A Study of Elliptic Curve Cryptography

E. Kesavulu Reddy

ABSTRACT

This paper basically two themes. One is the study of existing "Trapdoor One-way functions based on elliptic curves over Zn" and other is "Trapdooring Discrete logarithms on elliptic curves over Rings".

In 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. The security of the proposed scheme is based on the factoring composite numbers.

Keywords : Encryption, Decryption, rings, Factorization, Chaines Remained Theorem(CRT), Inverse, Discrete Logarithms, Groups, Homomorphic Attacks, Abelian Groups, Elliptic Curves, Smaller Keys, Finite Fields

1. Introduction

In 1976 Diffe 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. We review a TOF (or public key cryptographic schemes) based on elliptic curves over a ring Zn*[5] although an elliptic curve E over. Zn does not form a group. The security of this schemes are less efficient than the RSA and Rabin schemes but secure in the view point of some 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 and the system works on a fixed elliptic curves. The security of the system relies on the difficulty of factoring large composite numbers.

Assistant Professor, Dept of Computer Science, SVU College of Commerce Management and Information Sciences, Tirupati. Email : ekreddy2002@yahoo.com, Mobile: 9866430097

Here we proposed cryptosystem successfully answering the questions of[11] and [7] respectively. With guaranteed semantic security relatively to well identified computational problems. The first scheme is an embodiment of Naccache and Stern's cryptosystem on curves defined over Zn, n=pq which realizes a discrete log encryption is originally managed by Vanstone and Zuccherato Probablistic, our second cryptosystem relates to R-residuosity of a well-chosen curve over the ring ZpZq is provides an elliptic curve instance of O U encryption scheme.

2. Elliptic Curves

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

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

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

2.1 Elliptic Curves Over Prime Finite Field

We start with F_p ($P \in$ P, $p > 3$, char $(F_p) \neq 2,3$)[1] and perform the following change of variables

$$x \to x - \frac{a_2}{3} \qquad y \to y - \frac{a_1 x + a_3}{2}$$

After submission for on left side

$$Y = \left(Y - \frac{a_1 X + a_3}{2}\right)^2 + a_1 1X$$

$$\left(Y - \frac{(a_1 X + a_3)}{2}\right) + a_3 \left(Y - \frac{a_1 x + a3}{2}\right)$$

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:

$$= \ldots\ldots\ldots\ldots = Y^2 - \frac{a_1^{\,2} x^{\,2}}{4} - \frac{a_1 a_3 X}{2} - \frac{a_3^{\,2}}{2}$$

Both XY and Y have vanished, so their coefficients a_1 for X and take a look at the right side of (1) we get

$$\left(x - \frac{a_2}{3}\right)^3 + a_2 \left(\frac{x - a_2}{3}\right)^2 + a_4 \left(\frac{x - a_2}{3}\right) + a_6$$

$$= \ldots\ldots\ldots = x^3 + \left(\frac{a_2}{9} + a_4\right)x + \frac{2a_2^{\,3}}{27} - \frac{a_2}{3a_4 a_6}$$

$= \ldots\ldots$ setting $\left(\frac{1}{a} a^2 + a\right) = a$ and $\frac{2}{27} a$

$\frac{3}{2} - \frac{1}{2} a_2 a_4 a_6 = b$ In Fp equation (1) reduces to

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

2.2 Elliptic Curve Over Binary Finite Fields

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

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

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

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

3. Trapdooring Factorization On Elliptic Curves Over Rings

3.1 Elliptic Curves Over A Finite Field

Let F be the field of characteristics $\neq 2,3$ and let $a, b \in F$ be two parameters such that

$$4a^3 + 27b^2 \neq 0 \to \text{(A1)}.$$

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 $P=\infty$ thus $-P=\infty$ 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 $P+Q=\infty$. In all other cases the co-ordinates of $P+Q = (x_3,y_3)$ are computed as follows. Let λ be defined as

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\[2ex] \dfrac{3x_1^{\,2} + a}{2y_1} & \text{if } x_1 \neq x_2 \end{cases}$$

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.

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 $\left|EP(a,b)\right| = P+1+\alpha, 1\alpha 1 \le 2\sqrt{p}$ For every Elliptic cure over F_P

3.2. 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 $z=x^3+ax+b \pmod P$.

3.3 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 $E_p(a,b)$ X$E_q(a,b)$. By CRT, every element $C \in Z_n$ can be represented uniquely as a pair (C_p,C_q) where $C_p E Z_p$ 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 accruable 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 $(|E_p(a/,b)| + |E_q(a,/b)|)$ Therefore any $P \in E_n(a,b)$ and any integer K, $(K.N_n+1).P=P$

4. Trap Dooring Discrete Logarithms On Elliptic Curves Over Rings

4.1 Elliptic Curve Version

4.1.1 Elliptic Curve Naccache – Stern Encryption Scheme

The first encryption scheme that we describe here is a variant of Naccache and Stern's encryption scheme [4] 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 [4] that allowed to import factoring based cryptosystems like RSA [10] and Rabin [9] 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 $(x,y) \in Z_k X Z_k$ 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 $|E_n(a,b)| = \text{lcm}(1\, E_p(a,b)|, |Eq(a,b)|)$ 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.

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

Let p and q are both odd primes are chosen 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 $P + 1 = 6\,u\,p^1, \quad u = \prod P_i^{\delta i}$ (1)

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

$\mu = \text{lcm}(p + 1, q + 1)$, 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 $\mu = \text{lcm}(P+1, q+1)$

Encryption

To encrypt a message $m \in Z_s$, choose a random r < n, the cipher text 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 by CRT.

4.1.2 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 $E_p(\bar{a},\bar{b})$ 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-sub groups 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 theorem.

Lemma:

Let $E_P\left(\bar{a},\bar{b}\right): y^2 = x^3 + \bar{a}x + \bar{b}$ mod p be an elliptic curve of order

$\left| E_P\left(\bar{a},\bar{b}\right) \right| = P+1 = t$ where $|t| \leq 2\sqrt{P}$, than for any integers a,b such that a = $\bar{a}$ mod p and b = b mod p, we have $\left| E_P{}^2(a,b) = (P+1-t)(P+1+t)\right.$ the curve $Ep^2(a,b)$ is usually said to be a lift of $E_P\left(a,b\right)$ 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 $P \equiv 2 \pmod 3$ any lift $Ep^2(a,b)$ of $E_P\left(a,b\right)$ – to $F_P{}^2$ to $F_p{}^2$ is cyclic.

Theorem

There exists 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 $m = \frac{\psi_p(p)}{\psi_p(G)}$ mod p, provides $G \neq \infty p2$

Choose two large primes P (with $p \equiv 2 \pmod 3$) 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 to get the curve $E_n = E_n(a, b)$ where a, b ∈ z_n. Finally, the user picks a point G ∈ E_n of maximal order lcm $(|E_p{}^2, |E_q{}^1|)$ and sets H = n.G

∴ Public key : $n = P^2q$, 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

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

Conclusions

In the right of our study in this paper two existing problems were studied : "TRAPDOORING FACTORIZATION ON ELLIPTIC CURVES OVER RINGS" And "TRAPDOORING DISCRITE LOGARITHMS ON ELLIPTIC CURVES OVER RINGS". The first 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 presented two probabilistic encryption schemes on elliptic curves over rings .These cryptosystems are based on specific mechanisms allowing the recipient to recover discrete logarithms on different types of curves.

References

1. El Gamal. T, " *A Public Key Cryptosystem and a signature scheme based on discrete logarithms*", IEEE Transactions on Information theory, Vol. 31, PP. 469-472, IEEE, 1985.

2. 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, PP. 90-104, Springer Verlag, 2000.

3. Koblitz. N, " *A Course in Number Theory and Cryptography* ", 2nd Edition, Springer Verlag, 1994.

4. 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, PP. 252-266, Springer Verlag, 1992.

5. Koyamma. K, Maurer. U, Okamoto .T and Vamstone S.A, " *New Public Key Schemes based on elliptic curves over the ring Z_n*", Advances in Cryptology – Crypto 91, Springer Verlag, PP. 252-266.

6. Miller. V, *"Uses of elliptic curves in Cryptography"*, Advances in Cryptology – Crypto 85, PP. 417-426, Springer Verlag, 1985.

7. 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, PP. 308-358, 1998.

8. Poupard. G and Stern. J.Fair, *"Encryption of RSA Keys"*, In Advances in Cryptology, Eurocrypt'00, LNCS 1807, Springer Verlag, 2000.

9. Rabin. M.O, *"Digitalized signatures and Public Key functions as instruct as factorization"*, MIT/LCS/TR-212, MIT Labs for Computer Science, 1979.

10. Rivest. R, Shamir. A and Adleman.L, *"A method for obtaining Digital signatures and public-key cryptosystems"*, Communications of the ACM 21(2), PP. 120-126, 1978.

11. 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.

Author's Biography

E.Kesavulu Reddy working as Assistant professor in Dept. of. Computer Science (MCA) SVU College of CMIS, Tirupati (AP) and also worked as a Head in Dept of Computer Applications at SiTech Tirupati (AP) in India. I have six years experience in teaching and pursuing PhD, three years in the area of Cryptography and Network Security. I obtained MCA degree with First Class from SV University and M.Phil 2nd Class from Madurai Kamaraj University, Madurai.