Journal of
Applied & Computational Mathematics
ISSN: 2168-9679

Kumar and Gupta, J Appl Computat Math 2016, 5:1
DOI: 10.4172/2168-9679.1000288

Research Article Open Access

Cryptographic Schemes Based on Elliptic Curves over the Ring Zp[i]

Kumar M* and Gupta P

Department of mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Uttrakhand, 249404, India

Abstract

Elliptic Curve Cryptography recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller key size. The present paper includes the study of two elliptic curve $E_{a,b}$ and $E_{a,-b}$ defined over the ring Zp[i] where $i^2 = -1$. After showing isomorphism between $E_{a,b}$ and $E_{a,-b}$. We define a composition operation (in the form of a mapping) on their union set. Then we have discussed our proposed cryptographic schemes based on the elliptic curve $E = E_{a,b} \cup E_{a,-b}$. We also illustrate the coding of points over E, secret key exchange and encryption/decryption methods based on above said elliptic curve. Since our proposed scheme are based on elliptic curve of the particular type therefore the proposed schemes provides a highest strength-per-bit of any cryptosystem known today with smaller key size resulting in faster computations, lower power assumption and memory. Another advantage is that authentication protocols based on ECC are secure enough even if a small key size is used.

MSC 2010: 94A60, 14G50.

Keywords: Elliptic curve; Ring; Finite field; Isomorphism; Cardinality; Encryption/Decryption.

Introduction

Elliptic curve cryptography has been an active area of research since 1985 when Koblitz [1] and Miller [2] independently suggested using elliptic curves for public-key cryptography. Because elliptic curve cryptography offers the same level of security than, for example, RSA with considerably shorter keys, it has replaced traditional public key cryptosystems, especially, in environments where short keys are important. Public-key cryptosystems are computationally demanding and, hence, the fact that elliptic curve cryptography has been shown to be faster than traditional public-key cryptosystems is of great importance. Elliptic Curve Cryptographic (ECC) schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the Elliptic Curve Discrete Logarithmic Problem (ECDLP). Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA schemes. The competing system to RSA is elliptic curve cryptography. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size.

Auxiliary Result

In this section we mention some auxiliary results which are necessary to prove the main result.

For a prime number p, Let $Zp[i] = \{a + bi: a,b \in Z_p$ where $i^2 = -1\}$ be a ring having p^2 elements. We have the following assertion:

Lemma 1: An element a + ib is invertible in Zp[i] if only if $a^2 + b^2 \neq 0 (\text{mod } p)$ [3].

Proof: Let a + ib be invertible then there exists an element c + id in Zp[i] such that

$$(a+ib)(c+id)=1 \tag{1}$$

which implies (ac-bd) + i(bc + ad) = 1 i.e. ac-bd = 1and bc + ad = 0.

In (1) take the conjugate (a-ib)(c-id) = 1 (2)

Multiply (1) and (2), we get

$$(a+ib)(a-ib)(c+id)(c-id)=1$$

We deduce $a^2+b^2 \neq 0(\text{mod } p)$, so $a^2+b^2 \neq 0(\text{mod } p)$.

Lemma 2: Let p be a prime number. Then Zp[i] is field iff p≡3 (mod 4) [4].

Proof: Assume that Zp[i] is not field if p≡3(mod 4) then ∃ an element $a + bi \in Zp[i]$, which is not invertible. By Lemma 1 we have $a^2 + b^2 = 0(\text{mod } p)$. So $a^2 + b^2 = k$, where $k \in Z$. We can write $a = ta_1$, $b = tb_1$ with g.c.d $(a_1,b_1) = 1$. Suppose a is not divisible by p then p does not divide t but p divides $a_1^2 + b_1^2$. Using proposition 1 [5], we obtain $a_1^2 + b_1^2 = kp$. We have p≠3 (mod 4). Suppose p = 2, we can write $1^2 + 1^2 = 0(\text{mod } 2)$ then 1 + i is not invertible. Assume p = 1, then ∃ an element $c \in Z_p[i]$ such that $c^{\frac{p-1}{2}} \neq 1$ because $c^{p-1} = 1$ this implies that $c^{\frac{p-1}{2}} = -1$ and hence $(c^k)^2 = c^{2k} = -1$. So $12 + (c^k)^2 = 1\text{-}1 = 0$. We deduce that c^k + I is not invertible. This completes the proof of the result.

Theorem 1: For two isomorphic abelian groups $(G_1,*)$ an$(G_2,°)$d with the same unit element e, let $E = G_1 \cup G_2$ and also let $\oplus: E \times E \to E$ be a mapping defined by

$$(x,y) \to x \oplus y$$

***Corresponding author:** Kumar M, Department of mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Uttrakhand, 249404, India, Tel: 01334690011; E-mail: sdmkg1@gmail.com

Received January 19, 2016; **Accepted** February 03, 2016; **Published** February 05, 2016

Citation: Kumar M, Gupta P (2016) Cryptographic Schemes based on Elliptic Curves over the Ring Zp[i]. J Appl Computat Math 5: 288. doi:10.4172/2168-9679.1000288

such that $x \oplus y = \begin{cases} x * y & if\ x, y \in G_1 \\ x \circ y & if\ x, y \in G_2 \\ f(x) \circ y & if\ x \in G_1, y \notin G_1 \\ x \circ f(y) & if\ x \notin G_1, y \in G_1 \end{cases}$

where f is the isomorphism between G_1 and G_2. Then ⊕ is an internal composition law, commutative with identity element e and all elements in E are invertible [6].

Proof: It is clear that ⊕ is an internal composition law over E.

To show that e is the identity element with respect to binary operation ⊕.

Let x in E. If $x \in G_1$ then $x \oplus e = x*e = e*x = e \oplus x = x$,

Because $x \in G_1$ and e is the unit element of $(G_1,*)$.

Else $x \in G_2$, then $x \oplus e = x \circ e = e \circ x = e \oplus x = x,$

Because $x \in G_2$, $f(e) = e$ and e is unit element of (G2,°).

⊕ is commutative: We have $(G_1,*)$ and $(G_2,°)$ two abelian groups with the same unit element e [7-10].

Let $x,y \in E$. If $x,y \in G_1$ then $x \oplus y = x * y = y * x = y \oplus x$

If $x, y \in G_2$ then $x \oplus y = f(x) \circ y = y \circ f(x) = y \oplus x$

If $x \in G_1, y \notin G_2$ then $x \oplus y = f(x) \circ y = y \circ f(x) = y \oplus x$

If $x \notin G_1, y \in G_2$ then $x \oplus y = x \circ f(y) = f(y) \circ x = y \oplus x$.

Elliptic curve over the Field Z_p[i]

Let $E_{a,b}$,$E_{a,-b}$ be two elliptic curve over the field Z_p[i], where p is a prime number such that p = 3(mod 4), defined by $E_{a,b} = \{(x,y) : y^2 = x^3 + ax + b\} \cup \{O\}$ and $E_{a,-b} = \{(x,y) : y^2 = x^3 + ax - b\} \cup \{O\}$

Where O is the point at infinity [11-14].

Corollary 1: If b≠0 then $E_{a,b} \cap E_{a,-b} = \{O\}$

Proof: Let $(x,y) \in E_{a,b} \cap E_{a,-b}$, then $y^2 = x^3 + ax + b$ and $y^2 = x^3 + ax - b$ this implies that b = -b i.e. b = 0 which is a contradiction. Hence $E_{a,b} \cap E_{a,-b} = \{O\}$.

Main Result

Theorem 2

Let f be a mapping from $E_{a,b}$ to $E_{a,-b}$ defined by

F(x,y) = (-x,iy) and f(O) = 0

Then f is a bijection.

Proof: First we show that f is well defined.

Let $(x,y) \in E_{a,b}$ then $y^2 = x^3 + ax + b$, then $-y^2 = -x^3 - ax - b$ i.e.

$(iy)^2 = (-x)^3 + a(-x) - b$ therefore $(-x,iy) \in E_{a,b}$

Hence f is well defined.

f is one-one: Let $(x_1,y_1),(x_2,y_2) \in E_{a,b}$ such that

$f(x_1, y_1) = f(x_2, y_2)$

$(-x_0, i\, y_0) = (-x_1, i\, y_1)$

This implies that $x_1 = x_2$ and $iy_1 = iy_2$ i.e. $x_1 = x_2$ and $y_1 = y_2$

So, $(x_1,y_1) = (x_2,y_2)$

Hence, f is one-one.

f is onto: Let $(x,y) \in E_{a,-b}$. Then $y^2 = x^3 + ax - b$ or $-y^2 = -x^3 - ax + b$

This implies that $(-x,iy) \in E_{a,b}$ because $(iy)^2 = (-x)^3 + a(-x) - b$ and $f(-x,iy) = (x,y)$

Thus, f is onto.

f is homomorphism: Let $(x_1,y_1),(x_2,y_2) \in E_{a,b}$ there is three cases arises:

Case 1: When $x_1 \neq x_2$

We have $f((x_1, y_1) + (x_2, y_2)) = f(\lambda^2_{a,b} - x_1 - x_2, \lambda_{a,b}(x_2 - x_3) - y_2)$

$= (-\lambda^2_{a,b} + x_1 + x_2, i\,\lambda_{a,b}(x_2 - x_3) - iy_2)$

where $\lambda_{a,b} = \dfrac{y_2 - y_1}{x_2 - x_1}$ and $x_3 = \lambda^2_{a,b} - x_1 - x_2$

again $f((x_1, y_1)) + f((x_2, y_2)) = (-x_1, i\, y_1) + (-x_2, iy_2)$

$= (\lambda^2_{a,-b} + x_1 + x_2, \lambda_{a,-b}(-x_2 - x_4) - iy_2)$

where $\lambda_{a,-b} = \dfrac{iy_2 - iy_1}{-x_2 + x_1}$ and $x_4 = \lambda^2_{a,-b} + x_1 + x_2$.

It is obvious that $\lambda^2_{a,b} = -\lambda^2_{a,-b}$ this implies that $\lambda^2_{a,b} = -\lambda^2_{a,-b}$ and $x_3 = -x_4$

Therefore $f((x_1, y_1) + (x_2, y_2)) = f((x_1, y_1)) + f((x_2, y_2))$.

Case 2: When $x_1 = x_2$ and $y_1 = y_2$

$f((x_1, y_1) + (x_2, y_2)) = f(\lambda^2_{a,b} - 2x_1, \lambda_{a,b}(x_1 - x_3) - y_1)$

$= (-\lambda^2_{a,b} + 2x_1, i\,\lambda_{a,b}(x_1 - x_3) - iy_1)$

where $\lambda_{a,-b} = \dfrac{3x_1^2}{2y_1}$ and $x_3 = \lambda^2_{a,b} - 2x_1$

again $f((x_1, y_1)) + f((x_2, y_2)) = (-x_1, i\, y_1) + (-x_2, iy_2)$

$= (\lambda^2_{a,-b} + 2x_1, \lambda_{a,-b}(-x_1 - x_4) - iy_1)$

where $\lambda_{a,-b} = \dfrac{3(-x_1)^2}{2y_1}$ and $x_4 = \lambda^2_{a,-b} + x_1 + x_2$.

It is evident that $\lambda_{a,-b} = -i\dfrac{3x_1^2}{2y_1} = -i\lambda_{a,b}$ then, $\lambda^2_{a,b} = -\lambda^2_{a,-b}$ and $x_3 = -x_4$.

Therefore, $f((x_1, y_1) + (x_2, y_2)) = f((x_1, y_1)) + f((x_2, y_2))$

Case 3: When $x_1 = x_2$ and $y_1 = -y_2$

We have

$f((x_1, y_1)) + f((x_2, y_2)) = (-x_1, i\, y_1) + (-x_2, iy_2) = (-x_1, iy_1) + (-x_1, -iy_1) = O$

and

$f((x_1, y_1)) + f((x_2, y_2)) = (-x_1, i\, y_1) + (-x_2, iy_2) = (-x_1, iy_1) + (-x_1, -iy_1) = O$

Thus $f((x_1, y_1)) + f((x_2, y_2)) = f((x_1, y_1) + (x_2, y_2))$

Therefore, in either case f is a homomorphism. Hence f is a bijection.

Corollary 2: For two isomorphic abelian groups $E_{a,b}$ and $E_{a,-b}$ with the same unit element O, let $E = E_{a,b} \cup E_{a,-b}$ and also let ⊕: E×E→E be a mapping defined by

(P,Q)→P⊕Q

such that $P \oplus Q = \begin{cases} P + Q & if\ P, Q \in E_{a,b} \\ P + Q & if\ P, Q \in E_{a,-b} \\ f(P) + Q & if\ P \in E_{a,b}, Q \notin E_{a,b} \\ P + f(Q) & if\ P \notin E_{a,b}, Q \in E_{a,b} \end{cases}$

where f is the isomorphism between $E_{a,b}$ and $E_{a,-b}$. Then ⊕ is an internal composition law, commutative with identity element O and all elements in E are invertible.

Proof: Keeping in view the result of theorem 1, corollary 1, and theorem 2, it is evident that ⊕ is an internal composition law, commutative with identity element O and all elements in E are invertible.

Corollary 3: If $E_{a,b}$ and $E_{a,-b}$ are isomorphic groups i.e. they are both abstractly identical of groups then Card(E) = 2Card($E_{a,b}$)-1.

Proof: Since $E_{a,b}$ is isomorphic to $E_{a,-b}$ this implies Card($E_{a,b}$) = Card($E_{a,-b}$)

Now, $E = E_{a,b} \cup E_{a,-b}$

This implies that Card(E) = Card($E_{a,b}$) + Card($E_{a,-b}$)-Card($E_{a,b} \cap E_{a,-b}$)

Therefore, Card(E) = 2Card($E_{a,b}$)-1.

Cryptographic Applications

In this section we shall illustrate our proposed methods for coding of points on Elliptic Curve, then exchange of secret key and finally use them for encryption/decryption.

Coding of element on elliptic curve

It is described with the help of illustration-1 and illustration-2.

Illustration 1: For p = 3, a = 1 and b = 1, Then codes of elements of $E = E_{a,b} \cup E_{a,-b}$ are given by E = {00100,00101,00201,10001,10101,10201,20001,01101,01201,11001,11101,11201,21001,02101,02201,12001,12101,12201,22001}

Since, $E_{1,1} = \{(x,y): y^2 = x^3 + x + 1\} \cup \{O\}$

and $E_{2+3i,1+i} = \{(x,y): y^2 = x^3 + (2+3i)x + 1 + i\} \cup \{O\}$

Therefore $E_{1,1}$ = {(0,1), (0,2), (1,0), (i,1), (i,2), (1 + i,0), (2i,1), (2i,2), (1 + 2i,0)}{O}.

and $E_{1,-1}$ = {(1,1), (1,2), (2,0), (1 + i,1), (1 + i,2), (2 + i,0), (1 + 2i,1), (1 + 2i,2), (2 + i,0)}∪{O}.

Coding of element $E = E_{1,1} \cup E_{1,-1}$ are described as follow

Let P = [$x_0 + x_1 i; y_0 + y_1 i; z$], where $x_j, y_j \in Z_3$ for j = 0 or 1 and z = 0 or 1. Then coding method is given by $x_0x_1y_0y_1$

which produces the following codes

E={00100,00101,00201,10001,10101,10201,20001,01101,01201,11001,11101,11201,21001,02101,02201,12001,12101,12201,22001}

Illustration 2: For p = 7, a = 2 + 3i and b = 1 + i. The coding of points of $E_{a,b} \cup E_{a,-b}$ can be described as $E_{2+3i,1+i} = \{(x,y): y^2 = x^3 + (2+3i)x + 1 + i\} \cup \{O\}$ $E_{2+3i,-(1+i)} = \{(x,y): y^2 = x^3 + (2+3i)x - (1+i)\} \cup \{O\}$

Let P = [$x_0 + x_1 i$; $y_0 + y_1 i$; z], where $x_j, y_j \in Z_7$ for j = 0 or 1 and z = 0 or 1. Then coding method is given by $x_0x_1y_0y_1z$, which produces the following codes

E={00100, 00131, 00361, 00411, 00641, 01021, 01051, 01351, 01421, 02111, 02661, 03141, 03631, 04311, 04461, 05161, 05161, 05611, 06201, 06231, 06501, 06541, 10121, 10241, 10531, 10651, 12251, 12521, 14031, 14041, 14111, 14661, 15021, 15051, 15351, 15421, 16201, 16231, 16501, 16541, 20011, 20061, 23141, 23631, 25251, 25521, 26311, 26461, 31141, 311631, 33001, 33321, 33451, 35301, 35401, 36341, 36431, 41331, 41441, 42031, 42041, 44001, 44241, 44531, 46311, 46461, 50101, 50601, 51141, 51631, 52221, 52551, 54311, 54461, 60261, 60321, 60451, 60511, 61021, 61051, 61351, 61421, 62201, 62231, 62501, 62541, 63161, 63301, 63401, 63611, 65221, 65551}

The above scheme helps us to encrypt and decrypt any message of any length.

Exchange of secret key

1. For a publically integer p, and an elliptic curve E(Z_p[i]) let P∈E(Z_p[i]) of order n.

2. By P generate a subgroup and denoted it by $G = \langle P \rangle$. Which is used to encrypt the message m.

Now, key exchange between Alice and Bob can be described as follows:

3. Alice chooses a random number $0 \le N_A \le n-1$, computes K = N_AP and sends it to Bob.

4. Bob chooses a random number $0 \le N_B \le n-1$, computes K = N_BP and sends it to Alice.

5. Alice computes NAK′ = $N_A.N_B$P.

6. Bob computes N_B.K = $N_B.N_A$P.

7. Alice and Bob are agree with a point S = $N_A.N_B$P, choose the binary code of point S as a private key, which transformed on the decimal code <<S′>>.

Remark: With the secret key S′ such as the decimal code of point S Alice and Bob can encrypt and decrypt the message (m).

Illustration 3: Let $E_{3,45} = \{(x,y): y^2 = x^3 + 3x + 45\} \cup \{O\}$ and $E_{3,-45} = \{(x,y): y^2 = x^3 + 3x - 45\} \cup \{O\}$ are two elliptic curve defined over the same field Z_{8831}[i] having 8831^2 element, where 8831 be a prime number such that 8831≡3(mod 4) and a point P = (4,11)∈Z_{8831}[i] of order 4427.

(1) Alice choose a random number N_A = 12, compute K = 12(4,11) = (814,5822) and sends it to Bob.

(2) Bob chooses a random number N_B = 23 and comput K′ = 23(4,11) = (3069,3265) and sends to it Alice.

(3) Alice computes N_AK′ = 12.(3069,3265) = (3076,265).

(4) Bob computes N_B.K = 23.(814,5822) = (3076,265).

(5) Alice and Bob are agree with a point S = (3076,265), choose the binary code of point S as a private key, which transformed on the decimal code <<30760000265000001>>.

ECC key generation phase

Now, exchange of secret key involves the following steps:

1. Encode the message m on the point P_m.

2. Choose a random number k, compute Q = k.P_m and calculate P_b = S′.Q.

3. Public key is (a,b,p,P,P_b,Q).

4. Private key is (N_A,N_B,k,S).

ECC encryption phase

To encrypt P_m, a user choose an integer <<r>> at random and sends the point (r.Q,P_m + r.P_b). This operation is shown in Figure 1.

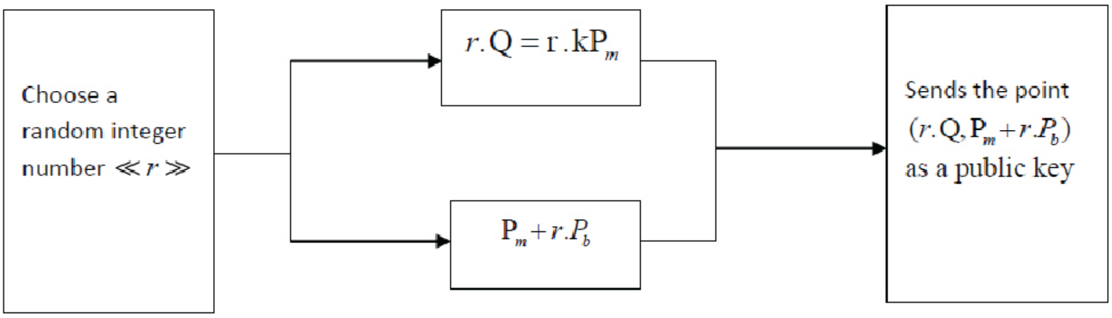

Figure 1: The encryption operation.

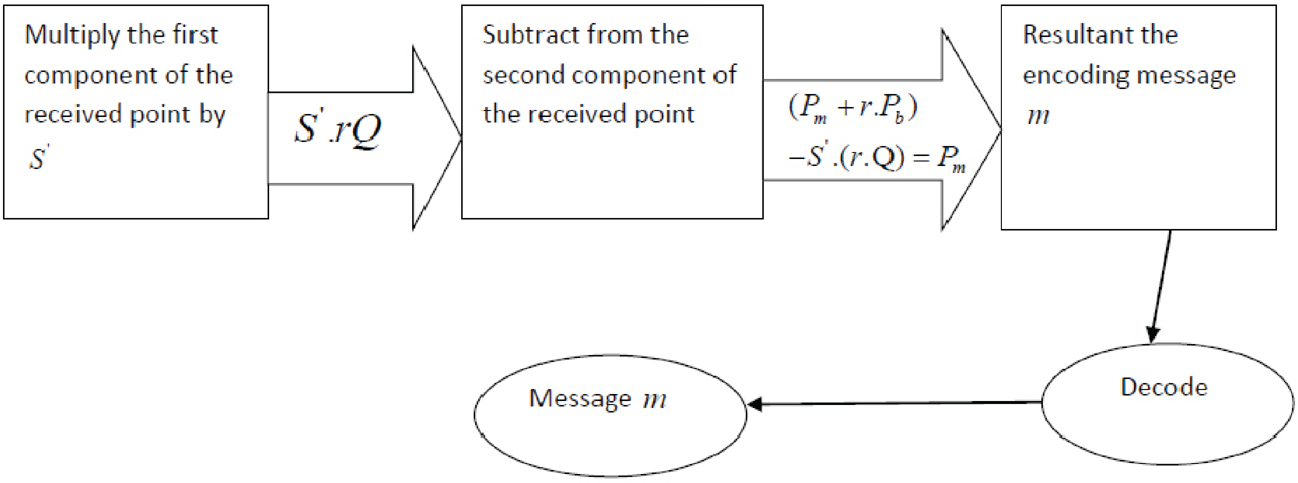

Figure 2: The decryption operation.

ECC decryption phase

Decryption of the message is done by multiplying the first component of the received point the secret key <<S'>> and subtract it from the second component: $(P_m + r.P_b)$-S'.(r.Q) = P_m + r.S'Q-S'.r.Q = P_m

This operation is shown in Figure 2.

Illustration 4: The $E_{3,45}$ = {(x,y): $y^2 = x^3 + 3x + 45$}∪{O} and $E_{3,-45}$ = {(x,y): $y^2 = x^3 + 3x-45$}∪{O} are two elliptic curve defined over the same field Z_{8831}[i] having 8831^2 element where 8831 be a prime number such that 8831≡3(mod 4) and a point P = (4,11)∈Z_{8831}[i] of order 4427.

Alice's message is point P_m = (5,1743).

Bob has chosen his secret random number k = 3 and computed Q = k.P_m = 3.(5,1743) = (445,3115) and calculated Pb = S.Q = 30760000265000001(445,3115) = (7093,2868) Bob publish the point. Alice chooses the random number r = 8 and compute r.Q = 8.(445,3115) = (7966,6354) and P_m + r.P_b = (5,1743) + 8.(7093,2868) = (5011,2629) Alice sends (7966,6354) and (5011,2629) to Bob, who multiplies the first of these point by S'.(r.Q) = 30650000265000001.(7966,6354) = (6317,6201). Bob then subtracts the result from the last point Alice sends him. Note that he subtracts by adding the point with the second coordinate negated:

$$P_m + r.P_b - S'.(r.Q) = (5011, 2629) - (6317, 6201) = (5,1743) = P_m$$

Bob has therefore received Alice's message.

Acknowledgments

This research work is supported by University Grant commission (UGC) New Delhi, India under the Junior Research Fellowship student scheme.

References

1. Koblitz AH, Koblitz N, Menezes A (2011) Elliptic curve cryptography: The serpentine course of a paradigm shift. Journal of Number Theory 131: 781-814.
2. Miller V (1985) Use of elliptic curves in cryptography. Advances in Cryptology-CRYPTO 85 (LNCS 218) pp: 417-426.
3. Gilbert WJ (2004) Modern algebra with application. Willey-Interscience.
4. Gallian JA (1998) Contemporary abstract algebra. Narosa publishing house.
5. Chillali A (2011) Elliptic curve over ring. International Mathematical Forum 6: 1501-1505.
6. Hankerson D, Menezes JA, Vanstone S (2004) Guide to Elliptic Curve Cryptography. Springer-Verlag.

7. Hardy GH, Wright EM (1938) An introduction to the theory of numbers. Oxford university press.
8. Koblitz N (1987) Elliptic Curve Cryptosystem. Journal of mathematics computation 48: 203-209.
9. Kumar S, Suneetha C, Chandrasekh A (2012) Encryption of data using elliptic curve over finite fields. International Journal of Distributed and Parallel Systems (IJDPS).
10. Schoof R (1985) Elliptic curves over finite fields and the computation of square roots mod p. Math Comp 44: 483-494.
11. Silverman J (1986) The Arithmetic of Elliptic Curves. Springer.
12. Srivastava K, Nand G (2015) Elliptic Curves for Data Provenance. Procedia Computer Science 45: 470-476.
13. Stinson DR (2006) Cryptography theory and practice. Chapman and Hall/CRC.
14. Washington LC (2008) Elliptic curves number theory and cryptography. Chapman and Hall/CRC.