

## ELLIPTIC-CURVE GROUPS IN QUANTUM-ERA CRYPTOGRAPHY

Michael N. John<sup>\*1</sup>, Udoaka O. G.<sup>2</sup>, Boniface O. Nwala<sup>3</sup><sup>1,2</sup> Department of Mathematics, Akwa Ibom State University<sup>3</sup> Department of Mathematics, Ignatius Ajuru University of Education.**\*Corresponding Author**

Michael N. John

Department of Mathematics, Akwa  
Ibom State University.**Article History**

Received: 09.10.2023

Accepted: 19.10.2023

Published: 12.11.2023

**Abstract:** Elliptic-curve group cryptography (ECC) has been widely recognized as a robust and efficient cryptographic system in the classical era. However, with the emergence of quantum computing, traditional public key cryptosystems are at risk of being broken, which has prompted the exploration of alternative cryptographic methods. This research paper explores the fundamental aspects of elliptic curve groups in cryptography, their properties, and their application in cryptographic protocols in quantum era, focusing on the potential vulnerabilities of ECC in the quantum computing age and the efforts to develop post-quantum secure ECC-based schemes.

**Keywords:** Elliptic-curve group, ECC, Cryptography, Encryption, Decryption.

## 1. INTRODUCTION

Cryptography plays a pivotal role in the safeguarding of sensitive information in today's digital world. Elliptic-curve Group Cryptography has gained significant attention due to its computational efficiency and strong security guarantees. Researchers began to explore other ways of enhancing secure encryption because of the threat of quantum computers. [6] has worked on Algorithm and Cube-Lattice-Based Cryptography, and [7] has a paper on Computational Group Theory and Quantum-Era Cryptography.

This paper provides an in-depth analysis of elliptic-curve groups and their applications in quantum era cryptographic schemes.

Elliptic curves are algebraic structures, defined by the equation;  $y^2 = x^3 + ax + b$  where  $a$  and  $b$  are curve parameters. The group structure of elliptic curves facilitates point addition and multiplication, which forms the foundation for ECC.

[1] Laid the groundwork for ECC. [2] On work on the Weil and Tate pairings introduced new avenues for cryptographic protocols.

## 2. FUNDAMENTAL CONCEPT

**Theorem;** The points on elliptic curve, together with  $\mathcal{O}$ , forms an abelian group under "geometric point addition"

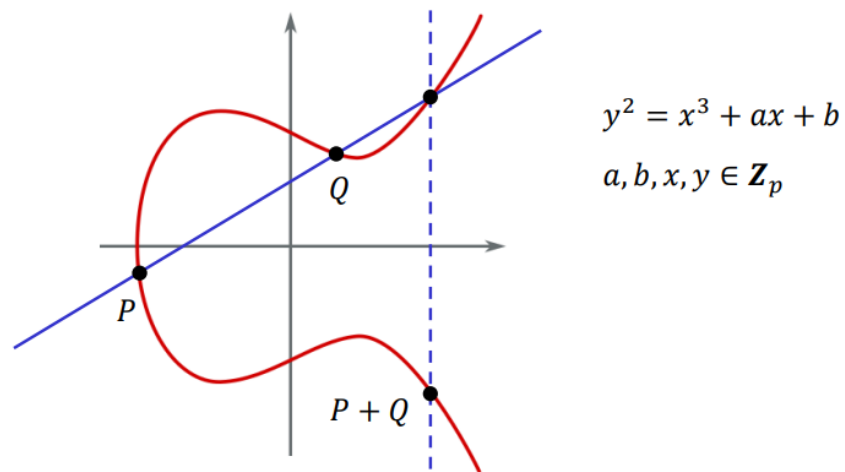
**Notation**

- $(E(\mathbb{R}), +)$  = is an elliptic curve group defined over the reals field.

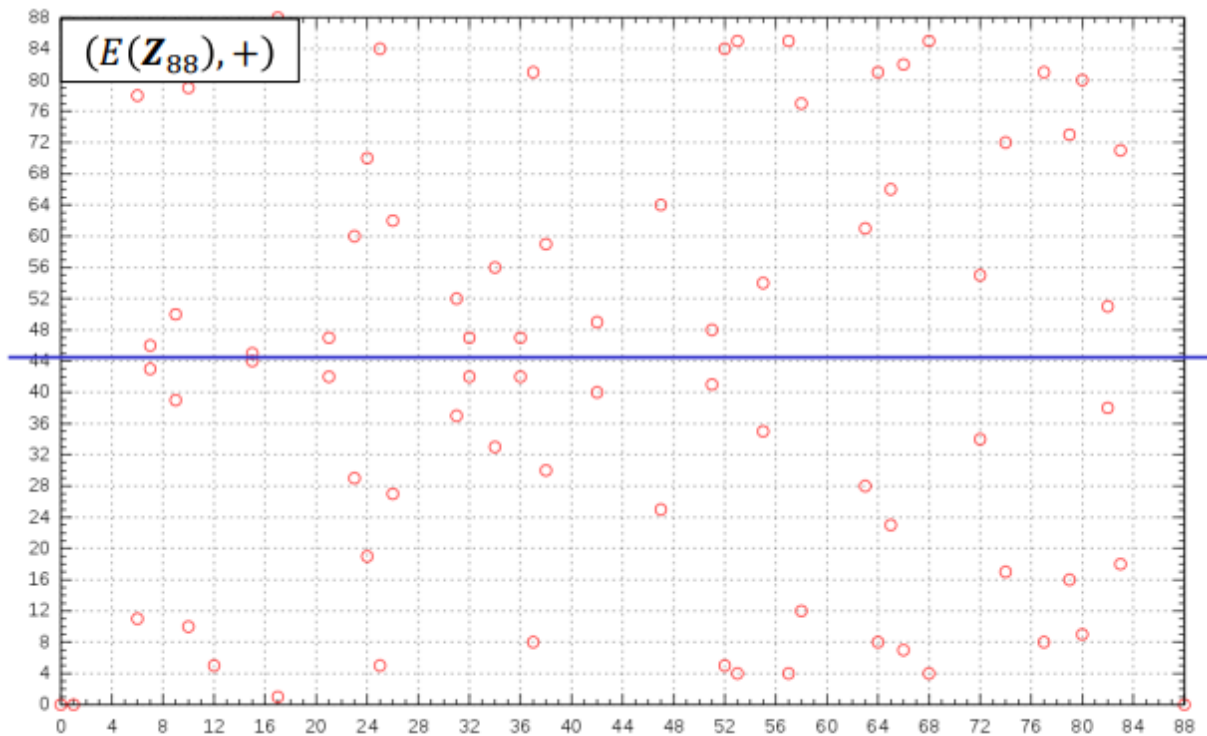
[3] has a comprehensive reference book that covers various aspects of cryptography, including elliptic curve cryptography. [4] Discussed the security of elliptic curve cryptography and its provable security properties on his paper; another look at 'provable security'.

Elliptic curve cryptography (ECC) is plays a significant part in modern cryptography due to the strong security mathematical properties it has, and efficiency. However, the advent of quantum computing has the potential to threaten the security of traditional ECC-based cryptographic schemes, as Shor's algorithm is efficient in solving the discrete logarithm problem (DLP), on which ECC relies. In response to this quantum threat, researchers have explored various approaches to secure elliptic curve groups in the quantum era. [5] introduced the concept of isogeny-based cryptography, which is a promising approach for post-quantum elliptic curve cryptography. Later on, [6] on his work explored the security aspects of supersingular isogeny-based cryptography. Recently, [8] discussed security considerations in the context of supersingular isogeny-based cryptosystems.

## Elliptic curves



- $(E(\mathbb{Z}_p), +)$  is an elliptic curve group defined over the  $\mathbb{Z}_p$



$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$x_3 = \frac{(x_1 x_1 - 2a)x_1 x_2 - 4b(x_1 + x_2) + a^2}{(x_1 x_2 + a)(x_1 + x_2) + 2y_1 y_2 + 2b}$$

$$y_3 = \frac{x_1 x_1 (x_1 + x_2) - x_3 (x_1 + x_2)^2 - x_1 x_1 + a - y_1 y_1 - b}{y_1 + y_2}$$

Currently no attacks has manage to exploit the algebraic structure of  $((\mathbb{Z}_p), +)$ . Best-know attacks are generic attacks, Baby-step giant-step, Pollard-rho • etc

### 3. COMPUTATIONAL KEY-EXCHANGE PROTOCOL

ECC-based key exchange protocols, such as ECDH, provide secure communication channels. Creating a full implementation of elliptic curve cryptography (ECC) in Python for encryption, decryption, key exchange, and security is a complex task that goes beyond a simple code example. However, we have provided a high-level overview and some code snippets on this section for key generation, encryption, and decryption, using ECC. You may need to implement additional security measures and details for a production-ready system.

1. Install the cryptography module:

```
pip install cryptography
```

2. ECC Key Generation:

```
from cryptography.hazmat.primitives.asymmetric import ec

# Generate an ECC key pair

private_key = ec.generate_private_key(ec.SECP256R1()) #
You can choose a different curve

public_key = private_key.public_key()
```

3. ECC Encryption:

```
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import ec
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding

# Loading the recipient's public key

recipient_public_key_pem =
"RECIPIENT_PUBLIC_KEY_PEM" # Replace with the
recipient's public key

recipient_public_key =
serialization.load_pem_public_key(recipient_public_key_pem
)

# Generating a shared secret

shared_key = private_key.exchange(ec.ECDH(),
recipient_public_key)

# Encrypt a message

message = b"Your message to encrypt"

ciphertext = recipient_public_key.encrypt(
message,
```

```
padding.OAEP(
    mgf=padding.MGF1(algorithm=hashes.SHA256()),
    algorithm=hashes.SHA256(),
    label=None
)
)
```

4. ECC Decryption

```
# Decrypt the message

plaintext = private_key.decrypt(
    ciphertext,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)
```

Keep in mind that ECC operations require careful handling of private keys and ciphertexts to ensure security. You should also consider error handling, proper key storage, and additional cryptographic best practices.

For a complete ECC-based security system, you would need to implement a protocol such as ECC-based key exchange (e.g., ECDH for key exchange) and use ECC for digital signatures in addition to encryption. The computational security of any ECC system is dependent on the choice of the elliptic curve, and the key sizes, so make sure to select appropriate parameters for your use case.

### 4. CONCLUSION

The era of quantum computing has introduced significant challenges to traditional ECC, but it has also sparked innovation in the development of quantum-resistant cryptographic solutions.

Elliptic curve groups have become a cornerstone of modern cryptography, offering a robust and efficient framework for secure communication. This paper presented an overview of fundamental concepts, applications with python.

### References

1. Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.
2. Miller, V. S. (1986). Use of elliptic curves in cryptography. *Advances in Cryptology—CRYPTO*.
3. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.
4. Kobitz, N., & Menezes, A. J. (2007). Another look at "provable security". In *Advances in Cryptology—CRYPTO'99* (pp. 171-191). Springer.

5. Jao, D., & De Feo, L. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4* (pp. 19-34). Springer Berlin Heidelberg.
6. Michael N. John & Udoaka O. G (2023). Algorithm and Cube-Lattice-Based Cryptography. *International journal of Research Publication and reviews*, Vol 4, no 10, pp 3312-3315 October 2023.
7. Michael N. John, Udoaka O. G., "Computational GroupTheory and Quantum-Era Cryptography",*International Journal of Scientific Research in Science,Engineering and Technology (IJSRSET)*, Online ISSN :2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 6,pp. 01-10, November-December 2023. Available at doi :<https://doi.org/10.32628/IJSRSET2310556>.