IJERT
ISSN : 2278 - 0181

THESIS

Thesis ID : IJERTTH00010

A Brief Study of Elliptic Curve Cryptography

Ekambaram Kesavulu Reddy

S.V.U. College of Arts & Sciences
India

Published By

International Journal of
Engineering Research and Technology
(www.ijert.org)

ISBN
9 788193 976104

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181

A Brief Study of Elliptic Curve Cryptography

Submitted in partial fulfillment of the requirement
for the award of the degree of

Master of Philosophy
in
Computer Science

By
EKAMBARAM KESAVULU REDDY
(A5A6686903)

Under the Esteemed Guidance of

Dr. M. PADMAVATHAMMA
Asso. Prof. & Head – Incharge
Dept. of Computer Science SCMIS
S.V.U. College of Arts & Sciences
Tirupati

MADURAI KAMARAJ UNIVERSITY
DIRECTORATE OF DISTANCE EDUCATION
PALKALAI NAGAR, MADURAI – 625 021

December 2005

DECLARATION

I here by declare that the work presented in this dissertation entitled ***"A Brief study of Elliptic Curve Cryptography"*** *is bonafied record of the research work done by me under the supervision of* ***Dr. M. Padmavathamma****, Associate Professor, Head – Incharge, Department of Computer Science, S.V.U. College of Arts and Sciences, Tirupati during the academic year 2004-2005. This research work is submitted to D.D.E. Madurai Kamraj University, Madurai in partial fulfillment of the requirements for the award of degree in "Master of Philosophy in Computer Science" during the year 2004-2005. This work has not been submitted for any other institution for any Degree, Diploma, Previously.*

Date :

Place :

(E. KESAVULU REDDY)
A5A6686903

Department of Computer Science
Madurai Kamaraj University

MADURAI – 625 021

CERTIFICATE

This is to certify that the M.Phil dissertation entitled ***"A Brief study of Elliptic Curve Cryptography"*** *submitted to Madurai Kamraj University, Madurai, for the award of Master of Philosophy in Computer Science, is a bonafied record of research work and investigations done by* ***Sri. E. Kesavulu Reddy (A5A6686903),*** *under my supervision as a Research Scholar (Part – Time) of the Department of Computer Science, S.V. University College of Arts and Sciences, Tirupati during 2004-2005 and that this work has not previously formed the basis of any degree, diploma or title to him.*

Sri Venkateswara University,
Tirupati

(Asso. Prof. Dr. M. Padmavathamma)
Research Supervisor

ACKNOWLEGEMENT

My sincere thanks remain to express Sri. Dr. S. Manickan Garu, Director in charge of DDE, Madurai Kamraj University, Madurai to introduce the research in Distance Learning Programming.

I am very thankful to the respectable Sri. N.M. Ganesan Garu Deputy Director of DDE, Madurai Kamraj University, Madurai for extending his full cooperation and encouragement in every aspect in contact seminar programming.

I am very thankful to Dr. Ganpathy Garu, Coordinator of Computer Science DDE, Madurai Kamraj University, Madurai for the approval of topic for dissertation and valuable guidance in completing the research.

My sincere thanks to my research guide Smt Dr. M. Padmavathamma, Head, Department of Computer Science, S.V.U. College of Arts and science, Tirupati for her valuable guidance for the successful completion of my research work.

I am also thankful to Sri. M. Ramaswamy, Sri, Kannaiah, DDE, Madurai Kamraj University, Maduri for his valuable guidance in contact seminar programming for the completion of my course.

My sincere thanks to Mr. P. Vasudeva Reddy, Research Scholar, Department of Mathematics, S.V. U. College of Arts and Sciences, Tirupati for his valuable suggestions to completion of my research work.

I am also very thankful to my colleagues and Research Scholars in Department of Computer Science, S.V. University College of Arts & Sciences, Tirupati for their co-operation for successful completion of this research work.

First and fore most I would like to thanks to my parents because of whom I have come up to this stage.

I am also very thankful to E. Digvijay Kumar Reddy and E. Sai Kumari for their encouragement in successful completion of this course.

I will be very thankful till my death to Smt.T.Jagdeeswaramma, T.Satyavathi and Smt. E. Gouri Sree without them I might not have studied this course.

(E. KESAVULU REDDY)

CONTENTS

ABSTRACT

This dissertation presents two main themes. One is the study of existing "Trapdoor one-way functions" based on elliptic curves over Z_n" and the other is "trapdooring discrete logarithms on Elliptic curves over rings". Specifically contribution of this thesis are as follows :

We present an over view of a "Trapdoor one-way functions" based on elliptic curves over a ring Z_n, whose security is based on the difficulty of factoring n. Also we propose a new public key cryptosystem based on the elliptic curves over a ring Z_n. This scheme can be used for both digital signatures and encryption/decryption schemes. The advantage of this scheme is very little restriction on the type of elliptic curves and types of primes that can be used. The security of the proposed scheme is based on the factoring composite numbers.

Finally, we present the elliptic curve version for the existing cryptosystems like Naccache-Stern, Okamoto-Uchiyama and Paillier Cryptosystems. The security and efficiency properties of these elliptic version schemes are same as the original cryptosystems.

CHAPTER – 1
INTRODUCTION

1.1 General introduction

As long as there are creatures endowed with language, there will be confidential messages intended for a limited audience. How can these messages be transmitted secretly, so that no unauthorised person gets knowledge of the content of the message?

And how can one guarantee that a message arrives in the right hands exactly as it was transmitted?

Traditionally, there are two ways to answer such questions. One can disguise the very existence of a message, perhaps by writing with invisible ink; or try to transmit the message via a trustworthy person. This is the method favoured throughout history by clandestine lovers and nearly all classical tragedies provide evidence of the method's shortcomings.

A totally different approach is to encipher (or encrypt) a message. In this case, one does not disguise its existence. On the contrary, the message is transmitted over a public, insecure channel, but encrypted in such a way that no one except the intended recipient may decipher it. This offers a rather tempting challenge to an enemy. Such challenges are usually accepted and not unusually overcome.

There is a satisfying appropriateness to cryptology's role in the birth of electronic computing. The arrival of the Information Age has revealed an urgent need for cryptography in the private sector. Today, vast amounts of sensitive information such as health and legal records, financial transactions, credit ratings and the like are routinely exchanged between computers via public communication facilities. Society turns to the cryptographer for help in ensuring the privacy and authenticity of such sensitive information.

Cryptographic techniques, such as enchiperment, digital signatures, key agreement and secret sharing schemes are important building blocks in the implementation of any security service. A cryptosystem defines encryption and decryption transformations, which depend on the value of 'S' keys. A symmetric cryptosystem uses one key for both transformations. A public key cryptosystem uses separate keys for each transformation.

The idea of the public-key technique was first introduced by Diffie and Hellman [5] in 1976, and began a revolution in cryptology. Public-key cryptosystems can be encryption or authentication schemes. The RSA algorithm can operate in both modes. The strength of RSA depends on the difficulty of factoring the product of two large primes. The selection of an appropriate modulus size can make RSA hard (modulus arbitrarily long). The ElGamal algorithm is an alternative public-key algorithm, the strength of which depends on the difficulty of computing discrete logarithms.

A digital signature is an electronic equivalent of verifying the source of a written message on the basis of a written signature. A digital signature is stronger than a seal, in that the recipient must not be able to generate a digital signature which is indistinguishable from one generated by the originator. Digital signatures usually employ public-key cryptosystems, often in conjunction with a one-way hash-function.

'Key agreement' denotes a protocol whereby two (or more) parties jointly establish a secret key by communicating over a public channel. In a key agreement scheme, the value of the key is determined as a function of inputs provided by both parties.

1.2 Overview of the Dissertation

This dissertation concern **"A brief study of Elliptic Curve Cryptography".** This dissertation has been split up into five chapters with the survey of elliptic curve cryptosystems. In this section, we overview the Subject matter of each chapters.

Chapter 1

In this chapter, we survey the background theory on which the subject matter of the rest of the thesis is band. First, we review the basics of abstract algebra, number theory and some computational primitives such as integer factorization, Discrete logarithm, the Diffie Hellman and Quadratic residuosity problems. We also review symmetric, public-key encryption schemes and digital signatures.

Chapter 2

In this chapter we discuss several aspects of elliptic curves and elliptic curve cryptography. First we will treat them more as mathematical objects, and then we discuss more cryptography related stuff. Everything in this chapter is written in a cryptographers view. We present some important properties that a cryptosystem must have and we assert that they hold for elliptic curve cryptography.

Chapter 3

In this chapter we review a "Trapdoor one-way function" (TOF) based on elliptic curves over a ring Z_n [21]. The security of this TOF depends on the difficulty of factoring n. Also we present a public key cryptosystem based on elliptic curves over a ring Z_n. This scheme can be used for both digital signatures and encryption applications, doesn't expand the amount of data that needs to be transmitted and appears to be immune from homomorphic attacks. The main advantage of this scheme is very little restriction on the type of elliptic curves and types of primes that can be used. In addition the system works on a fixed elliptic curves. The security of the system relies on the difficulty of factoring large composite numbers.

Chapter 4

In this chapter we propose the elliptic curve version for the existing cryptosystems like Naccache-Stern cryptosystem [18], Okamoto-Uchiyama [22] and Paillier cryptosystem [23]. The first elliptic curve Naccache-Stern cryptosystem defined on curves over the ring Z_n, n=pq which relies a discrete log encryption as originally issued by Vanstone and Zuccherato probabilistic scheme. Our second cryptosystem relates to p-residuosity of a well-chosen curve over a Zp^2q.

Finally, we show how to extend the same design to frame work of Paillier encryption, while preserving all security and efficiency properties inherent to the original Paillier's Cryptosystem.

1.3 Abstract Algebra

The purpose of this section is to introduce the algebraic definitions and results that are necessary for understanding the results in this dissertation. Most of the theorems are quoted without proof, but with references to where proof can be found.

Definition : A binary operation '.' on a set S is a mapping from S x S to S. That is, '.' is a rule which assigns to each ordered pair of elements from S x S to an element of S.

1.3.1 Groups

Definition: A group G(.) or simply G consists of a set G with a binary operation '**.**' on G satisfying the following properties.

(i) For every a, b, c $\in$ G, a . (b . c) = (a . b) **.** c (Associative)

(ii) There is an element e $\in$ G such that every a in G, a . e = e . a = a. (Identity)

(iii) For every a $\in$ G, there is an element a^{-1} in G such that a . a^{-1} = a^{-1} **.** a = e.

(Inverse)

A group G is abelian (or commutative) if, furthermore

(iv) a . b = b . a for all a, b $\in$ G.

Note : A group G is called an additive group when the operation is additive (+), while a group G is called a multiplicative group under the operation of multiplicative (x). In a group with an additive operation, we have a + (-a) = (-a) + a = 0, where the inverse element of a is written as -a. In this case, the identity of element e is 0. Under the multiplicative operation, the identity element e is 1 and inverse element of a is written as a^{-1}, so that a a^{-1} = a^{-1} a = 1.

Definition : Let G be a group. If G has a finite number of elements, say n, then we say that the **order of** G is n. We write this symbolically by o(G) = n, and in this case we say G is a **finite group.**

Definition : A nonempty subset H of a finite group G is a **subgroup** if H is a group with the same binary operation as G.

Theorem Let G be a group with binary operation and let g be an element of G. Then $H = \{ g^i \mid i \text{ is an integer}\}$ is a subgroup of G.

Definition: A group H is said to be **cyclic** if there exists an element g Є H such that every element of H can be written as gn for some integer n. In this case, H is called the **cyclic group generated by** g and g is called a **generator** of H. If H is a subgroup of another group G, then H is called a **cyclic subgroup**.

Corollary If G is a finite group of order n, then $g^n = e$ for all g Є G. A proof can be found [10] in page 46.

Corollary The order of every element of a finite group is a divisor of the order of the group. A proof can be found [10] in Page 46.

Corollary If G is a finite group of order p where p is a prime integer, then G is cyclic and every element of G except the identity is a generator of G. A proof can be found [10] in page 46.

Definition : A **homomorphism** from $(G_1,\cdot)$ to $(G_2,*)$ H is a mapping f from G to H such that $f(a.b) = f(a) * f(b)$

Definition Let $(G_1,\cdot)$ and $(G_2,*)$ be groups and let α be a homomorphism from G to H. If α is both onto and one-to-one, then α is called an **isomorphism.** If α is an isomorphism, then G and H are said to be **isomorphic**, and we write G ≅ H.

1.3.2 Rings and Fields

We present another algebraic system called a ring. We define ring and prove several elementary theorems about rings. Then we study subrings and their homomorphisms and isomorphisms. We also study two special types of rings namely, Integral domains and fields. These two algebraic systems are important because our usual 'arithmetic' is carried out in either an integral domain or a field.

Definition : A ring R(+, .) or simply R consists of a set R with two binary operations, denoted by + and . called addition and multiplication, which satisfy the following axioms.

(i) (a + b) + c = a + (b + c) for all a, b, c Є R. (Associativity of addition)

(ii) There exists an element 0 Є R such that 0 + a = a for all a Є R. (existence of additive identity)

(iii) For each a Є R, there exists x Є R such that a + x = 0. (existence of additive inverse)

(iv) a + b = b + a for all a, b Є R. (Commutative of addition)

(v) (a . b) . c = a . (b . c) for all a, b, c Є R. (Associativity of multiplication)

(vi) a . (b + c) = (a . b) + (a . c) and (a + b) . c = (a. c) + (b. c) for all a, b, c Є R (Distributive)

Definition : Let R be a ring. We say R is a **ring with unity** if there exists e Є R such that a . e = e . a = a for all a Є R. If such an element e exists, it is called a **unity element** of R.

Definition : Let R be a ring. Then R is said to be commutative ring if a . b = b . a for all a, b Є R.

Definition : A nonempty set S is a **subring** of a ring R if S is a subset of R and if S itself is a ring with respect to the addition and multiplication of R.

We defined homomorphism between two rings. Since rings have two binary operations defined on them, rather than one, it is not unreasonable that a homomorphism between two rings must preserve both the addition and multiplication of the rings.

Definition : Let R and S be rings. A ring homomorphism is a mapping α from R to S such that

(i) α (a + b) = α (a) + α (b)

(ii) α (a . b) = α (a) . α (b) for all a, b Є R.

Definition : A field F is a commutative ring in which all the nonzero elements form an abelian group under multiplication.

Definition : Let a and b be two elements of a commutative ring R, with $a \neq 0$. The element a **divides** b, denoted a|b, if there exists an element c Є R such that b = ac.

Definition : Let a1, ….., an be elements of a commutative ring R. A nonzero element c Є R is a common divisor of a_1,……, a_n if $c|a_i$ for i = 1,…., n.

Definition : Let a1,…., an be elements of commutative ring R. A nonzero element d Є R is a greatest common divisor of a_1,……..., a_n, denoted by d =gcd(a_1,……., a_n), if

(i) d is a common divisor of $a_{1,\ldots\ldots,}$ a_n, and

(ii) whenever $c|a_i$ for i Є {1,…., n}, then c|d.

Definition Let a and b be two elements in a commutative ring R with unity. Then a and b are **coprimes** or **relatively prime** if gcd (a, b) is a unit.

Definition Let R be a commutative ring. A **polynomial** in the indeterminate x over the ring R is an expression of the form

$$f(x) = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$$

where each a_i Є R and n≥ 0. The element a_i is called the **coefficient** of x_i in f(x). The largest integer m for which $a_m \neq 0$ is called the **degree** of f(x), denoted by deg f(x); am is called the **leading coefficient** of f(x).

If $f(x) = a_0$ (a constant polynomial) and $a_0 \neq 0$, then f(x) has degree 0. If all the coefficients of f(x) are 0, then f(x) is called the zero polynomial and its degree, for mathematical convenience, is defined to be -1.

The polynomial f(x) is said to be **monic** if its leading coefficient is equal to 1.

Definition : If R is a commutative ring, the polynomial ring R[x] is the ring formed by the set of all polynomials in the indeterminate x having coefficients in R. The two operations are the standard polynomial addition and multiplication, with coefficient arithmetic performed in the ring R.

Definition : Let F be a field and f(x) Є F[x] be a polynomial. Then f(x) is said to be irreducible over F if it cannot be written as the product of two polynomials in F[x], each of positive degree.

Definition : (Division algorithm for polynomial) Let F be a field if g(x), h(x) Є F[x], with h(x) ≠ 0, then ordinary polynomial long division of g(x) by h(x) yields polynomials q(x) and r(x) Є F[x] such that g(x) = q(x)h(x) + r(x); where deg r(x) < deg h(x). Moreover, q(x) and r(x) are unique. The polynomial q(x) is called the quotient, while r(x) is called the remainder. The remainder of the division is sometimes denoted g(x) mod h(x), and the quotient is sometimes denoted by g(x) div h(x).

Definition : An integral domain R is Euclidean ring if for all nonzero a Є R, there is defined a non negative integer d(a) such that

(i) for all nonzero a, b Є R, d(a) ≤ d(ab), and

(ii) for any a; b Є R with b ≠ 0, there exist m, r Є R such that a = mb + r with either r = 0 or d(r) < d(b).

Lemma : Let R be a Euclidean ring. Any two elements a and b in R have a greatest common divisor d which can be expressed in the form d = λa + μb for some λ,μ∈ R.

Theorem : Let a and b be two elements in a Euclidean ring R. The n gcd(a,b) can be calculated in R as follows:

$a = q_0 b + r_1$, where $d(r_1) < d(b)$

$b = q_1 r_1 + r_2$, where $d(r_2) < d(r_1)$

$r_{n-2} = q_{n-1} r_{n-1} + r_n$, where $d(r_n) < d(r_{n-1})$

$r_{n-1} = q_n r_n$,

where r_n = gcd(a, b).

1.4 Number Theory

The set of integers { …., -2, -1, 0, 1, 2, … } is denoted by the symbol **Z .**

Definition : Let a, b be integers. Then a Divides b (equivalently : a is a divisor of b, or a is a factor of b) if there exists an integer c such that b = ac . If a divides b, then we write a|b.

Proposition :Properties of divisibility : For all a,b c ∈ Z, the following are true :

(i) a|a

(ii) If a|b and b|c, then a|c.

(iii) If a|b and a|c, then a|(bx+cy) for all x,y ∈ Z.

(iv) If a|b and b|a, then a = ± b .

Definition : Division algorithm for integers : If a and b are integers with b ≥ 1, then ordinary division of a by b yields integers q (the quotient) and r (the remainder) such that

a = qb +r , where 0 ≤ r ≤ b.

Moreover, q and r are unique. The remainder of the division is denoted a mod b, and the quotient is denoted a div b.

Definition : A non – negative integer d is the **least common multiple** of integers a and b, denoted d = lcm(a,b), if

(i) a|d and b|d ; and

(ii) whenever a|c and b|c, then d|c.

Equivalently, lcm(a,b) if n is the smallest non-negative integer that is divisible divided by both a and b. In fact, lcm(a,b) = ab / gcd (a,b).

Definition : If a and b are integers, then a is said to be **congruent** to b modulo n, write $a \equiv b \pmod{n}$, if n divides (a – b). The integer n is called the modulus of the congruence.

Definition : The **equivalence class** modulo n of an integer b is the set of all integers congruent to b modulo n.

Definition : The ring of **integers modulo** n, denoted by Z_n , is the set of (equivalence classes of) is the integers {0,1,2,, n–1}. Addition, subtraction, and multiplication in Z_n are performed modulo n.

Definition : An integer $b \in Z_n$ is said to be **invertible** or a **unit** of Z_n , if there is an integer $x \in Z_n$, such that $bx \equiv 1 \pmod{n}$. If such an x exists, then it is referred to as the **multiplicative inverse** of b in Z_n, and denoted by b^{-1} .

Theorem : Let a, b and n > 0 be integers , and g = gcd (a,n). The congruence $ax \equiv b \pmod{n}$ has a solution if and only if g|b. If this condition is met, then the solutions form an arithmetic progression with common difference n/g, giving g solutions modulo n.

A proof can be found [29] in Page 62. Therefore, $b \in Z_n$ has a multiplicative inverse if and only if gcd (b, n) = 1 . Therefore, if n is prime, every non –zero $b \in Z_n$ has a multiplicative inverse.

Theorem (Chinese Remainder Theorem) : Suppose n_1 , n_2 , …, n_r are r positive integers that are pair-wise coprime, and let a_1 , a_2 ,…, a_r denote any r integers.

Then the congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$x \equiv a_r \pmod{n_r}$$

have a common solution which is unique modulo $n = n_1 n_2 \ldots n_r$.

A proof can be found [20] in Page 136.

So given n_1 and n_2 coprime any pair of simultaneous congruences

$x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$ have the same solutions as the single congruence $x = a_2 t_1 n_1 + a_1 t_2 n_2 \pmod{n_1 n_2}$,

where $t_1 n_1 + t_2 n_2 = 1$. In particular , if $a_1 = a_2$, then $x \equiv a_1 \pmod{n_1 n_2}$.

Definition : The multiplicative group of Z_n is $Z_n^* = \{ a \in Z_n \mid \gcd(a,n) = 1 \}$.

Definition : Let $a \in Z_n^*$. The **order** of a , denoted 0(a), is the least positive integer k such that $a^k \equiv 1 \pmod{n}$.

Theorem (Fermat's Theorem) : Let p be a prime. If (p,a) = 1, then $a^{p-1} \equiv 1 \pmod{p}$. A proof can be found [20] in Page 187.

Definition : The **Euler Totient Function** $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n. Note that $\phi(n) = |Z_n^*|$.

Theorem (Euler's Theorem) : Let n ≥ 2 . If gcd (a,n) = 1 , then $a^{\phi(n)} \equiv 1 \pmod{n}$.

A proof can be found [20] in pages 203 – 204.

Corollary : If gcd(a,n) = 1 then 0(a) modulo n divides $\phi(n)$.

A proof can be found [20] in Page 98.

Theorem : Let n = 1, 2 , 4, p^{α} , or $2p^{\alpha}$, where p is an odd prime. If gcd(a,n) = 1, then the congruence $x^b \equiv a$ (mod n) has gcd (b, ϕ(n)) solutions or no solutions, according to whether $a^{\phi(n)/gcd(b,\phi(n))} \equiv 1$ (mod n) or not.

1.5 Computational Primitives

Number theory is the source of several computational problems that serve as primitives in the design of cryptographic schemes.

The security of many cryptographic techniques depends upon the hardness (intractability) of a certain computational problems.

We only review the "Integer Factorization" and "Discrete logarithm" problems, which are the most widely – used computational problems in public key cryptographic schemes.

1.5.1 The Integer Factorization Problem : The integer Factorization problem, can be informally defined as follows :

"Given a positive integer n, find its prime factorization, that is, write $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where the p_i are pair-wise distinct primes and each $e_i \geq 1$".

This problem is believed to be hard for general n where n is large. Some ingeneous methods have been devised in an attempt to factorize large composite numbers n. The three methods that are most effective on very large numbers are quadratic sieve, the elliptic curve method and the number field sieve. Other well known methods that were precursors include Pollard's rho-method and P-1 method, William's P+1 method, the continued fraction algorithm, and of course, trace division. A good overview of factoring methods can be found in [28].

We remark that the integer factorization problem and its related computational problems were used to build up various cryptographic schemes by RSA [28], Rabin [27], Okamoto and Uchiyama [21] and Paillier [23].

1.5.2 Discrete Logarithms :

Another widely used computational problems is the Discrete Logarithms problem.

Let G be a finite cyclic group of order n with generator g. For a more concrete approach, one may find it convenient to think of G as the multiplicative group of integers modulo p (for p prime).

Definition :

Let G be a finite Cyclic group of order n. Let g be a generator of G, and y $\in$ G. The Discrete logarithm of y to the base g, denoted by $\log_g y$, is the unique integer x, $0 \leq x \leq n-1$, such that $y = g^x$.

The discrete logarithm problem, which we simply call the "DLP", can be informally defined as follows :

"Given a prime p, a generator g of Z_p^*, and an element $y \in Z_p^*$, find the integer x, $0 \leq x \leq p-2$ such that $y = g^x \bmod p$".

As in the case of factorization, efficient technique exist for solving the discrete logarithm problem when the group G has a particular structure, an example of such a technique being the Pollig – Hellman algorithm [24], which efficiently computes discrete logarithms when the group G has order

$n = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$, where p_1 , p_2 ,…, p_r are primes less than or equal to a small bound B. A good overview of techniques for calculating discrete logarithms can be found in [14].

1.5.3 Diffie – Hellman Problem

The Diffie–Hellman problem is closely related to the well studied discrete logarithm problem (DLP). The Diffie – Hellman problem (DHP) is the following:

"Given a prime p, a generator g of Z_p^* and elements $g^a \bmod p$ and $g^b \bmod p$, find $g^{ab} \bmod p$".

The generalized Diffie – Hellman problem (GDHP) is the following :

"Given a finite cyclic group G, a generator g of G, and group elements g^a and g^b , find g^{ab}" .

Suppose that the discrete logarithm problem in Z_p^* could be efficiently solved. Then given (g, p, g^a mod p, g^b mod p), one could first find a from (g, p and g^a mod p) by solving a discrete logarithm problem, and compute ($g^b)^a = g^{ab}$ mod p. Thus, the DHP is no harder than DLP.

For attack algorithms on the Discrete Logarithm problem in a general group D Shank's "baby–step , gaint step " and Pollard's ρ methods are used. As a sub exponential algorithm for solving the DL problem in Z_p^* , the "index calculus " method is well known.

Finally, we remark that there have been a large number of cryptographic schemes based on the above problems. Examples include the digital signature schemes based on the Discrete Logarithm problem such as ElGamal [6], Schnorr [30], and Digital singrutune standard (DSS) [19] ; the public key encryption schemes based on DHP such as Pointcheral [25], Beak – Leen –Kin [1], Tsiousnis – Yung [33], and Cramer – Group [4].

The Quadratic Residuosity Problem :

The security of the Gold Wassar – Micali probabilistic encryption scheme is based on the hardness of the quadratic residuosity problem (QRP).

Definition : (To be defined quadratic residue)

Definition : (QRP): Given an odd composite integer n and a $\in J_n$ (the Jacobian symbol), decide whether or not a is a Quadratic residue modulo n.

1.6 Cryptography

The word Cryptology stems from Greek meaning "hidden word", and is the umbrella term used to describe the entire field of secret communications. Cryptology splits into two subdivisions : Cryptography and Cryptanalysis.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, data origin authentication and non – repudiation. The Cryptanalyst seeks to undo the Cryptographer's work by breaking a cipher or by forging coded signals that will be accepted as authentic.

General information as Cryptography can be found in [16] , [32], and [31]; There are two major types of Cryptosystems. One is Symmetric – key Cryptosystems and the other is public – key cryptosystems. We will pay particular attention to public – key cryptosystems. Thus, we give a formal definition of a Cryptosystem.

Definition : A Cryptosystem is a five – tuple (M,C, K, E, D), where the following conditions are satisfied.

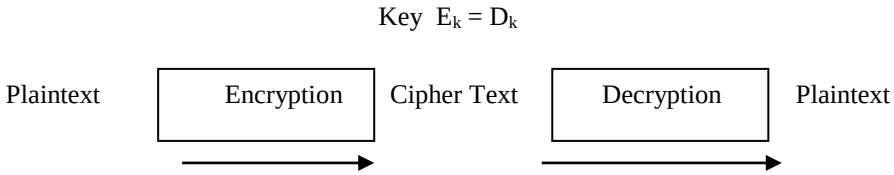
1. M is a finite set of possible plain texts or messages.
2. C is a finite set of possible cipher texts or cryptograms.
3. K is a finite set of possible keys.
4. For each k $\in$ K, there is an encryption rule $E_k \in \varepsilon$ and a corresponding decryption rule $D_k \in D$. Each $E_k : M \rightarrow C$ and $D_k : C \rightarrow M$ are functions such that $D_k (E_k(m)) = m$ for every message m $\in$ M.

The main property is property 4. It is the property that enables a user to decrypt a received ciphertext, since $D_k(E_k(m)) = m$ for all messages m $\in$ M . For unambiguous decryption, it is obviously required that $E_k(m_1) \neq E_k(m_2)$ if $m_1 \neq m_2$. Otherwise , if $E_k(m_1) = E_k(m_2)$, $m_1 \neq m_2$, decryption is not unique, and therefore it is not possible for a user to decide whether the intended message was m_1 or m_2 upon receipt of $E_k(m_1) = E_k(m_2)$.

1.6.1 Symmetric – Key Crytography

Consider an encryption scheme consisting of the sets of encryption and decryption transformations $\{ E_k \mid k \in K \}$ and $\{ D_k \mid k \in K \}$, respectively, where K is the key space. The encryption scheme is said to be symmetric – key if for each encryption or decryption transformation pair (E_k , D_k), it is computationally "easy" to determine D_k knowing only E_k and to determine E_k from D_k .

Since $E_k = D_k$ in most practical symmetric – key encryption schemes, the term symmetric – key becomes appropriate. Other terms used in the literature are single key, one – key, and conventional encryption,



Symmetric Cryptography

1.6.2 Public – Key Cryptography :

The concept of public key cryptography was first introduced by Diffie and Hellman [5] in 1976. The main motivation for public key cryptography is to remove the burden of key sharing in the symmetric – key cryptography in which a separate key needed for each pair of users to communicate in private. More precisely, if there are n users who want to exchange secret data using the symmetric key cryptography, n(n-1)/2 keys are needed and this number increases rapidly as the number of users grows. Yet, in public key cryptography, each user creates a pair of keys, one of which is to be publicized while the one is kept secret. The publicized key, referred to as "public key " , is used as encryption key, but the secret key, referred to as "private key " , is used as decryption key. As a result, there is no key sharing problem as in symmetric key cryptography. Another remarkable achievement of public key cryptography is that one can construct a digital signature scheme by using the private key as signature generation key while using the public key as verification key.

1.7 Public – Key Encryption

A public key encryption scheme is one of the fundamental public key cryptographic schemes and can be described as follows.

* (descryption of Alice & Bob)

Key Generation	:	The Bob (receiver) creates his private key and public key pair, which we denote by SK_B and PK_B respectively.
Encryption	:	Using Bob's public key PK_B , the Alice (sender) encrypts her message m, which we call a 'plain text ' and obtains a ' Cipher text ' C.
Decryption	:	Upon receiving the cipher text C from Alice, Bob decrypts it using his private key SK_B to recover the plain text m.

The following figure illustrates schematic out line of a public key encryption scheme.

Of course, Bob's public key PK_B should not compromise the secrecy of the private key SK_B . This is an important property is guaranteed by the trapdoor one way function which can be informally defined as follows :

Definition : One – way function : A one way function is a function $f : X \rightarrow Y$ such that for each $x \in X$ (domain), it is easy to compute f(x) ; but for all $y \in Y$ (range), it is computationally infeasiable to find any x such that y = f(x).

Definition : Trapdoor One-way Function. A trapdoor one – way function is a one way function f with the additional property that gives some extra information (called the trapdoor information), it becomes computationally feasible to compute an x for any $y \in Y$ such that $y = f(x)$.

In their seminal paper [5], Diffie and Hellman constructed a trapdoor one–way function based on module exponentiation. This function made it possible for them to design a surprising protocol in which the remote users who have not met each other before can share the common secret key. This protocol is known as the "Diffie – Hellman key exchange protocol".

However, the first practical realization of public key (encryption) Cryptosystem was accomplished by Rivert, Shamir and Adleman [28] in 1978. Their public key (encryption scheme) cryptosystem , which we simply call "RSA public–key cryptosystem " . This cryptosystem works in Z_n, where n is the product of two large primes p and q, and its security is based on the difficulty of factoring n.

The RSA cryptosystem can be described as follows :

Key Generation : The receiver Bob chooses large primes p and q at random ; compute $n = pq$; computes $\phi(n) = (p-1)(q-1)$ choose a random integer e,

where $0 < e < \phi(n)$ such that gcd (e, $\phi(n)$) = 1 ; using the Euclidean algorithm to compute the unique integer d, where $0 < d < \phi(n)$, such that $ed \equiv 1 \pmod{\phi(n)}$; publicize his public key $PK_B = (n, e)$ while keeps his private key $SK_B = (p,q,d)$.

Encryption : Using Bob's public key PK_B , the sender Alice represents her message m as an integer in the range 0, 1 2,…, (n-1) and encrypts m by creating a ciphertext c such that

$$C = m^e \pmod{n}$$

Decryption : Upon receiving the cipher text c from Alice, Bob decrypts it using his private key SK_B and recover the plain text m by computing.

$$m = c^d \pmod{n}$$

Note that the one–wayness of the above RSA scheme is based on the intractability of computing the e–th root of a cipher text c modulo integer n, which is related to the "Integer Factorization Problem ".

Soon after Rivest , Shamir , and Adleman proposed the above encryption scheme, ElGamal [6] constructed a new Public – key Cryptosystem , which can be described as follows .

ElGamal public – key cryptosystem : This cryptosystem can be based on any family of groups for which the discrete logarithm is considered intactable. Usually a subgroup G_q of order q of Z_p is used, where p, q are large primes satisfying $q \mid p-1$. We present the construction in the group Z_p , where p is a large prime.

Key generation : The receiver Bob chooses large prime p and a generator g of the multiplicative group Z_p of the integers modulo p. Bob also selects a random integer α , $1 \le \alpha \le p-2$, and computes $h = g^{\alpha}$. He publicizes his public key $PK_B = (p, g, h)$ while keeps his private key $SK_B = \alpha$.

Encryption : Using Bob's public key PK_B , the sender Alice encrypts her message m ($0 \le m < p$) for Bob. Alice do the following :

Select a random integer k, $0 \le k \le p-2$, computes $x = g^k$, $y = m.h^k$ and send this ciphertext $c = (x,y)$ to Bob.

Decryption : Upon receiving the cipher text C from Alice, Bob decrypts it by using his private key $SK_B(=\alpha)$ and recovers the plain text m by computing $m = \frac{y}{x^{\alpha}}$.

1.8 Probabilistic Encryption

In 1948, Glod wassar and Micali [9] introduced the notation of probabilistic encryption. A probabilistic encryption method allows one to encrypt a fixed value in many different ways. Thus, even given the encryption of a value and details of encryption mechanism, it is not necessarily possible for an adversary to determine or not the encryption represents the encryption of a chosen value.

Gold Wassar and Micali develop a bit encryption function based on the problem of quadratic residusosity problem.

"QRP: Given and odd composite positive integer n and an integer z having Jacobian symbol +1. Decide whether are not z is a quadratic residue modlo n".

This is a simple effective polynomial time procedure originally due to Gauss [8] which computes the Jacobian symbol of an integer with respective given modules. There is, however no known polynomial time procedure to, without factorization of n, determine whether or not an integer with Jacobian symbol +1 to quadratic residue modules. In addition, given a single integer z of Jacobian symbol +1 which is not in Qn, it is possible to uniformly select quadratic residues or quadratic non-residues modules, even if the factorization of n is not known.

Thus, a probabilistic public-key bit encryption function proposed by Gold Wassar and Micali can be defined by a user by selecting an n of known factorization n = pq, where p,q are distinct odd primes and realizing this n together with a z of Jacobian symbol +1 which is not in n. An encrypted bit may be sent to his user by realizing a quadratic residue to indicate a zero or a quadratic non residue of Jacobians symbol +1 to indicate a one. The user which posses the factorization of n can easily determine which is the case. Without the factorization, however distinguishing between the how cases is an apparently difficult problem.

1.9 Digital Signature Scheme

Another fundamental public key cryptographic scheme is a digital signature scheme, whose concept was first proposed by Diffie and Hell man [5]. As mentioned earlier, the ability to construct a digital signature scheme is a great advantage of public key cryptography over symmetric-key cryptography. A digital signature scheme can be described as follows:

Key generation : The signer Alice creates her private key and public key pair, which we denote by SK_A and PK_A respectively.

Signature Generation : Using her private key SK_A, Alice creates a signature σ on his message m.

Signature verification: Having obtained the signature σ and the message m from Alic, the verifier Bob checks whether σ is a genuine signature on M using Alic's public key PK_A. If it is, he returns "Accept". Other wise he returns "Reject".

Since only a single entity is able to sign a message and the resulting signature is verifier by anybody in digital signature, a dispute over who created the signature can be easily settled. This often called "non-repudiation", is one of the important security services that digital signature schemes can provide.

Indeed, non-repudiation is an essential security requirement in electronic commerce applications.

Key Generation: The signer Alice chooses large primes p and q at random; computes n=pq; computes φ (n) = (p-1) (q-1); chooses a random integer e<φ(n) such that gcd

(e, φ(n)=1, computes the integer d such that ed=1 (mod φ (n)); Public her private key PK_A=(n,e) while keys her private key SK_A=(p,q,d) secret.]

Signature generation: Using her private key SK_A, Alice creates a signature on her message m by computing $\sigma = m^d \bmod n$.

Signature Verification : Having obtain the signature σ and the massage m from Alice, Bob checks wether $m=\sigma^e \pmod n$.

Using Alice's public key PK_A. If the above equation holds Bob returns "Accept". Otherwise, he returns "Reject". The unforgeability of the above RSA signature scheme sis again based as the intractability of computing eth root of a Cipher text C modulo integer n.

We remark that the construction of signature scheme bases on the "Discrete logarithm problem, which we discussed in section was given by ElGamal [6].

CHAPTER – II
INTRODUCTION TO ELLIPTIC CURVES AND ELLIPTIC CURVE CRYPTOGRAPHY

2.1 Introduction

From the beginning of the public key cryptography there are two major cryptosystems namely RSA & ElGamal that seem to defeat all attacks. For this reason, these two cryptosystems are the most respected and widely used public-key cryptosystems now a days. One can use both cryptosystems for encryption, decryption and digital signature schemes. All important security standards cover those cryptosystems, so it should be safe to use implementations of these systems.

Elliptic curve cryptosystems were invented around 1985 independently by Miller [17] and Koblitz [11]. Since their introduction a broad discussion on their security and efficiency has been carried on. It is very efficiency that makes them so interesting for us to day. This is due to the fact that information technology is developing very fast. For example, most computers today do not look like the old fashioned personal computers anymore. We use handhelds, and mobile phones and of course we have a need in securing communication on these devices. But in this case there have to be several constraints taken into account: this is very limited memory and computing power on these device and it not possible to spend much band width for communications over head. What we need is a cryptosystem with small keys, and a small signature size. Efficient encryption / decryption is not so important because there operations are usually done with a private key cryptosystem.

Elliptic curve cryptosystem has exactly the desired properties. This comes from the fact that there are no sub-exponential algorithms for Elliptic curse Discrete Logarithm Problem known to day. This means that we can use shorter keys (compared to the other cryptosystems) for high security levels.

2.2. Contribution of this chapter

In this chapter we will discuss several aspects of elliptic curves and elliptic curve cryptography. First we will treat them more as mathematical objects, and then we discuss more cryptography related Stuff. Everything is this chapter is written in a cryptographers view. This means, we know same properties that a cryptosystems must have, and we asserts that they hold for elliptic curve cryptography.

2.3 Basic Facts about Elliptic Curves

Definition-1. An elliptic curve **E** over the field **F** is a smooth curve in the so called "long weierstrassform".

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad a_i \in F \qquad (1)$$

We let E(F) denote the set of points (x,y) Є F^2 that satisfy this equation, along with "a point at infinity" denoted ∂.

Note that smooth means that there is no point in E($\bar{F}$) where both partial derivatives vanish. The definition given above is valid for any field. But in cryptography we are only interested in finite fields. Considering only finite fields we get an "easier' equation. Two finite fields are of particular interest. The finite field F_p with p Є P elements, because of it's structure, and the finite field F_{q^m} with q = p^r elements, since setting p = 2 the arithmetic in this field will be well suited for implementations in hardware.

2.3.1 Elliptic Curves over Prime Finite Field

We start with F_p (p Є P, p > 3, char (F_p) ≠ 2,3)[1] and perform the following change of variables

$$x \to x - \frac{a_2}{3}$$

$$y \to y - \frac{a_1x + a_3}{2}$$

Let's take a look what is happening to the left side after the substitution for

$$Y : (Y\text{-}a1X+a_3)/2)^2 + a_1X(Y\text{-}(a_1X+a_3)/2) + a_3\,(Y\text{-}(a_1X+a_3)/2$$

$$=\ldots\ldots=Y^2 - a_1^2X^2/4 - a_1a_3X/2 - a_3^2/4$$

Both, XY and Y have vanished, so their coefficients a_1 and a_3 must equal zero! That reduces the left side to a singe to a single Y^2. If we make the substitution for X and take a look at the right side of (1) we get :

$$(X-a_2/3)^3 + a_2(X-a_2/3)^2 + a_4 (X-a_2/3) + a_6$$

$$= \ldots\ldots = X^3 + a^2/9+a_4)X+2a_2^3/27-a_2/3a_4a_6$$

$$= \ldots\ldots \text{ Setting } \left(\frac{1}{9}a^2 + a_4\right) = a \text{ and } \frac{2}{27}a\frac{3}{2} - \frac{1}{3}a_2a_4a_6 = b$$

we have the much nicer form X^3+aX+b. In F_p equation (1) reduces to

$$Y^2 = X^3 + aX + b. \qquad (2)$$

2.3.2 Elliptic curve over Binary Finite Fields

Now we work in the field ($G_F(2^m)$ where we have characteristic=2. Here we only consider so called" nonsupersingular curves". They have the property $a_1 \neq 0$. So we can make the following change of variables:

$$X \rightarrow a_1^2X + \frac{a_3}{a_1}$$

$$Y \rightarrow a_1^3Y + \frac{a_1^2a_4 + a_3^2}{a_1^3}$$

This leads us to following definition.

Definition 3. A (nonsupersingular) elliptic curve E over the finite field F_2^m is given through an equation of the form

$$Y^2+XY = X^3+aX^2+b, \qquad a, b \in F_2^m. \qquad (3)$$

2.3.3 Addition Law

In order to define a cryptosystem on the set of points on an elliptic curve, we need to define an algebraic structure on the points. The easiest algebraic structure which provides us with all necessary tools is the group. Therefore we need to define an neutral element, inverse element, and the addition of two elliptic curve points which needs to be associative.

Definition 4. Let E be an elliptic curve over F_p or F_2^m, and let P and Q be two point on E.

1. Zero element: If P is the point ∂, then we define – p to be ∂. For any point Q we define ∂ +Q to be Q. In F_p we can visualize ∂ as sitting infinitely far up the y-axis
2. Inverse element: In F_p we define the negative of the point P=(x,y) to be –P=(x,-y). If Q= -P, then we define P+Q= ∂. For F_2^m we define –P =(x,x+y).
3. P+Q: If P≠Q, then we shall soon show that the line l= $\overline{PQ}$ intersects the curve in exactly one more point R. Then we define P+Q to be–R, that is the inverse of the third point of intersection.
4. 2P: Let l be the tangent line to the curve at P, let R be the only (the third) point of intersection of l with the curve, and define 2P = -R.

This set of rules can be summarized in the following succint manner:

The sum of the three point where a line intersects the curve is zero.

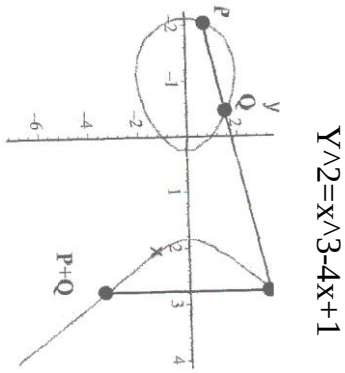


Fig. I : Point addition

We now show, why there is exactly one more point where the line l through P and Q intersects the curve, and we derive formulas for the point addition. We restrict or calculations here on the field F_p because the other case can be treated in the same fashion. Let P=(x_1,y_1)Q=(x_2, y_2), R(x_3, y_3) we'd like to express x_3 and y_3 in terms of x_1, y_1,x_2,y_2.

We first discuss the case where P≠Q. Let y=αx+β be the equation of the line through P and Q. Then we have $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$, and $\beta = y_1 - \alpha x_1$. A point (x,αx+β) lies on the elliptic curve if and only if $(\alpha x+\beta)^2 = x^3+ax+b$. Thus, there is one intersection point for each root of the cubic equation. We already know the two roots $x_1$and x_2, because they correspond to the points P and Q on the curve. Since there are at most three roots of the cubic equation, we conclude that the third root must equal to x_3. It is easy to show that the sum of the roots of a monic polynomial is equal to minus the coefficient of the second – to-highest power, so we conclude that this third root is $x_3=\alpha^2-x_1-x_2$. (Compare the coefficients of the equations $(x-x_1)(x-x_2)(x-x_3)$ and $x^3-(\alpha x+\beta)^2+ax+b$). We also know that

$$y_3 = -((\alpha x_3+\beta) = \alpha(x_1-x_3)-y_1$$

The case when P=Q is similar, except that α is now the derivative dy / dx at P. Implicit differentiation of equation (3) leeds to $\alpha = (3x_1^3+a)/2y_1$, and we obtain the formula for the coordinates of 2P. The following table lists all obtained formulas together with the formulas for F_2^m.

	F_p	F_2^m
P+Q	$x^3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$	$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \left(\frac{y_1 + y_2}{x_1 + x_2}\right) + x1 + x2 + \alpha$
	$y^3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$	$y^3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_2) + x_3 + y_1$
2p	$x_3 = \left((3x_1^2 + a)/2y_1\right)^2 - 2x_1$	$x_3 = x_1^2 + \frac{b}{x_1^2}$
	$y_3 = -y_1 + \left((3x_1^2 + a)/2y_1\right)^2 (x_1 - x_3)$	$y^3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3$
-P	$(x,-y)$	$(x, x + y)$

2.4. Properties of Cryptographic Interest

Here we discuss some topics, which are of interest for cryptographers. We already defined an algebraic structure called "elliptic curve" and found a way to make the set of points on such a curve to an abelian group. Basically we could start building a cryptosystem, but there are some more questions that should be considered in advance.

- How "big" is an elliptic curve ?
- How do I find a point on an elliptic curve ?
- How do I find a curve ?

In the rest of this section we will mostly deal with the finite field F_q, where $q = p^r$.

2.4.1 Calculating the number of points on an elliptic curve over F_q :

With the following easy counting method it is possible to give an lower and an upper bound for the number of F_q points. Therefore we choose an $x \in F_q$ and assert if there is a corresponding y on the curve i.e. we look if $f(x) = x^3 + \alpha + b$ is a square in F_q. We restrict our considerations to the case q = p. Then we can introduce the $(easier)^2$ notation which is used to work with squares, or how mathematicians call them "quadratic residues" (short QR).

Definition 6 (The Legendre symbol). Let a be an integer and p > 2 be a prime. The Legendre symbol (a/p) is defined as follows :

$$(a/p) = \begin{cases} 0, & \text{if } p/a; \\ 1, & \text{if a is quadratic residue modulo P} \\ -1, & \text{if a in not a quadratic residue modulo P} \end{cases}$$

The Legendre symbol tells us whether or not an integer is a quadratic residue modulo p. A simple method to compute the value of the Legendre symbol is given in the next proposition.

Proposition 2

$(a/p) = a^{(p-1)/2} \bmod p$.

Proof. For the trivial case where a = 0 both sides are $\equiv 0 \bmod p$. suppose a >0 and $p \neq a$. Fermats little theorem states that the square of $a^{(p-1)/2}$ is 1, so $a^{(p-1)/2}$ itself is ± 1. Let g be a generator of F_p^* and let $a = g^j$ is a quadratic residue if and only if j is even. And $a^{(p-1)/2} = g^{j\,(p-1)/2}$ is 1 If and only if j(P-1)/2 is divisible by (P-1) i.e. if and only if even. Thus both sides are ± 1 in F_p, and each side is +1 if and only if α is a square.

Depending whether f(x) is a quadratic residue or not modulo q, we can have the following cases.

- f(x) is QR : Then there are two points $(x, \pm y)$
- f(x) divides p : Then there is a single point (x, 0).
- F(x) in not QR : Then there is no point

Putting all three cases into one formula results in

$$\neq E(F_q) = 1 + \sum_{x \in F_q} \left(1 + \left(\frac{f(x)}{q}\right)\right) = q + 1 + \sum_{x \in F_q} \left(\frac{f(x)}{q}\right)$$

2.4.2 Constructing an Elliptic curve over a given finite field

We motivate this section with the following

Example 2. Let E be the elliptic curve given through the equation $y^2 = x^3 + 3x + 1$ over F_p, $P = 10^7 + 19$. The order of the curve is $n = \neq E(F_p) = 9999846 = 2.3^2.347.1601 = 18.347.1601$. We take the curve points P = (2,4417259) and Q = (1, 866032) with Q = xP, x unknown. If we want to determine x we have to solve the elliptic curve discrete logarithm problem which is the analog of the discrete logarithm problem and will be defined more formatly in the next section. This problem is the underlying problem of all cryptosystems based on elliptic curves and has to be hard! But know look at this: Since we know the factorization of n we get the following set of equations

$$x \frac{n}{18} P = \frac{n}{18} Q \quad \text{given } x \equiv 14\,(18)$$

$$x \frac{n}{347} P = \frac{n}{347} Q \quad \text{given } x \equiv 81\,(347)$$

$$x \frac{n}{1601} P = \frac{n}{1601} Q \quad \text{given } x \equiv 854\ (1601)$$

We know for example that 18. n/18P = nP = ∂ so we can reduce the space for the possible values of x significantly (we just have to look between zero and 17). Now we can easy check every x and get the relation x ≡ 14 (18). According to this method we can obtain all of the left equations. Then just have to apply the Chinese remainder theorem to get x = 5553122.

The method sketched in the example is called Silver-Pohlig-Hellman method. It works so well in the example because n has small divisors (one says E has "smooth" order). It is clear that for cryptographic purposes one should avoid those curves!

This makes our effort in obtaining curves even more difficult. We have to find a curve (over a given finite field) which does not have a smooth order and additionally has a base point with large (prime) order. This can be accomplished by the following four approaches:

- Select a curve equation at random, compute its order directly, and repeat this process until an appropriate order is found.
- Select curve coefficients with particular (desired) properties, compute the curve order directly, and repeat the process until an appropriate order is found.
- If $q=2^m$ where m is divisible by a "small" integer d, then select a curve defined over F_{2^d} and compute its order over F_{2^m}. Repeat if possible until an appropriate order is found.
- Search for an appropriate order, and construct a curve of that order.

2.5 Elliptic Curve Cryptosystems

We are familiar with public key cryptography know the definition of the discrete logarithm problem in the multiplicative group of a finite field. We can give an analog definition for the group of points on an elliptic curve.

Definition : If E is an elliptic curve over F_q and B Is a point of E, then the discrete log problem on E (to the base B) is the problem, given a point $P \in E$, of finding an integer $x \in Z$ such that xB = P if such an integer x exists.

What can we say about the hardness of this problem? Until 1990, the only discrete log algorithms known for an elliptic curve cryptosystem were the ones that work in any group. These are exponential time algorithms, provided that the order of the group is divisible by a large prime factor. Menezes, Okamoto and Vanstone found a new approach to the discrete log problem on an elliptic curve. They used the Weil pairing to embed the group of points on E into the multiplicative group of some extension field $F_q k$ It is essential for the extension degree k to be small. The only elliptic curves for which k is small are the so-called "super singular" curves.

2.5.1 Embedding plaintext on an elliptic curve

Suppose we would like to encrypt some plaintext with ECC. There has to be a method, which takes some arbitrary text and embedded it in elliptic curves, i.e. which gives a bisection between the points on an elliptic curve and a plaintext block. We sketch such an algorithm.

1. Step: We choose an alphabet with N letters and fix the length l of a plaintext block. The characters of the alphabet are then identified with the numbers 0, ….., N-1. With the following assignment we get a bijection between the plaintext blocks w and the numbers $0 \le x_w \le N^l$:

$w = (a_0 a_1 \ldots a_l\text{-}1) \rightarrow x_w = a_o N^{l-1} + a_1 N^{l-2} + \ldots + a_{1\text{-}2} N + a_l\text{-}1,\ 0 \le x_w \le N^l$:

Idea : For such an x_w there need not be a point on the elliptic curve. But it should be possible to find the "next" curve point x_1 close to x_w efficiently. Given a number k we would like to have a high probability (i.e. $1 = (1/2)^k$) for $x_w \le x_1 < x_w + k$.

2. Step : We choose an appropriate k, i.e. that the success probability is high and that $q > kN^1$. For each j we obtain an element of F_q through $kx_w + j$. We take the first curve point $(j \ge 0)P_w$ with x-coordinate $\ge kx_w$, i.e. $P_w = (kx_w + j, *) \in E(Fq)$.

3. Step : We can recover the plain text block from the point by

$x_w = (x / k)$

2.5.2 Elliptic Curve Diffe-Hellman key exchange (ECDH)

Suppose two communication parties, Alice and Bob, want to agree upon a key which will be later used for encrypted communication in conjunction with a private key cryptosystem. They first fix a finite field F_q, an elliptic curve E defined over it and a base point $B \in E$ (with high order). To generate a key, first Alice chooses a random $a \in F_q$ (of high order) which she keeps secret. Next she calculates a $B \in E$ which is public and sends it to Bob. Bob does the same steps ie. she chooses a random integer b (secret) and calculates bB which is sent to Alice. Their secret common key is then $P = abB \in E$.

2.5.3 Analog of ElGamal

We start with a fixed publicly known finite field F_q, an elliptic curve E defined over it and a base point $B \in E$. Each user chooses a random integer a, which is kept secret and computes the point x = aB which is the public key. To send a message P to Bob. Alice chooses a random integer k and sends the pair of points (kB, P + k(bB))(where bb is Bobs public key) to Bob. To read the message, Bob multiplies the first point in the pair by his secret b and subtracts the result from the second point : P + k (bB) – b (kB) = P.

2.5.4 Elliptic Curve Digital Signature Algorithm (ECDSA)

The ECDSA is the elliptic curve analog of the DSA. ECDSA was first proposed in 1992 by Vanstone. In response to NIST's (National Institute of Standards and Technology) request for comments on their first proposal for DSS. Digital signature schemes are the counterpart to handwritten signatures. A digital signature is a number that depends on the secret key only known by the signer and on the contents of the message being signed. Signatures must be verifiable without access to the signer's private key. Signatures should be existentially unforgeable under chosen message attacks. This asserts that an adversary who is able to obtain Alice's signatures for any messages of his choice cannot forge. Alice signature on a single other message.

Suppose Alice wants to send a digitally signed message to Bob. They first choose a finite field F_q, an elliptic curve E, defined over that field and a base point G with order n. Alice's key pair is (d, Q), where d is her private and Q is her public key. To sign a message M Alice does the following :

1. Choose a random number k with k:$1 \leq k \geq n - 1$.
2. Compute $kG = (x_1, y_1)$ and $r = x_1 \bmod n$. If r=0 then go to step 1
3. Compute $k^{-1} \bmod n$.
4. Compute e = SHA-1(M)
5. Compute $s = k^{-1} (e+dr) \bmod n$. If s = 0 then go to step 1.
6. Alice signature for the message M is (r, s).

ECDSA Signature Generierung

To verify Alice's signature (r, s) on the message m, Bob obtains an authentic copy of Alice's parameters and public key. Bob should validate the obtained parameters ! Bob then does the following :

1. Verify that r, s are integers in the intevall (1, n-1)
2. Compute e = SHA-1 (M)
3. Compute $w = s^{-1} \bmod n$.
4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
5. Compute $X = u_1G + u_2Q$. If $X = \partial$ then reject the signature.

   Otherwise compute $v = x_1$ and n where $X = (x_1, y_1)$.
6. Accept the signature if and only if V = r.

ECDSA Signature Verification

If the signature (r,s) on the message m was indeed generated by Alice, the $s = k^{-1}(e+dr)$ (n). With this information we have

$K \equiv s^{-1} (e + dr) \equiv s^{-1} e + s^{-1} rd \equiv we + wrd \equiv u_1 + u_2d$ (n). Thus $u_1G + u_2Q = (u_1 + u_2d) G = kG$ and so v = r as required. For a discussion on known attacks and how they can be avoided consult (4).

CHAPTER – III
TRAPDOORING FACTORIZATION ON ELLIPTIC CURVES OVER RINGS

3.1 Introduction

In 1976, Diffie and Hellman introduced the concept of a trapdoor one-way function (TOF). A TOF is a function that is easy to evaluate but infeasible to invert, unless a secret trapdoor is known in which the case inversion is also easy.

The first implementation of a TOF was proposed by Rivest, Shamir and Adleman in 1978 [28]. Its security relies on the difficulty of factoring a composite number n. some other implementation of TOF have been proposed based on the difficulty of factoring and discrete logarithm. Form another direction, one of the recent topics in the field of elliptic curves is their applicability to cryptography. The points of an elliptic curve E over a finit field form an abelian group. Hence the group E can be used to implement analogs of the Diffie Hellman key exchange scheme and the ElGamal public key cryptosystem as explained in [6] .

The security of these analogous systems rests on the difficulty of the discrete logarithm problem on an elliptic curve.

3.2 Contribution of this Chapter

In this chapter we review a TOF (or public key cryptographic schemes) based on elliptic curves over a ring Z_n* [13] although an elliptic curve E over Z_n does not form a group. The security of this TOF depends on the difficulty of factoring n. Although these schemes are less efficient than the RSA and Rabin schemes, this scheme seem to be move secure from the view point of some attacks that do not use factoring such as low multiplier attacks. From the some reasons, even when the RSA system can be broken without factoring the modules, this scheme seems to remain secure.

Also we present a public key cryptosystem based on elliptic curves over the ring Z_n. This scheme can be used for both digital signatures and encryption applications does not expand the amount of data that needs to be transmitted and appears to be immune from homomorphic attacks. The main advantage of this scheme is very little restriction on the types of elliptic curves and types of primes that can be used. In addition, the system works on fixed elliptic curves. The security of the systems relies on the difficulty of factoring large composite numbers.

3.3 Elliptic curves over a finite field

Let F be the field of characteristics ≠2,3 and let a, b ∈ F be two parameters such that $4a^3 + 27b^2 \neq 0 \rightarrow$ (A1).

An elliptic curve over F with parameters a, b is defined as the set of points (x,y) with x,y∈F satisfying the equations $Y^2=x^3+ax+b \rightarrow$ (A2) together with a special element ∞ and called the point at infinity.

Let E be an elliptic curve and let P and Q be two points on E. The point P+Q is defined according to the following rules. If P=∞ thus –P=∞ and P+Q=Q

Let $P=(x_1,y_1)$ and $Q=(x_2,y_2)$. If $x_1=x_2$ and $y_1= -y_2$ then P+Q=∞. In all other cases the co-ordinates of $P+Q = (x_3,y_3)$ are computed as follows. Let λ be defined as

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \end{cases}$$

$$\begin{cases} \dfrac{3x_1^{\,2}+a}{2y_1} & \text{if } x_1 \neq x_2 \end{cases}$$

The resulting point P+Q = (x_3,y_3) is defined as

$$X_3=\lambda^2-x_1-x_2$$

$$Y_3=\lambda(x_1-x_2)-y_1$$

Clearly, the first equation is equivalent to $x_3=\lambda^2-2x_1$ when P=Q. All computations are in the field over which E is defined. In particular in the field is F_p, all computations are modulo P.

It is straight forward to verify that the defined addition operation satisfies the axioms for a group.

The order of the group, denoted by $|E_p(a,b)|$, is given by $\left|Ep(a,b)\right| = 1+\sum_{x=1}^{p}\left(\left(\frac{Z}{P}\right)+1\right)$ Where (Z/P) is the Legender Symbol and

$$Z \equiv x^3 + ax + b \pmod P$$

It is well know that $\left|EP(a,b)\right| = P+1+\alpha, 1\alpha 1 \leq 2\sqrt{p}$ For every Elliptic cure over F_P

Complementary group on a given elliptic curve :

Let P be a prime > 3 and again a, b are integers chosen such that (A1) holds. In addition, Let $\overline{E_p(a,b)}$ denote the elliptic curve group module P whose elements (x,y) satisfying equation (A2), as before, but y is an in determinant in the field F_p for non-negative integer values of x. i.e. y is of the form $y=u\sqrt{v} \pmod P$, where u is non-negative integer < P and v is a fixed quadratic non-residue modulo P. The identity element, ∞, and the addition operations are identical to those defined in above. It is clear that all the group axioms hold for the above definition.

The order of this complementary group is given by $\overline{E_p(a,b)} = 1+\sum_{x=1}^{p}\left(1-\left(\frac{Z}{P}\right)\right)$ where $\left(\frac{Z}{P}\right)$ is the legendere symbol and $z=x^3+ax+b \pmod P$.

3.4 Elliptic curves over a ring

Consider elliptic curves over the ring Z_n, where n is an odd composite square free integer. Similar to the definition of $E_p(a,b)$, an elliptic curve $E_n(a,b)$ can b defined as the set of pairs $(x,y) + z_n^2$ satisfying $y^2=x^3+ax+b \pmod n$ together with a point ∞ at infinity. An addition operation on $E_n(a,b)$ can be defined in the same way as the addition operation an $E_p(a,b)$, simply by replacing computations in F_p by computations in Z_n. However two problems occur. The first problem is that because the computation of λ requires a division which in a ring is defined only when the division is a unit, the addition operation on $E_n(a,b)$ is not always defined. The second problem, which is related to the first is that $E_n(a,b)$ is not a group. It seems therefore impossible to base a cryptographic system an $E_n(a,b)$. In the following we represent a natural solution to these problems.

Let n=Pq in the sequel be the product of only two primes as in the RSA system. Moreover, the addition operation an $E_n(a,b)$ described above, whenever it is defined, is equivalent to the group operation on $E_p(a,b)$ $XE_q(a,b)$. By CRT, every element $C \in Z_n$ can be represented uniquely as a pair (C_p,C_q) where C_pEZ_p and $C_q \in Z_q$. Thus every point P=(x,y) on $E_n(a,b)$ can be represented uniquely as a pair $[P_p, P_q]=[(x_p,y_p), (x_q,y_q)]$ where $P_p \in E_p(a,b)$ and the points at ∞ an $E_p(a,b)$ are exhausted except the pairs of points of (P_p, P_q) for which exactly one of the points P_p and P_q is the point at ∞. It is important to note that when all prime factors of n are large, it is extremely unlikely that the send of two points an $E_n(a,b)$ is undefined. Infact if the

probability of the addition operation being undefined were non-negligible then every execution of a computation on $E_n(a,b)$ would be a feasible factoring algorithm, which is assumed not to exist. Therefore, the first problems can be solved by considering the occurable probability.

The second problem, that $E_n(a,b)$ is not a group, can be solved by the following lemma i.e., although we can't us the proportions of a finite group directly, we can use a property of $E_n(a,b)$ which is similar to that of a finite group. The following lemma can be easily determined from the CRT.

Lemma : Let $E_n(a,b)$ be an Elliptic curve state that GCD $(4a^3+27a^2,n)=1$ and $n=Pq$. Let N_n be lcm $(|E_p(a,b)| + |E_q(a,b)|)$

Then, for any $P \in E_n(a,b)$ and any integer K, $(K.N_n+1).P=P$

3.5 KMOV public key system based on Elliptic curves over Z_n

Key Generation : U chooses p,q state that $p \equiv q \equiv 2 \pmod 3$

User U computes $n=pq$ and $N_n=\text{lcm}(p+1, q+1)$

Also user U chooses an integer e state that $(e, N_n)=1$ and computes an integer d state that $ed \equiv 1 \pmod{N_n}$

A's secret key is d,

A's public key is n, e.

Encryption : A plain text $M=(m_x,m_y)$ is an integer pair,

where $m_x \equiv Z_n$, $m_y \in Z_n$.

Let $M = (m_x,m_y)$ be a point on the elliptic curve $E_n(0,b)$

Sender A encrypts the point M by encryption faction E(.) with the receiver's public key e and n as $C = E(M) = e.M$ over $E_n(a,b)$ and sends a ciphertext pair $C=(C_x,C_y)$ to a receiver B.

Decryption : Receiver B decrypts a point C by decryption function D(.) with his secret key d and public key n as $M = D(c) = d.c$ over $E_n(a,b)$

3.6 Proposed Scheme :

Select two primes and let $n=pq$

Select an elliptic curve $y^2=x^3+ax+b$ with the parameters a and b,

where gcd of $(4a^3+27b^2, n) = 1$

Let $|E_p(a,b)| = 1+p+\alpha$, $|E_q(a,b)| = 1+q+\beta$

$|\overline{E_p(a,b)}| = 1+p-\alpha$, $|Eq(a,b)| = 1+q-\beta$

Where $|\alpha| \le 2\sqrt{p}$, $|\beta| \le 2\sqrt{q}$, for every elliptic curve Fp and Fq

Let n represent the plaintext and C be the cipher text

(where $0 \le mn$, $C \le n-1$, $0 \le n-1$)

Encryption :

The encryption is defined as

$(c,t) = (x,y) \# e \pmod n$ (1)

Where (x,y)#e (or ep) denotes the point p=(x,y) Multiplied by e. Multiplication of a point P by i is defined as the addition of the point P to itself i times.

Decryption

Decryption is defined as

$(x,y) = (c,t) \# d_i \pmod n$ (2)

Where $e.d_i = 1 \pmod{N_i}$, i=1 to 4 (3)

And gcd $(e, N_i) = 1$, i=1 to 4 (4)

$N_1 = \text{lcm}(P+1+\alpha, q+1+\beta)$,if $(w/p) = 1$ & $(w/q) = 1$ (5)

$N_2 = \text{lcm}(P+1+\alpha, q+1+\beta)$,if $(w/p) = 1$ & $(w/q) \neq 1$ (6)

$N_3 = \text{lcm}(P+1+\alpha, q+1+\beta)$,if $(w/p) \neq 1$ & $(w/q) = 1$ (7)

$N_4 = \text{lcm}(P+1+\alpha, q+1+\beta)$,if $(w/p) \neq 1$ & $(w/q) \neq 1$ (8)

$Z = x^3+ax+b \pmod n$ (9)

$y=\sqrt{z}$ (10)

$w=C^3+ac+b \pmod n$ (11)

and $t=\sqrt{w}$ (12)

Alternatively, the decryptions time may be reduced T by a factor approaching 4, by computing (2) modulo p and modulo q the combining the results via the CRT.

Note that only the first coordinates, x and C, have to be computed in this scheme. Computation of the second co-ordinates y and t can be avoided using the rules and algorithms described in [13].

Also note that if p,q,a and b are chosen such that $\alpha = \beta = 0$ in equations (5) to (8), then $N_i = \text{lcm}(p+1, q+1)$ remains fixed for all i, consequently di is fixed for all i, and decryption is independent of the Legender Symbol (w/p) and (w/q).

CHAPTER – IV
TRAP DOORING DISCRETE LOGARITHMS ON ELLIPTIC CURVES OVER RINGS

4.1 Introduction

At the present time, one of the most challenging open problems in cryptography is certainly the realization of a trapdoor in the discrete logarithm problem. A discrete log encryption scheme over a group G intends to encrypt a plaintext m by simply raising some base element $g \in G$ to the power m, while decryption recovers n upto a public bound. Motivations for this may be diverse. The main advantage in comparison to other public-key techniques such as RSA or ElGamal comes from the additive homomorphic property of ciphertexts. This property constitutes the necessary condition for many cryptographic protocols to exist in fields like electronic voting[7], key escron [26] or group signatures, to quote a few. Clearly, discovering novel discrete log encryption techniques has a crucial positive impact on these research domains. In contrast direct applications of these for simple encryption purposes may be of more moderate interest as malleability destroys chosen cipher text security anyway.

Without considering all potential applications, this chapter focus on providing and analyzing new discrete log trapdoors and composing their properties with the ones vacantly discovered in [26].

Higher degree residuosity was introduced by Benaloh [2] as an algebraic framework to extending the properties of quadratic residuosity to prime degree greater than two. Since then, successive works have considerably improved the efficiency of residuosity – based encryption . Naccache and Stern [18] utilizing a smooth degree modulo n=pq; increased Benaloh's encryption rate upto $\cong 1/5$. More recently, Okamoto - Uchiyama [22] and Paillier [23] came up with modules independent encryption rates of 1/3 and 1/2 respectively, basing trapdoorness as a joint use of Fermat quotients and clever parameter choices. Interestingly, there three cryptosystems only stand in the multiplicative groups Zn* where n=pq, p^2q or p^2q^2 and p, q are large prime numbers.

There have been several attempts, in the meantime, to realize discrete log encryption over elliptic curves instead of standard groups. This was motivated by the fact that no sub-exponential time algorithm for extracting discrete logarithms is known so far, at least for most elliptic curves. As a matter of fact, all such design proposals have revealed themselves unsuccessful. Vanstone and Zuccherato [34] proposed a deterministic DL encryption scheme that was shown to be in secure a few months later by McKee and Pinch [15] and Coppersmith [3]. Independently, Okamoto and Uchiyama failed in attempting to design DL encryption over composite anomalous curves [22].

4.2 Contributions of this chapter

In this chapter we propose cryptosystems successfully answering the questions of [34] and [22] respectively. With guaranteed semantic security relatively to well identified computational problems. The first scheme is an embodiment of Naccache and Stern's cryptosystems on curves defined over Z_n, n=pq which realizes a discrete log encryption as originally imaged by Vanstone and Zuccherato probabilistic, our second cryptosystem relates to ρ-residuosity of a well-chosen curve over the ring Z_{p^2q}, i.e. provides an elliptic curve instance of OU encryption scheme. Finally we show how to extend the same design frame work of Paillier' encryption [12] while preserving all security and efficiency properties inherent to the original cryptosystems.

All these three schemes are reasonably efficient, simple to understand additively homomorphic, probabilistic and provably secure against chosen plaintext attacks in the standard model.

Elliptic Curve Version

4.3 Elliptic curve Naccache – Stern Encryption Scheme

The first encryption scheme that we describe here is a variant of Naccache and Stern's encryption scheme [12] where the working group is an elliptic curve over the ring Zn. The construction of such a curve is similar to the work of KMOV [12] that allowed to import factoring based cryptosystems like RSA [28] and Rabin [27] on a particular family of curves over the ring Z_n. We describe briefly their construction.

In the sequeal, p and q denote distinct large primes of product n. Recall that for any integer K, $E_k(a,b)$ is defined as the set of points $(x,y) \in Z_k \times Z_k$ such that $y^2 = x^3 + ax + b \pmod K$, together with a special element O_k called the point at infinity. It is known that given a composite integer K, a curve $E_k(a,b)$ defined over the ring Z_k has no reason to be a group. This problem however, does not have real consequences in practice when k = n because exhibiting a litigious addition leads to factors and this event remains of negligible probability. Furthermore, projections of $E_n(a,b)$ over F_p and F_q being finite abelian groups, the CRT easily conducts to the following statement :

Lemma : (Koyamma et al.,)

Let E_n (a,b) an elliptic curve, where n = pq is the product of two primes gcd $(4a^3 + 27b^2, n) = 1$. Let us define the order of E_n (a,b) as $|E_n(a,b)| = lcm(1 E_p(a,b)|, |Eq(a,b))$ then for any point $P \in E_n(a,b)$, we have $|E_n(a,b)|, P = O_n$. Where O_n denote the point at infinity of E_n (a,b). Although not being a group in a strict sense, the structure of $E_n(a,b)$ complies to lagrange's theorem and, from this stand point, can be used as a group. Koyama et al., take advantage of this feature by focusing curves of the following specific forms.

$$E_n(o,b) : y^2 = x^3 + b \bmod n \text{ for } b \in Z_n^* \text{ - I/C.}$$

Let p and q are both odd primes are choosen congruent to 2 modulo 3 so that the two curves $E_P(o,b)$ and $E_q(o,b)$, $b \in Z_n^*$ are cyclic groups of orders P + 1 and q + 1 (by KMOV)

We also impose $P + 1 = 6 u p^1$, $u = \prod P_i^{\delta i}$ (1)

$q + 1 = 6 v q^1$, $v = \prod P_i^{\delta i}$ (2)

for some B smooth integers u and v of equal bit size such that gcd $(6,u,v,p^1,q^1) = 1$. The integers p^1, q^1 are taken prime.

Let $\sigma = uv$. The base point G can be chosen of maximal order

μ = lcm (p + 1, q + 1), computed separately mod p and mod q, and recombined at the very end by Chinese Remainder Theorem (CRT).

Public key = n, b, σ, G

Secret key = (p,q) or μ = lcm (P+1, q+1)

Encryption

To encrypt a message $m \in Z_\sigma$, choose a random r < n, the ciphertext C is $C = (m + r\sigma)\ G$

Decryption

To decrypt C, first compute U is = $(\mu/\sigma)\ c = m\ G^1$.

To recover m, use Pohlig – Hellman and Baby–step gain – step to recover the discrete log of u in base G^1.

Decryption can also be performed over $E_P(o,b)$ and $E_q(o,b)$: in this case, one separately computes m mod u and m mod v. The plaintext m is then recovered modulo σ by CRT.

4.4 Elliptic curve Okamoto-uchiyama encryption scheme

Here we show how to extend the setting the defined to one of the elliptic curves. It is known that the curves $Ep(\bar{a},\bar{b})$ over F_p which have to trace of Frobenius one present the property that computing discrete logarithm on them is very easy. We extend the discrete logarithm recoverability property to a p-subgruops of $E_{p2}(a,b)$ so that the projection onto F_p gives the twist of an anomalus curve. This is done as follows. We begin by stating a few useful facts that derive from Hasse's theorm.

Lemma: Let $E_p(\bar{a},\bar{b}) : y^2 = x^3 + \bar{a}x + \bar{b} \bmod p$ be an elliptic curve of order $|E_p(\bar{a},\bar{b})| = P + 1 = t$ where $|t| \le 2\sqrt{P}$, than for any integers a,b such that a = ā mod p and b = b mod p, we have $|E_p^2(a,b) = (P+1-t)(P+1+t)$ the

curve $Ep^2(a,b)$ is usually said to be a lift of $E_p\left(\bar{a},\bar{b}\right)$ to $F_p^{\,2}$ one consequence of the above lemma is that if $E_p\left(\bar{a},\bar{b}\right)$ has P + 2 points, then any lift $Ep^2(a,b)$ must be of order P(P+2).

Lemma: let $E_p\left(\bar{a},\bar{b}\right)$ be an elliptic curve over F_P order P+2 provided that P≡2 (mod 3) any lift $Ep^2(a,b)$ of $E_p\left(\bar{a},\bar{b}\right) - \text{to } F_p^{\,2}$ to $F_p{}^2$ is cyclic.

Theorem

There exist a polynomial time algorithm that computes dLs on E[p]

Proof

Since E[P] is the group of p-torsion points of $Ep^2(a,b)$ we observe that any point P belongs to E[P] iff it is a lift of $\infty_p \in E_p\left(\bar{a},\bar{b}\right)$ where from E[P] is the kernel of the reduction map P → p mod p. Hence the p-adic elliptic logarithm [sec[ ]of page-]

$$\Psi_p(x, y) = -\frac{x}{y} \bmod p^2$$

is well defined and can be applied on any point of E[p]. Ψ_p being actually a morphism, if p=m.G stands for any arbitary points p,G ∈ P[p],

we have

$$m = \frac{\psi_p(p)}{\psi_p(G)} \bmod p, \text{ provides } G \neq \infty_{p2}$$

Choose two large primes P (with p ≡ 2 (mod 3)) and q of bit size k, and set n = pq. The user than picks integers $\bar{a}_p, \bar{b}_p \in F_p$ Such that $E_p(a_p, b_p)$ is of order p+2, by using the techniques such as [22]. He then chooses some lift $E_p^2\left(\bar{a}_q,\bar{b}_q\right)$ of $E_q\left(\bar{a}_q,\bar{b}_q\right)$ to F_{p2} as well as a random curve $E_q\left(\bar{a}_q,\bar{b}_q\right)$ defined over F_q. Using CRT, the user combines $E_p^2(a_p, b_p)$ and $E_q\left(\bar{a}_q,\bar{b}_q\right)$ to get the curve $E_n = E_n(a, b)$ where a, b ∈ z_n. Finally, the user picks a point a point G ∈ E_n of maximal order lcm ($\left|E_{p^2}, \left|E_{q^1}\right|\right.$)and sets H = n.G.

∴ Public key : $n = P^2 q$, E_n, G of maximal order, H

Private key : P

Encryption

To encrypt a plaintext $m < 2^{k-1}$, pick a random $r < 2^{2k}$ then the ciphertext

C = m.G + H. r

Decryption

Recover the plaintext m by computing

$$m = \frac{\psi_p[(P+2).G]}{\psi_p[(P+2).G]} \bmod P.$$

4.5 Elliptic Curve Paillier Encryption Scheme

Here we show that how to construct an efficient yet natural embodiment of Paillier's cryptosystem [23] on elliptic curves. We first extend the setting of the above section [FOO scheme] to curves defined over z_n^2 where n=pq. Suppose $E_p^2(a_p,b_p)$ is some lift of a curve of trace P+2 defined over F_p Considering E_n^2 (a,b) as the CRT of E_p^2 (a_p, b_p) and E_q^2 (a_p, b_p), it is easily seen that E_n^2 (a,b) is of order n μ,. where μ = μ (n) = lcm (p+2, q+2).

We extend theorem upto the present setting as follows :

Noting that E[n] = μ E_n^2 (a,b)

Corollary

There exists a polynomial time algorithm that computes the discrete logarithm on E[n].

Proof

This is easily proven, either by applying the theorem twice on curves E[P] ≅ E[n] mod p^2 and E[q] ≅ E[n] mod q^2 and then by CRT, local logarithm or more compactly by defining over E[n] an n-adic elliptic logarithm

$$\Psi_n(x, y) = \frac{-x}{y} \bmod n^2$$

Provided that P = m. G for P, G ∈ E[n] and G ≠ ∞_n^2 we retrieve m by computing

$$m = \frac{\psi_n[p.]}{\psi_n[G]} \bmod n.$$

The user choose two large prime and q (with P ≡ q ≡ 2 (mod 3)) and sets n = pq. He then picks up integer $\bar{a}_p, \bar{b}_p \in F_p$ and $\bar{a}_q, \bar{b}_q \in F_q$ such that $E_p\left(\bar{a}_p, \bar{b}_p\right)$ is of order p + 2 and $E_q\left(\bar{a}_q, \bar{b}_q\right)$ is of order q +2.

Lifted curves $E_p^2(a_p, b_p)$ and $E_q^2(a_q, b_q)$ are chosen and combined to get $E_n^2(a, b)$. Finally, a base point G ∈ E_n^2 is chosen of order divisible by n, possibly of maximal order n μ.

Public key : n = Pq, E_n^2, G

Privet key : μ = lcm (p +2, q+2)

Encryption:

To encrypt a message m ∈ Z_n, Pick a random r < n, then the ciphertext C is

C = (m + r n). G

Decryption

The plain text can be recovered as $$m = \frac{\psi_n[\mu.c]}{\psi_n[\mu.G]} \bmod n.$$

CHAPTER - V
CONCLUSIONS

In the right of our study in this dissertation, two existing problems were studied : "TRAPDOORING FACTORIZATION ON ELLIPTIC CURVES OVER RINGS" and "TRAPDOORING DISCRITE LOGARITHMS ON ELLIPTIC CURVES OVER RINGS".

First, we review a TOF based on elliptic curves over a ring Z_n. The security of this TOF depends on the difficulty of factoring n. Although this scheme is less efficient then the RSA and Rabin Schemes. We presented a Public – Key Cryptosystem based on elliptic curves over the ring Z_n. This Scheme can be used for both digital signatures and encryption applications, does not expand the amount of data that needs to be transmitted and appears to be immune from homomorphic attacks. The main advantage of this scheme is very little restriction on the type of elliptic curves and types of primes that can be used. In addition the system works on fixed elliptic curves. The security of the system relies on the difficulty of factoring large composite numbers.

Also we presented three probabilistic encryption schemes on elliptic curves over rings. These cryptosystems are based on three specific mechanisms allowing the recipient to recover discrete logarithms on different types of curves. More specifically, we showed how to design embodiments of Naccache-Stern, Okamoto-Uchiyama and Paillier discrete – log encryption schemes. Each provided cryptosystem is probabilistic and semantically secure relatively to the high residuosity problem associated with its curve type. We believe that the work in this Chapter positively concretizes all previous research work on discrete log encryption in the elliptic curve setting.

REFERENCES

1. Beak, J. Lee, B. and Kim. Probable secure length – saving public key encryption scheme under the computational DHA, Electronics and Telecommunications Research Institute (ETRI) Journal, Vol. 22, No. 4, Pages 25-31, 2000.
2. Benaloh, J.C. Verification – Secret Ballot Elections, Ph.D. thesis, Yale University, 1987.
3. Coppersmith D. Specialized Integer Factorization. In Advances in Cryptology, Proceedings of Eurocrypt'98, LNCS 1403, Pages 542-545, Springer Verlag, 1992.
4. Cramer R. and Shoup V. A practical Public Key Cryptosystem. Probably secure against adoptive chosen Cipher text attack, Advances in Cryptology – Proceedings of CRYPTO'98, LNCS 1462, Pages 13-25, Springer Verlag, 1998.
5. Diffie. W and Hellman M. New Directions in Cryptography. IEEE Transactions on Information theory, Vol. 10, Pages 74-84, IEEE, 1977.
6. El Gamal. T. A Public Key Cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information theory, Vol. 31, Pages 469-472, IEEE, 1985.
7. Fouque P.A., Poupard G. and Stern. J. Sharing Decryption in the content of voting or Lotheries. In proceedings of Financial Cryptography – Vol.1962 of LNCS, Pages 90-104, Springer Verlag, 2000.
8. Gauss, C.F. Disquistioners Arithematicae, 1801, English translation by Arthur A. Clarke, Springer Verlag, New York, 1986.
9. Gold Wassar, S., Micali S. Probabilistic Encryption, Journal of Computer and System Sciences, Vol. 28, Pages 270-299, Eluvier Incy. 1984.
10. Hesstein. I.N. : Topics in Algebra, Wiley Publications, 1987.
11. Koblitz. N. : A Course in Number Theory and Cryptography, 2nd Edition, Springer Verlag, 1994.
12. Koyamma, K. Maurer, U., Okamoto T. and Vamstone S. New Public Key Schemes based on Elliptic Curves over the ring Zn. In Advances in Cryptology, Proceedings of Crypto'91, LNCS 576, Pages 252-266, Springer Verlag, 1992.
13. Koyamma, K., Maurer, U. Okamoto T., Vamstone S.A. New Public Key Schemes based on elliptic curves over the ring Z_n, Advances in Cryptology – Crypto 91, Springer Verlag, 252-266.
14. Maurer, O.M. Towards the equivalence of breaking the Diffie-Hellman protocol and discrete logarithms. In Y.G. Demsat editor, In advances in Cryptology – CRYPTO'94, Pages 271-281, Springer Verlag, 1994.
15. McKee J. and Pinch. R. On a Cryptosystem of Vanstone and Zuccherato, Preprint, 1998.
16. Menezes, A.J. Van Oorschot, P.C. and Vamtone S.A. A Hand Book of applied Cryptography, CRC Press, 1996.
17. Miller. V. Uses of elliptic curves in Cryptography. Advances in Cruyptology – Crypto 85, Pages 417-426, Springer Verlag, 1985.
18. Naccache D. and Stern. A New Cryptosystem based on Higher Residues. In Proceedings of the 5th CCCS, ACM Press, Pages 59-66, 1998.
19. National Institute of Standards and Technology. Digital Signature standards, U.S. Dept. of Commerce, NIST FIPS Pub, 186, May 1994.
20. Nieven, I., Zuckerman, H., and Mongomery, H. An introduction to theory of numbers, Wiley Publications, 1991.
21. Okamoto T. and S. Uchiyama. A new Public Key Cryptosystem as secure as Factoring. In advances in Cryptology, Proceedings of Eurocrypt'98, LNCS 1403, Springer Verlag, Pages 308-358, 1998.

22. Okamoto T. and Uchiyama S. Security of an Identity – Based Cryptosystem and the Related Reduction. In advances in Cryptology, Eurocrypt'98, LNCS 1403, Pages 546-560. Springer Verlag, 1998.
23. Paillier, P. Public Key Cryptosystems based on composite residuosity classes, Advances in Cryptology, Proceedings of Eurocrypt'99, LNCS 1592, Pages 223-238, Springer Verlag, 1999.
24. Pohlig. S and Hellman M.E. An improved algorithm for computing logarithms over GF (P) and its Cryptographic significance, IEEE Transactions on Information theory, Vol. 24, Pages 106-110, IEE, 1978.
25. Pointcheral D. Chosen-Cipher tent security for any one-way cryptosystem, PKC Procedings 2000, LNCS, Vol. 1751, Pages 129-146, Springer Verlag, 2000.
26. Poupard G. and Stern. J. Fair Encrypton of RSA Keys. In Advances in Cryptology, Eurocrypt'00, LNCS 1807, Springer Verlag, 2000.
27. Rabin. M.O. Digitalized signatures and Public Key functions as instruct as factorization, MIT/LCS/TR-212, MIT Labs for Computer Science, 1979.
28. Rivest. R., Shamir, A. and Adleman L. A method for obtaining Digital signatures and public-key cryptosystems, Communications of the ACM 21(2), Pages 120-126, 1978.
29. Rosen. K.H. Elementary number theory and its applications, Wiley Publications, 1993.
30. Schnorr. C.P. Efficient Identification and signatures for smart cards, Advances in Cryptology. Proceedings of LRYPTO'89, LNCS. Vol. 435, Pages 235-251, Springer Verlag, 1990.
31. Simmons, G.J. Contemporary Cryptography. The Science of Information Integrity, IEEE, Press, 1992.
32. Stinson, D.R. Cryptography theory and Practice, CRC Press, 1995.
33. Tsiounis Y. and Yung M. On the security of El Gamal – Based Encryption, Proceedings of PKL'98, LNCS, Vol. 1807, Springer Verlag, 2000.
34. Vanstone S. and Zuccherato R. Elliptic curve Cryptosystem using curves of smooth order the ring Zn, In IEEE Transactions on Information Theory, Vol. 43, No. 4, IEEE, 1997.