Cryptographic Schemes Based on Elliptic Curves over the Ring \( \mathbb{Z}_p[i] \)

Kumar M* and Gupta P

Department of mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Uttarakhand, 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 curves \( E_{a,b} \) and \( E_{a,-b} \) defined over the ring \( \mathbb{Z}_p[i] \) 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 is 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 \( \mathbb{Z}_p[i] = \{a + bi : a, b \in \mathbb{Z}_p \} \) where \( i^2 = -1 \) be a ring having \( p^2 \) elements. We have the following assertion:

**Lemma 1:** An element \( a + ib \in \mathbb{Z}_p[i] \) if only if \( a^2 + b^2 \equiv 0 \pmod{p} \).

**Proof:** Let \( a + ib \) be invertible then there exists an element \( c + id \) in \( \mathbb{Z}_p[i] \) such that

\[
(a + ib)(c + id) = 1
\]

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

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 \(a^2 + b^2 \equiv 0 \pmod{p} \), so \(a^2 + b^2 \equiv 0 \pmod{p} \).

**Lemma 2:** Let \( p \) be a prime number. Then \( \mathbb{Z}_p[i] \) is field iff \( p \equiv 3 \pmod{4} \).

**Proof:** Assume that \( \mathbb{Z}_p[i] \) is not field if \( p \equiv 3 \pmod{4} \) then \( \exists \) an element \( a + bi \in \mathbb{Z}_p[i] \), which is not invertible. By Lemma 1 we have \(a^2 + b^2 \equiv 0 \pmod{p} \). So \(a^2 + b^2 = kp \), where \( k \in \mathbb{Z} \). We can write \( a = ta_1, b = tb \), with \( \gcd(a,b) = 1 \). 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 \( p \equiv 3 \pmod{4} \). Suppose \( p = 2 \), we can write \( 1 + 1 = 0 \pmod{2} \) then \( 1 + i \) is not invertible. Assume \( p = 1 \), then \( \exists \) an element \( c \in \mathbb{Z}_p[i] \) such that \( c^2 \neq 1 \) because \( c^2 = 1 \) this implies that \( c \neq c^2 = 1 = -1 \) and hence \( c^4 = c^8 = 1 \). So 12 + (c)^4 = 1 = 0. We deduce that \( c^4 + 1 \) is not invertible. This completes the proof of the result.

**Theorem 1:** For two isomorphic abelian groups \( (\mathbb{Z}^*_p)^d \) and \( (\mathbb{Z}^*_p)^d \) with the same unit element \( e \), let \( E = G_1 \cup G_2 \) and also let \( \oplus : E \times E \rightarrow E \) be a mapping defined by

\[
(x,y) \mapsto x \oplus y
\]
such that \( x \oplus y = \begin{cases} 
  x \times y & \text{if } x, y \in G_1 \\
  x \times y & \text{if } x, y \in G_2 \\
  f(x) + y & \text{if } x \in G_1, y \notin G_1 \\
  x + f(y) & \text{if } x \notin G_1, y \in G_1 \\
  f(x) + y & \text{if } x \in G_1, y \notin G_1 \\
  x + f(y) & \text{if } x \notin G_1, y \in G_1 
\end{cases} \)

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

**Proof:** It is clear that \( \oplus \) is an internal composition law over \( E \).

To show that \( e \) is the identity element with respect to binary operation \( \oplus \).

Let \( x \in E \). If \( x \in G_1 \) then \( x \oplus e = x \times e = e \times x = e \oplus x = x \), \( e \in G_1 \).

Because \( x \in G_2 \) and \( e \) is the unit element of \((G_2, \circ)\).

Else \( x \in G_2 \), then \( x \oplus e = e \circ e \circ x = e \oplus x = x \), \( e \in G_2 \).

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

\( \oplus \) is commutative: We have \((G_1, \times)\) and \((G_2, \circ)\) two abelian groups with the same unit element \( e \) \([7-10]\).

Let \( x, y \in E \). If \( x, y \in G_1 \) then \( x \oplus y = x \times y = y \times x = y \oplus x \).

Therefore, \( f \) is a homomorphism. Hence \( f \) is a bijection.

**Theorem 2**

Let \( E_{a,b} \times E_{a,b} \) be two elliptic curve over the field \( \mathbb{Z}_p[i] \), where \( p \) is a prime number such that \( p = 3 \text{mod } 4 \), defined by \( E_{a,b} = \{(x,y): y^2 = x^3 + ax + b \} \cup \{0\} \) and \( E_{a,-b} = \{(x,y): y^2 = x^3 + ax - b \} \cup \{0\} \)

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

**Corollary 1:** If \( b = 0 \) then \( E_{a,b} \cap E_{a,-b} = \{0\} \).

**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 \( E_{a,b} \cap E_{a,-b} = \{0\} \).

**Main Result**

**Theorem 2**

Let \( f \) be a mapping from \( E_{a,b} \) to \( E_{a,b} \) defined by

\[ f(x,y) = (-x,y) \text{ and } f(O) = 0 \]

Then \( f \) is a bijection.

**Proof:** First we show that \( f \) is well defined.

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

\[ f(x_1, y_1) = f(x_2, y_2) \]

\[ (-x_1, iy_1) = (-x_2, iy_2) \]

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 are three cases arises:

**Case 1:** When \( x_1 \neq x_2 \)

We have \( f((x_1, y_1) + (x_2, y_2)) = f((-x_1^2 - x_1 + x_2, i(x_1 - x_2) - y_1)) \)

\[ = (-x_1^2 - x_1 + x_2, i(x_1 - x_2) - y_1) \]

**Case 2:** When \( x_1 = x_2, y_1 \neq y_2 \)

We have \( f((x_1, y_1) + (x_2, y_2)) = f((x_1, i(y_2)) \cup (-x_1, y_1) \cup (-x_1, y_2)) \)

\[ = (-x_1^2 - x_1 + x_2, i(y_2)) \]

**Case 3:** When \( x_1 = x_2, y_1 = y_2 \)

We have \( f((x_1, y_1) + (x_2, y_2)) = f((x_1, y_1)) \cup f((x_2, y_2)) \)

\[ = (-x_1, y_1) \cup (-x_1, y_2) \cup (-x_1, y_1) \cup (-x_1, -y_1) = O \]

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 \( @: E \times E \rightarrow E \) be a mapping defined by

\[ (P, Q) @: Q = \begin{cases} 
  P + Q & \text{if } P, Q \in E_{a,b} \\
  P + Q & \text{if } P, Q \in E_{a,-b} \\
  f(P) + Q & \text{if } P \in E_{a,b}, Q \notin E_{a,b} \\
  P + f(Q) & \text{if } P \notin E_{a,b}, Q \in E_{a,b} 
\end{cases} \]

\[ @: E \times E \rightarrow E \]
where $f$ is the isomorphism between $E_a$ and $E_{a,b}$. Then $\oplus$ 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 $\oplus$ 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($E_a,b$) = Card($E_{a,b}$).

**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($E_{a,b}$)

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 $E = E_a \cup E_{a,-b}$ are given by $E = \{(00100,00101,00201,10001,10101,10201,20001,01101,01201,11001,11101,11201,21001,02101,02201,12001,12101,12201,22001)\}$

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

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

Therefore $E = \{(0,1), (0,2), (1,0), (i,1), (i,2), (1 + i,0), (2i,1), (2i,2), (1 + 2i,0)\}$

and $E_{a,-b} = \{(1,1), (1,2), (2,0), (1 + i,2), (1 + 2i,0)\}$

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

Let $P = [x_0 + x_1i; y_0 + y_1i; z]$, where $x_j,y_j \in \mathbb{Z}$ 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 $E_{a,b}$ can be described as $E_{a,b} = \{(x, y): y^2 = x^3 + 3x + 45\} \cup \{O\}$

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

Therefore $E = \{(0,1), (0,2), (1,0), (1 + i,1), (1 + i,2), (2 + i,0), (1 + 2i,1), (1 + 2i,2), (2 + i,0)\}$

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

Let $P = [x_0 + x_1i; y_0 + y_1i; z]$, where $x_j,y_j \in \mathbb{Z}$ 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

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

Now, exchange of secret key involves the following steps:

1. Choose a random number $N_a$, compute $K = N_aP$ and sends it to Bob.
2. Bob chooses a random number $0 \leq N_b \leq n-1$, computes $K = N_bP$ and sends it to Alice.
3. Alice computes $N_AK = N_A(N_bP)$.
4. Bob computes $N_bK = N_b(N_AP)$.
5. Alice and Bob are agree with a point $S = N_A \cdot N_bP$, 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 $(m)$.

**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 $Q = kP_m$ and calculate $P_k = S \cdot Q$.
3. Public key is $(a,b,P,P,P_0,Q)$.
4. Private key is $(N_A,N_b,k)$.

**ECC encryption phase**

To encrypt $P_m$, a user choose an integer $<r>$ at random and sends the point $(r \cdot Q,P_m + r \cdot P_k)$. This operation is shown in Figure 1.
**ECC decryption phase**

Decryption of the message is done by multiplying the first component of the received point the secret key $\langle S' \rangle$ and subtract from the second component: 

$$(P_m + r.P_b) - S'.(r.Q) = P_m + r.S.Q - S'.r.Q$$

This operation is shown in Figure 2.

**Illustration 4:** The $E_{3,45} = \{(x,y): y^2 = x^3 + 3x + 45\} \cup \{O\}$ and $E_{3,-45} = \{(x,y): y^2 = x^3 + 3x - 45\} \cup \{O\}$ are two elliptic curve defined over the same field $\mathbb{Z}_{8831}[i]$ having 88312 element where 8831 be a prime number such that $8831 \equiv 3 \pmod{4}$ and a point $P = (4,11) \in \mathbb{Z}_{8831}[i]$ 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 $P_b = S.Q = 3076000265000001(445,3115) = (7093,2868)$ 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 $S'.(r.Q) = 3065000265000001.(7966,6354) = (6317,6201).$ 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**