, g) $(g^{12}, 0)$ $(0, 1)$

These points are graphed below:

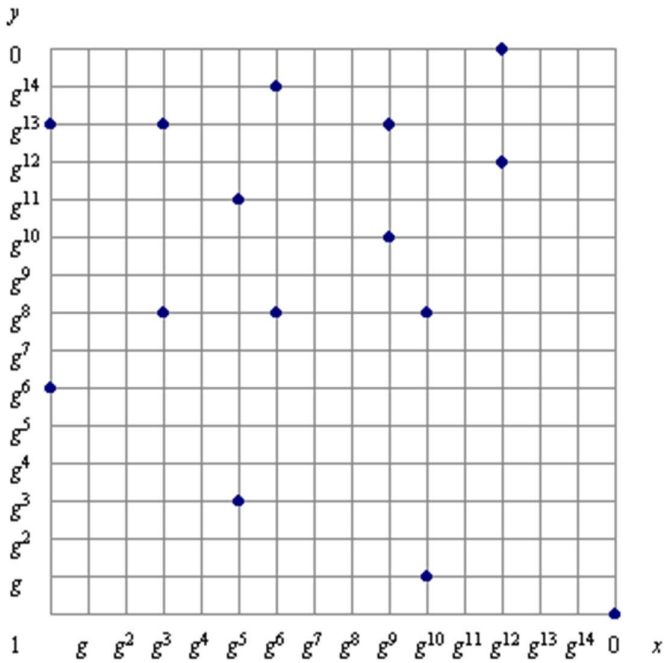


Figure 3.3

Elliptic curve groups over F_2m have a finite number of points, and their arithmetic involves no round off error. This combined with the binary nature of the field, F_2m arithmetic can be performed very efficiently by a computer.
The following algebraic rules are applied for arithmetic over F_2m :

3.4 Elliptic curves over binary fields:

Let $y^2+xy=x^3+ax^2+b$ let $a=g^4$, $b=1$ the points and the graph is given by:

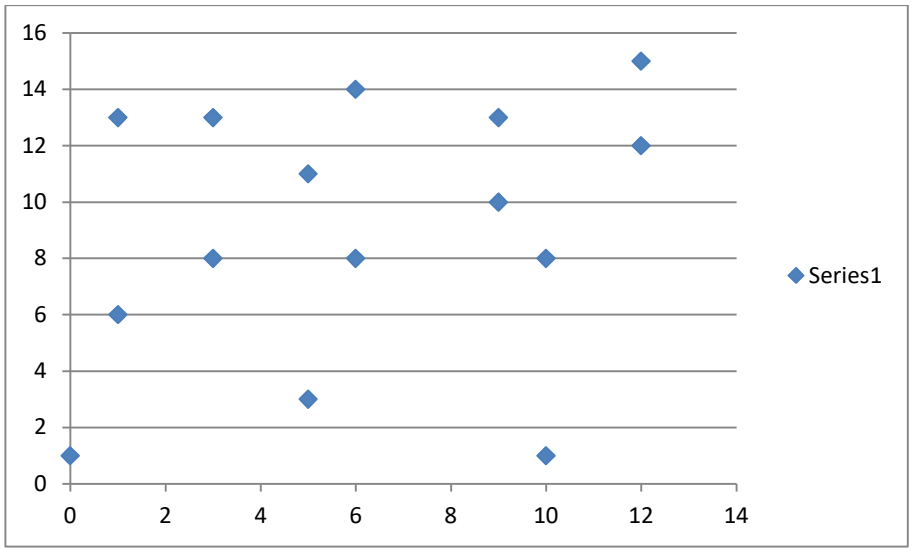


Figure 3.4

4 The Elliptic Curve Discrete Logarithm Problem:

rithms are fundamental[13] to a number of public-key4algorithms,including, Diffie-Hellman key nd the digital signature algorithm(DSA).This section provides a brief overview of discrete

The power of an Integer ,modulo n

For $a^{\emptyset(n)} \equiv 1(\text{mod}n)$

Where $\emptyset(n)$,Euler's totient function, is the number of positive integers less than n and relatively prime to n.now consider the general expression :

$a^m \equiv 1 \ (\text{mod } n)$ (1)

and n are relatively prime then there is at least one integer m that satisfies the Equation(1),namely , m=$\emptyset(n)$.The least positive exponent m for which equation holds is referred to in several ways:

Y	log_2^y(mod29)	22	26
1	28	23	20
2	1	24	8
3	5	25	16
4	2	26	19
5	22	27	15
6	6	28	14
7	12		
8	3		

9	**10**
10	**23**
11	**25**
12	**7**
13	**18**
14	**13**
15	**27**
16	**4**
17	**21**
18	**11**
19	**9**
20	**24**
21	**17**

1. Certicom, "standards for Efficient Cryptography,SEC 1:Elliptic curve

2. Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK, Version 2.1.USA: SANS Press, 2003.

3.J.Edge,an introduction to elliptic curve ,cryptography, http://Iwn.net/Articles/174127/.2006.

4.N.Koblitz,A course in Number theory and cryptography,2nd ed.,brookes/Cole,1997.

5.J.H.Silverman,The Arithmetic of Elliptic curves, Springer –Verlag,1986.

6.RSA" Wikipedia.wikipedia,n.d.web.09 feb 2011.Stalings,William. Cryptography and network security.fourth,pearson,2009.print.

7.Alfredj Menezes, paul c,vanoorschot and scott A.vanstone,guide to Elliptic curve Cryptography ,1996.

8.N.Koblitz.CM-curves with good cryptographic properties. In Advances in Cryptology: Crypto 91' volume 576 of in computer science, pages 279-287,springer-verlag,1992. Notes

9.The Thesis of on 2-Spreads in PG(5,3) by K. Hanumanthu under the super vision of Prof.K.Satyanarayana.

10.Thesis of Dr. K .V. Durga Prasad : "Construction ofTranslation planes and Determinition of their translation complements",Ph.D Thesis,Osmania University

11.Diffie, W., and M. E. Hellman. "New directions in cryptography." *IEEE Transactions on Information Theory,*, 1976: 644- 654.

12. A Scalar Multiplication in Elliptic Curve Cryptography with Binary Polynomial Operations in Galois Field Hero Modares(thesis of master science.

13.Mousa, A. "Security and Performance of ElGamal Encryption Parameters." *Journal of Applied Sciences 5(5):883-886,2005, ISSN 1812-5654*, 2005.

14.Huang, J. "Fpga Implementations Of Elliptic Curve Cryptography And Tate Pairing Over Binary Field." *University Of North Texas*, August 2007.

15.Quisquater, J. J., and C. Couvreur. “Fast decipherment algorithm for RSA public-key cryptosystem.” *Electronics Letters*, 1982: 18(21):905–907.

16.Stalling, W. *Network and Internet work Scurity.* IEEE Press, 1995.

17.Tata, E. “Elliptic Curve Cryptography, An Implementation Guide.” In *Anoop MS*. India: Anoop, MS, 2007

18.Rivest, R. L., A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” *Communications of the ACM*, 1978: 120-126.