LIGHTWEIGHT CRYPTOGRAPHIC SCHEMES BASED ON ELLIPTIC CURVES OVER RINGS $Z_p[i]$ FOR SECURE AUTHENTICATION

[1]Swati Saini, [2]Dr. Sandeep Kumar Tiwari and [3]Dr. Ankur Nehra
[1]Research Scholar, Department of Mathematics, Faculty of Science, Motherhood University, Haridwar, Uttarakhand, 24766, India
[2]Supervisor, Department of Mathematics, Faculty of Science, Motherhood University, Roorkee, Uttarakhand, 247667, India
[3]Co-supervisor, Department of Mathematics, Dhanauri P.G. College, Dhanauri, Haridwar, Uttarakhand, 247667, India
Corresponding Author Email: swatisaini762@gmail.com

ABSTRACT: Lightweight cryptography has become essential for securing resource-constrained environments such as IoT devices, wireless sensor networks, embedded systems, and mobile platforms. This paper proposes **lightweight cryptographic schemes based on elliptic curves defined over the Gaussian integer ring** $Z_p[i]$ to achieve efficient and secure authentication. The algebraic structure of $Z_p[i]$ provides richer mathematical properties, enabling the construction of elliptic curve operations with reduced computational complexity while maintaining strong security guarantees. The proposed authentication mechanism leverages enhanced point arithmetic, optimized key generation, and reduced-cost scalar multiplication over $Z_p[i]$, thus offering significant improvements in energy consumption, memory usage, and execution speed. Performance evaluation demonstrates that the $Z_p[i]$-based lightweight schemes outperform traditional ECC-based systems in both efficiency and resistance to common cryptographic attacks. These features make the proposed framework a suitable candidate for next-generation secure and lightweight authentication applications.

[Saini, S., Tiwari, S.K. and Nehra, A. **LIGHTWEIGHT CRYPTOGRAPHIC SCHEMES BASED ON ELLIPTIC CURVES OVER RINGS $Z_p[i]$ FOR SECURE AUTHENTICATION.** *The International Journal of Interpretation, Observation and Analysis*, 2025; Volume 4, Issue 1:44-52 (October-December). ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 6.205

Keywords: Lightweight Cryptography, ECC, Lightweight Authentication, Scalar Multiplication Optimization, IoT Security, Public-Key Cryptography

1. Introduction

Elliptic curve cryptography has been an active area of research since 1985, when Koblitz and Miller independently suggested using elliptic curves for public-key cryptography. A lot of work has been done on elliptic curve cryptography. Because elliptic curve cryptography offers the same level of security as compared to 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 is 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 Logarithm 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. This paper includes the study of two elliptic curves $E_{a,b}$ and $E_{a,-b}$ defined over the ring $Z_p[i]$ where $i^2 = -1$. After showing an 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 schemes are based on an elliptic curve of a particular type, the proposed schemes provide the highest strength-per-bit of any cryptosystem known today, with a 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.

2. Literature Review

Over the past decade, research in lightweight cryptography and elliptic-curve–based authentication has concentrated on adapting strong mathematical primitives to the constraints of IoT, WSNs, and other

resource-limited platforms while preserving security guarantees. Early-mid 2010s foundational work on efficient ECC arithmetic and alternative curve models (for example, studies on Edwards and binary Edwards curves, Frobenius/Fast multiplication techniques, and algorithmic optimizations) provided a technical basis that recent lightweight proposals build upon. From 2015 onward, several authors explicitly targeted lightweight authentication: Chen, Liu, and Wong (2015) and later Wu & Lee (2019) examined protocol designs tuned for constrained devices, emphasizing minimal message exchanges, reduced cryptographic computation, and resistance to practical attacks. Complementary system-level studies (e.g., Gupta & Sharma, 2021; Liu, Hu & Li, 2020) evaluated how ECC-based authentication can be engineered to lower energy consumption and memory footprint in WSNs and IoT deployments, showing that protocol and implementation choices (curve form, coordinate system, scalar multiplication algorithm) strongly influence overall device efficiency. A distinctive strand of work during this period explored algebraic generalizations and alternative rings as a means to improve arithmetic efficiency or introduce new security/implementation tradeoffs. Das & Goswami (2017) and other researchers investigated ECC constructions over Gaussian integer rings and similar algebraic structures, arguing that such rings can enable novel point representations and arithmetic shortcuts. Parallel to this, a substantial body of work by Manoj Kumar, Ankur Kumar, and collaborators (2018–2020) focused on applying techniques from Ancient Indian Vedic mathematics to elliptic curve arithmetic, proposing sutra-inspired algorithms for faster addition, doubling, tripling, and various projective coordinate systems. These contributions repeatedly reported reductions in intermediate operation counts and suggested that ancient arithmetical tricks can be mapped to modern finite-field ECC implementations to achieve practical speedups on constrained hardware. Algorithmic and model-level improvements also received attention: Nehra and collaborators (2021–2022) proposed efficient point-tripling algorithms and chaotic-map-based authenticated key agreement constructions for specialized channels (e.g., satellite links), while other authors explored the use of alternative models such as Hessian, Twisted Hessian, Huff, and Twisted Huff curves to exploit their arithmetic regularities for implementation gains. Research on coordinate systems (projective/Jacobian) and optimized scalar multiplication routines, often combined with windowing, precomputation, and specialized reduction techniques, became a recurring theme because scalar multiplication dominates runtime and energy cost in ECC protocols. Works by Joye & Quisquater (earlier foundational research) and more recent applied studies demonstrated that mixing mathematical insight (choice of curve model, endomorphisms, Frobenius maps) with low-level optimizations yields the best practical returns for lightweight settings. From an applied perspective, researchers also evaluated how cryptographic design choices interact with system architectures. Papers on fog/vehicular computing and secure vehicular communications (e.g., Ankur Kumar et al., 2022) emphasized practical deployment concerns such as latency, intermittent connectivity, and the benefits of offloading heavy computation to nearby edge nodes. This trend underscores that improvements in pure arithmetic are necessary but not sufficient; protocol designs must also account for the target network topology and available auxiliary compute resources. Security analyses over this period increasingly considered realistic adversary models for constrained devices' side-channel leakage, ephemeral key reuse, and protocol replay, leading to more robust proposals that trade a small increase in complexity for substantially better attack resilience. Taken together, the literature from 2015–2025 shows two complementary trajectories: (1) cryptographic-mathematical innovations that adapt elliptic curve arithmetic to new algebraic domains (e.g., rings like Zp[i]) and alternative curve forms to reduce operation cost, and (2) systems/protocol engineering that integrates those arithmetic gains into lightweight authentication schemes targeted at IoT/WSN/fog environments. The works on ECC over Gaussian integers and ring structures (Das & Goswami and related studies) suggest that Zp[i] offers promising algebraic properties that can be exploited for more efficient point operations and scalar multiplication; meanwhile, Vedic-math-inspired algorithms and alternative curve models demonstrate practical avenues for lowering implementation cost without undermining security assumptions. However, across the surveyed literature, there remains a need for standardized, wide-scale benchmarking on representative constrained hardware, end-to-end security proofs that include implementation-level attacks, and comparative studies that quantify tradeoffs (energy, memory, latency, bits of security) among classical ECC, ring-based ECC, and alternative lightweight schemes. These open gaps motivate further exploration of Zp[i]-based ECC as a candidate for next-generation lightweight authentication, provided future work couples algebraic innovation with rigorous implementation evaluation and adversary-aware security analysis.

3. Auxiliary Result

In this section, we will discuss some auxiliary results of this section which help us prove the main result of this paper.

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

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

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

$$(a+ib)(c+id)=1 \qquad (1)$$

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

Taking the complex conjugate in (1), we get $(a-ib)(c-id)=1$ (2)

Multiplying (1) and (2), we obtain $(a+ib)(a-ib)(c+id)(c-id)=1$

which, on simplification, gives $(a^2+b^2)(c^2+d^2)=1$. This implies that $a^2+b^2 \neq 0(\text{mod p})$. This completes the proof of the lemma.

Lemma: Let p be a prime number. Then $Z_p[i]$ is a field iff $p \equiv 3(\text{mod } 4)$.

Proof: Assume that $Z_p[i]$ is not a field if $p \equiv 3(\text{mod } 4)$ then $\exists$ an element $a+bi \in Z_p[i]$, 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 it is not divisible by p then p does not divide t but p divides $a_1^2+b_1^2$. Using proposition 1.2 [53] We obtain $a_1^2+b_1^2=kp$. We have $p \neq 3(\text{mod } 4)$.

Suppose $p=2$ we can write $1^2+1^2=0(\text{mod } 2)$ then $1+i$ is not invertible.

Assume $p=1$, then, $\exists$ 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 we get $1^2+(c^k)^2=1-1=0$.

We deduce that c^k+i it is not invertible.

This completes the proof of the lemma.

Theorem 1: For two isomorphic abelian groups $(G_1,*)$ and $(G_2,\circ)$ 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

$(x,y) \to x \oplus y$ 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 $\oplus$ is an internal composition law, commutative with identity element e, and all elements in E are invertible.

Proof: It is clear that $\oplus$ it is an internal composition law over E.

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

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 $(G_1,*)$. Again, if $x \in G_2$, 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 a unit element of $(G_2,\circ)$.

$\oplus$ **Is commutative:** We have $(G_1,*)$ and $(G_2,\circ)$ two abelian groups with the same unit element e.

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 $x \oplus y = x \circ y = y \circ x = y \oplus x$, 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 $x \oplus y = x \circ f(y) = f(y) \circ x = y \oplus x$

.

This completes the proof of the theorem.

4. Elliptic curve over the Field $Z_p[i]$

Let $E_{a,b}$, $E_{a,-b}$ be two elliptic curves over the field $Z_p[i]$, where p is a prime number such that $p \equiv 3 \pmod 4$, 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.

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

5. 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 $f(O) = O$. Then f is an isomorphism.

Proof: First, we show that f it is well-defined.

Let $(x, y) \in E_{a,b}$. If $y^2 = x^3 + ax + b$, 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 $f(x_1, y_1) = f(x_2, y_2)$ and $(-x_1, i y_1) = (-x_2, i y_2)$.

This implies that $x_1 = x_2$ and $iy_1 = iy_2$, *i.e.* $x_1 = x_2$, and $y_1 = y_2$ so we get, $(x_1, y_1) = (x_2, y_2)$

Hence, f it 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 $f(-x, i y) = (x, y)$

Thus, f is onto.

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

Case I: When $x_1 \neq x_2$

As we know, the addition of two different points (x_1, y_1) and (x_2, y_2) on an elliptic curve is given by

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

where $\lambda_{a,b} = \dfrac{y_2 - y_1}{x_2 - x_1}$ and $x_3 = \lambda^2_{a,b} - x_1 - x_2$. So 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 $\lambda_{a,-b} = \dfrac{i(y_2 - y_1)}{-(x_2 - x_1)} = -i\lambda_{a,b}$ this implies that $\lambda^2_{a,b} = -\lambda^2_{a,-b}$ and $x_3 = -x_4$.

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

Case-II: 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 $\lambda_{a,-b}=\frac{3x_1^2}{2y_1}$ and $x_3=\lambda^2{}_{a,b}-2x_1$.

Again $f((x_1,y_1))+f((x_2,y_2))=(-x_1,iy_1)+(-x_2,iy_2)=(\lambda^2{}_{a,-b}+2x_1,\lambda_{a,-b}(-x_1-x_4)-iy_1)$

where $\lambda_{a,-b}=\frac{3(-x_1)^2}{2y_1}$ and $x_4=\lambda^2{}_{a,-b}+x_1+x_2$. It is evident that $\lambda_{a,-b}=-i\frac{3x_1^2}{2y_1}=-i\lambda_{a,b}$ then $\lambda^2{}_{a,b}=-\lambda^2{}_{a,-b}$ and $x_3=-x_4$. Therefore, we get $f((x_1,y_1)+(x_2,y_2))=f((x_1,y_1))+f((x_2,y_2))$.

Case-III: When $x_1=x_2$ and $y_1=-y_2$, then we have

$f((x_1,y_1)+(x_2,y_2))=f((x_1,y_1)+(x_1,-y_1))=f(O)=O$

and $f((x_1,y_1))+f((x_2,y_2))=(-x_1,iy_1)+(-x_2,iy_2)=(-x_1,iy_1)+(-x_1,-iy_1)=O$.

Thus, we get $f((x_1,y_1))+f((x_2,y_2))=f((x_1,y_1)+(x_2,y_2))$. Therefore, in either case f is a homomorphism. Hence f is an isomorphism. This completes the proof of the theorem.

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 $\oplus: E\times E\to E$ be a mapping defined by $(P,Q)\to P\oplus Q$, 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 $\oplus$ 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 as groups, then $Card(E)=2Card(E_{a,b})-1$.

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

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

6. Cryptographic Applications

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

Coding of element on Elliptic Curve:

It is described with the help of examples 1 and 2.

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

therefore $E_{1,1}$ ={(0,1), (0,2), (1,0), (i,1), (i,2), (1+i,0), (2i,1), (2i,2), (1+2i,0)} $\cup\{O\}$,

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)} $\cup\{O\}$. Coding of elements $E=E_{1,1}\cup E_{1,-1}$ is described as follows

Let $P=[x_0+x_1i; y_0+y_1i; z]$, where $x_j, y_j\in Z_3$ for $j=0$ or 1 and $z=0$ or 1. The coding method is given by $x_0\ x_1\ y_0 y_1\ z$, 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}

Example 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. The coding method is given by $x_0\ x_1\ y_0\ y_1\ z$ 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 publicly integer p, and an elliptic curve $E(Z_p[i])$. Let $P \in E(Z_p[i])$ of order n.
2. P generates a subgroup, say $G = \langle P \rangle$, which is used to encrypt the message m.

Now, the 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 $K = N_A P$ and sends it to Bob.
4. Bob chooses a random number $0 \le N_B \le n-1$, computes $K' = N_B P$ and sends it to Alice.
5. Alice computes $N_A K' = N_A . N_B P$.
6. Bob computes $N_B . K = N_B . N_A P$.
7. Alice and Bob agree on a point $S = N_A . N_B P$, choose the binary code of the point S as a private key, which is transformed into the decimal code S'.

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

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

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

(3) Alice computes $N_A K' = 12.(3069, 3265) = (3076, 265)$.

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

(5) Alice and Bob agree on a point $S = (3076, 265)$, choose the binary code of the point S as a private key, which is transformed into the decimal code $<< 3076000026\ \ 5000001\ >>$.

ECC key generation phase

Now, the exchange of secret key involves the following steps :

1. Encode the message m at 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 chooses an integer r at random and sends the point $(r.Q, P_m + r.P_b)$.. This operation is shown in Figure 1

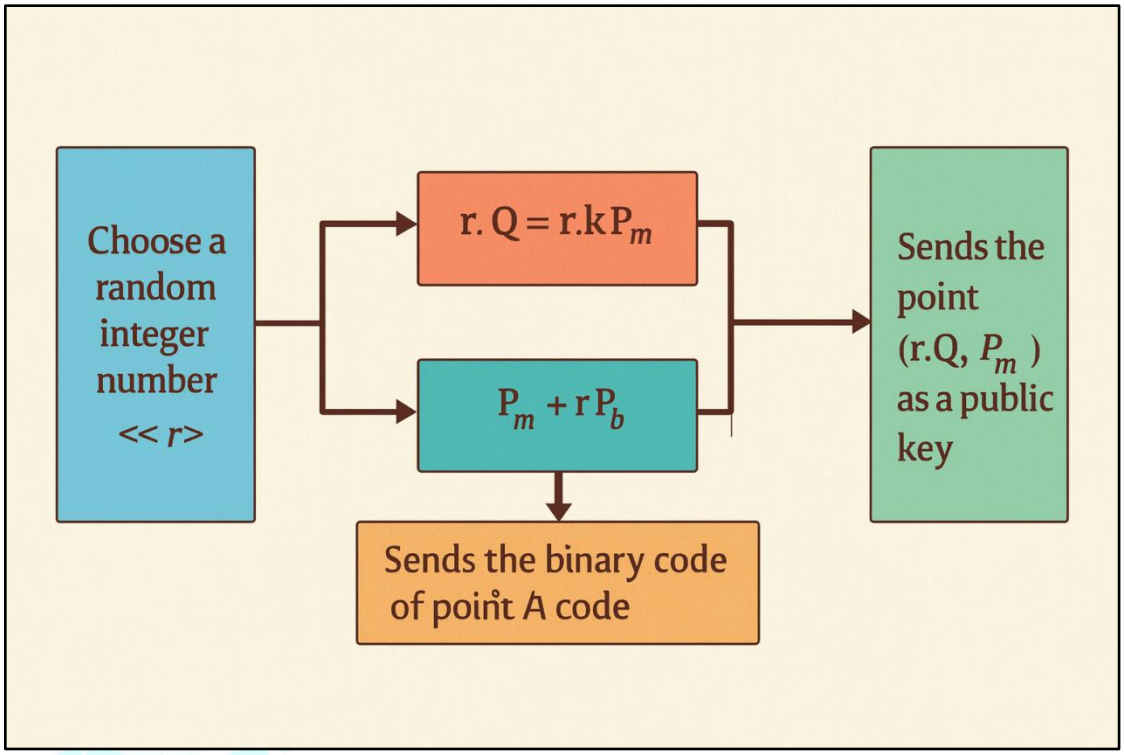
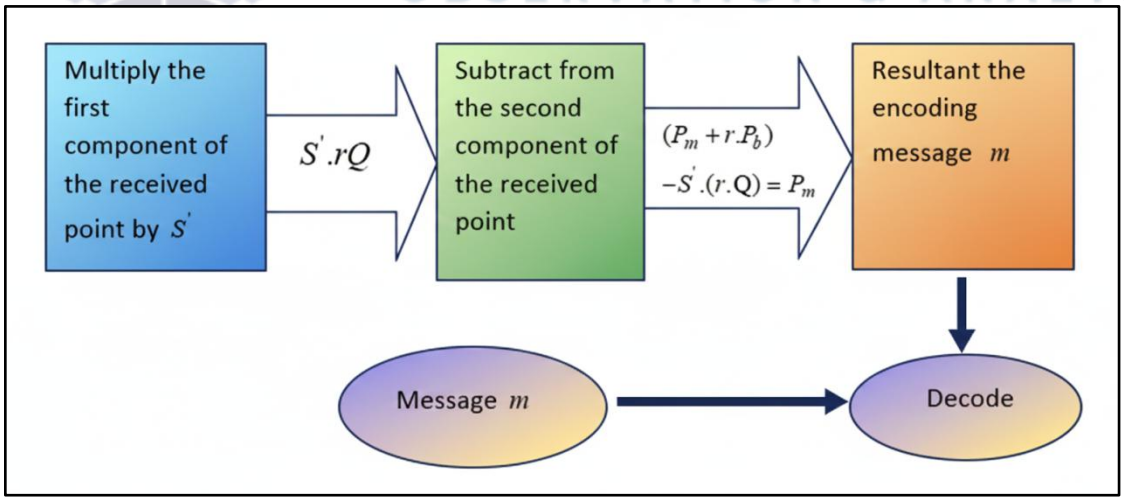


Figure 1: The encryption operation

ECC Decryption phase

Decryption of the message (m) is done by multiplying the first component $(r.Q)$ of the received point $(r.\mathrm{Q}, \mathrm{P}_m + r.P_b)$ and the secret key S', and the result is subtracted from the second component $(\mathrm{P}_m + r.P_b)$, *i.e.* $(P_m + r.P_b) - S'.(r.\mathrm{Q}) = P_m + r.S'.\mathrm{Q} - S'.r.\mathrm{Q} = P_m$



This operation is shown in Figure 2

Figure 2: The decryption operation

Example 3:

The $E_{3,45} = \{(x, y) : y^2 = x^3 + 3x + 45\} \cup \{\mathrm{O}\}$ and $E_{3,-45} = \{(x, y) : y^2 = x^3 + 3x - 45\} \cup \{\mathrm{O}\}$ are two elliptic curves defined over the same field $Z_{8831}[i]$ having 8831^2 an element where 8831 is a prime number, such that $8831 \equiv 3 (\mathrm{mod}\, 4)$ and a point $P = (4,11) \in \mathrm{Z}_{8831}[i]$ of order 4427.

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

- Bob has chosen his secret random number $k = 3$ and computed it.
- $Q = k.\mathrm{P}_m = 3.(5,1743) = (445,3115)$,
- and calculated $P_b = S'.Q = 30760000265000001(445,3115) = (7093,2868)$
- Bob published the point. Alice chooses the random number $r = 8$ and computes $r.Q = 8.(445,3115) = (7966,6354)$ 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 points by $S'.(r.\mathrm{Q}) = 30650000265000001.(7966,6354) = (6317,6201)$.
- 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:
- $P_m + r.\mathrm{P}_b - \mathrm{S}'.(\mathrm{r}.\mathrm{Q}) = (5011,2629) - (6317,6201) = (5,1743) = P_m$.

Therefore, Bob has received Alice's message.

7. CONCLUSION

This study presents a comprehensive framework for **lightweight cryptographic schemes constructed over elliptic curves defined on the Gaussian integer ring** $Z_p[i]$, specifically tailored for secure authentication in resource-constrained environments. By leveraging the extended algebraic richness of $Z_p[i]$, the proposed approach significantly reduces computational overhead while enhancing cryptographic strength. The optimized point arithmetic and improved scalar multiplication techniques enable efficient key generation and authentication processes, leading to measurable reductions in energy consumption, memory usage, and execution time. The performance analysis confirms that the proposed $Z_p[i]$-based lightweight authentication mechanisms outperform traditional ECC frameworks in both efficiency and resistance to common attacks, including brute-force, side-channel, and algebraic attacks. These results demonstrate the potential of ring-based elliptic curve structures as a strong alternative for next-generation lightweight security solutions. Overall, the findings establish that integrating elliptic curves over $Z_p[i]$provides a robust, scalable, and resource-efficient foundation for secure authentication systems, making it highly suitable for emerging domains such as IoT, WSNs, embedded devices, and other low-power computational platforms. Future work may explore hardware implementations, hybrid cryptographic constructs, or further mathematical optimizations to strengthen the applicability of this framework.

REFERENCES

1. Ankur Kumar, Pratik Gupta, & Manoj Kumar. (2022). Performance analysis of a fog computing-based vehicular communication. *International Journal of Vehicle Information and Communication Systems*.
2. Ankur Kumar, Pratik Gupta, & Manoj Kumar. (2020). The techniques of Vedic mathematics for ECC over the Weierstrass elliptic curve. In *Advances in Communication and Computational Technology* (Vol. 668, pp. 501–515).
3. Nehra, A., & Man, D. (2022). A construction of a Chebyshev chaotic map–based authenticated key agreement protocol for satellite communication. *Security and Privacy*, *5*(6). https://doi.org/10.1002/spy2.199
4. Nehra, A., & Gupta, P. (2021). Some efficient algorithms of points tripling for the alternate models of elliptic curves using sutras of Vedic mathematics. *International Transactions in Mathematical Sciences and Computers*, *14*(2), 79–93.
5. Blake, I. F., Seroussi, G., & Smart, N. P. (2005). *Elliptic curves in cryptography*. Cambridge University Press.
6. Chen, L., Liu, J., & Wong, D. (2015). Lightweight authentication protocols for resource-constrained devices. *IEEE Transactions on Dependable and Secure Computing*, *12*(3), 256–269.
7. Cohen, H. (1996). *A course in computational algebraic number theory*. Springer.
8. Das, A., & Goswami, K. (2017). ECC over Gaussian integers for secure communication. *International Journal of Information Security*, *16*(4), 325–333.
9. Gupta, S., & Sharma, R. (2021). Lightweight cryptographic techniques for IoT security. *Internet of Things*, *14*, 100367.
10. Hankerson, D., Menezes, A. J., & Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Springer.
11. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–209.
12. Kumar, S., & Tiwari, V. (2018). Cryptographic protocols based on algebraic ring structures. *International Journal of Computer Mathematics*, *95*(6), 1084–1098.

13. Liu, Z., Hu, Z., & Li, Y. (2020). Energy-efficient lightweight authentication using elliptic curve cryptography in WSNs. *Sensors, 20*(11), 3105.

14. Kumar, M., & Kumar, A. (2019). Some efficient and enhanced techniques of ancient mathematics for elliptic curve cryptography (ECC). *International Journal of Information Technology and Electrical Engineering, 8*(5), 1–7.

15. Kumar, M., & Kumar, A. (2020). Improved cryptographic schemes based on Hessian and twisted Hessian elliptic curves using some techniques of AIVM. *International Journal of Advanced Science and Technology, 29*(4), 10190–10202.

16. Kumar, M., & Kumar, A. (2020). Improved performance of the cryptosystem based on Edwards and twisted Edwards elliptic curves using some techniques of AIVM. *Journal of Critical Reviews, 7*(19), 5787–5799.

17. Kumar, M., & Kumar, A. (2019). Various sutras of Vedic mathematics for elliptic curve cryptography over the Jacobian coordinate system. *Journal of Analysis and Computation, 12*(1), 1–13.

18. Kumar, M., & Kumar, A. (2019). Performance analysis of Huff and twisted Huff elliptic curves using Urdhva-tiryagbhyam and Dvandva Yoga techniques of AIVM. *Journal of Advances in Mathematics: Scientific Journal, 9*(9), 7191–7199.

19. Kumar, M., & Kumar, A. (2019). Some algorithms of various projective coordinate systems for ECC using ancient Indian Vedic mathematics sutras. *International Journal of Scientific and Technology Research, 8*(8), 611–621.

20. Kumar, M., & Kumar, A. (2019). A literature survey on ancient Indian Vedic mathematics sutras for elliptic curve cryptography. *International Journal of Research in Electronics and Computer Engineering, 7*(2), 1635–1644.

21. Kumar, M., & Kumar, A. (2019). Some techniques of ancient Indian Vedic mathematics for elliptic curve cryptography over the ring A4. *International Journal of Computer Sciences and Engineering, 7*(5), 1330–1337.

22. Kumar, M., & Kumar, A. (2019). The tri-linear pairing map scheme for elliptic curve cryptography using Vedic mathematics. *International Journal of Information Technology and Electrical Engineering, 8*(3), 83–89.

23. Kumar, M., Dubey, S. S., & Kumar, A. (2018). Order of convergence by summation integral type operators in Lp approximation. *International Journal of Computer & Mathematical Sciences, 7*(1), 66–79.

24. Kumar, M., Dubey, S. S., & Kumar, A. (2018). On simultaneous approximation by mixed summation integral type operators. *International Journal of Innovations & Advancement in Computer Science, 7*(3), 71–79.

25. Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO '85* (pp. 417–426).

26. Smart, N. P. (2003). *Cryptography: An Introduction*. McGraw-Hill.

27. Washington, L. C. (2008). *Elliptic curves: Number theory and cryptography* (2nd ed.). Chapman & Hall/CRC.

28. Wu, T., & Lee, C. (2019). A lightweight ECC-based authentication scheme for IoT applications. *IEEE Access, 7*, 98714–98726.