Comparative Study of Group Structures in Modern Cryptosystems

Bhavesh kumar sahu[1] , Dr. Akanksha Dubey[2]

[1] Dept of Mathematics

[2]Assistant Professor, Department of Mathematics

[1,2] Shri Rawatpura Sarkar University, Raipur, Chhattisgarh

Abstract- *An analysis of algebraic group structures used in contemporary cryptosystems is presented in this paper. The multiplicative group of integers modulo n (used in RSA and classical Diffie–Hellman), cyclic subgroups of finite fields, elliptic curve groups (used in ECC), pairing-based groups (bilinear pairings on elliptic curves), and other algebraic structures closely related to group theory that support post-quantum schemes (e.g., module/ring structures in lattice cryptography and isogeny-based groups) are all covered. We go over the mathematical description, cryptographic applications, security presumptions, algorithmic complexity (for group operations and principal assaults), efficiency and implementation factors, and suggested parameter selections for each structure. The study ends with a side-by-side comparison that highlights the advantages, disadvantages, and potential paths forward.The hardness of particular computational tasks specified over algebraic structures, especially groups, is a critical component of the security of contemporary public-key cryptosystems. The group structures underlying modern cryptographic schemes, such as finite cyclic groups (used in Diffie-Hellman and DSA), elliptic curve groups (ECC), and newly developed post-quantum structures like lattices, isogenies, and multivariate polynomials, are all thoroughly compared in this paper. We look at the mathematical underpinnings of each group, related hard problems, trade-offs between security and efficiency, implementation issues, and defense against classical and quantum attacks. The analysis shows that the emergence of quantum computing is propelling a shift toward more sophisticated non-abelian and structured lattice-based groups, even if elliptic curve groups now dominate practical deployments because to their efficiency and compactness.*

In order to help choose group structures for upcoming cryptography standards, this paper summarizes important findings.

Keywords: *fields, RSA, , bilinear pairings, Discrete Logarithm Problem, Elliptic Curve Cryptography, Lattice-Based Cryptography, Post-Quantum Cryptography, Group theory and Isogenies.*

I. INTRODUCTION

The algebraic foundation of many public-key cryptosystems is provided by group theory. An algebraic structure with an associative binary operation, an identity element, and an inverse for each element is called a group. In order to provide one-way functions, key exchange, signatures, and encryption, cryptography uses the computational difficulty of some problems specified over groups, most notably the Integer Factorization Problem (IFP) and the Discrete Logarithm Problem (DLP).The main group structures utilized in contemporary cryptography are examined in this study, along with a comparison of their computational and security characteristics and an analysis of how these characteristics affect the selection of practical protocols. The choice of group profoundly impacts security, key size, computational speed, bandwidth, and resistance to emerging threats like quantum computers.This paper systematically compares the primary group structures in use or under consideration for modern cryptosystems

II. MATHEMATICAL BACKGROUND

2.1 Fundamental definitions

• Group (G, *): A set G with an operation ∗ such that inverses, closure, associativity, and identity hold.
•An abelian group is one whose all operations are commutative.
• A cyclic group is one that is created by a single element g, meaning that each element is g^k for some integer k.
• Order: The order of an element (smallest positive m with g m = e) and the order of the group G (finite or infinite).

2.2 The Classical Foundation of Finite Cyclic Groups

Structure of Mathematics: Cryptosystems such as the Digital Signature Algorithm (DSA) and Diffie-Hellman Key Exchange (DHKE) function in the multiplicative group of a cyclic finite field F*p (or a subgroup thereof). The Discrete Logarithm Problem (DLP)—given g and h=gx in G, determine x—is the foundation of the security. For ~112-128 bit security, large parameters (2048-3072-bit primes) are required.

• Quantum Threat: Shor's method solves DLP in polynomial time O((log n)3), completely breaking it in a quantum setting.
• Features of Performance: • Key Size: Large (for example, 2048 bits for 112-bit security).
• Efficiency: For equivalent security, modular exponentiation requires more computing power than ECC operations.
• Bandwidth: Less effective in areas with limited resources. The original Diffie-Hellman over F*p system is an example.

III. MULTIPLICATIVE SUBGROUPS AND FINITE FIELD GROUPS

3.1 Multiplicative groups of finite fields

The multiplicative group F*q of a finite field Fq (where q=pm) is cyclic of order q−1. Cyclic subgroups of F*q are used in several cryptosystems (e.g., classical DH over prime fields when (q=p) or other pairing-friendly constructs).

3.2 Attacks and security

• DLP in finite fields: sub-exponential index-calculus techniques; the degree of extension and field characteristics determine the difficulty. Special attacks (Coppersmith, etc.) may be quicker for limited characteristic fields.

3.3Applications

• Conventional DH over prime fields F*q • Multiplicative groups of finite field extensions (the target group GT in pairings) are occasionally used in pairing constructions.

IV. GROUPS OF ELLIPTIC CURVES

4.1 Meaning

The collection of solutions (x, y) to a cubic equation (short Weierstrass form:
$y^2 = x^3+ax+b$) plus a point at infinity O constitute an elliptic curve E over a field Fq. A geometric chord-and-tangent rule states that points on E form an abelian group.

4.2 Benefits of cryptography

•Because there are no known sub-exponential methods (like index calculus) for universal elliptic curves—the most well-known attacks are generic (Pollard rho) with O(p) complexity—smaller key sizes are required for comparable security to finite-field systems.
•ECC security is based on the elliptic-curve discrete log problem (ECDLP).

4.3 Common curves and applications

NIST P-256/P-384, Curve25519, and Curve448 are examples of widely used curves. Critical implementation aspects include side channel protection and constant-time arithmetic.

4.4 Effectiveness

• Applications: ECDH, ECDSA, EdDSA, and many contemporary protocols (TLS, SSH, blockchain wallets). • Point addition and doubling are more computationally costly per operation than modular multiplication, but smaller parameter values mean overall better performance and storage.

4.5 Security factors

• It is necessary to steer clear of weak curves with small subgroup factors or unique structure (anomalous curves).
• Validation of public points, cofactor handling, and twist-security are crucial.

V. GROUPS BASED ON PAIRINGS (BILINEAR MAPS)

5.1 Group tuple and definition

Three groups G1, G2 (often additive groups of points on elliptic curves), a multiplicative target group Gt (a subgroup of the multiplicative group of a finite field), and a bilinear map $e:G1\times G2\rightarrow Gt$ that satisfies bilinearity, non-degeneracy, and computability are used in pairing-based encryption.

5.2 Applications of cryptography

• Pairings are used in attribute-based encryption, identity-based encryption (IBE), short signatures, and several sophisticated primitives.

5.3 Assumptions about security

• Hardness depends on assumptions such as Bilinear Diffie-Hellman (BDH) or variations (SXDH, XDH) and DLP variants in source/target groups.
• Security relies on thwarting attacks on finite-field DLP in Gt and on carefully choosing the embedding degree and pairing type (Weil, Tate, optimal ate pairing).

5.4 Trade-offs between efficiency and parameters

• Although pairing computation (ate pairing, Miller loop, final exponentiation) can be optimized, it is more costly than fundamental EC operations.
• To provide effective pairings and an appropriate embedding degree, pairing-friendly curves (BN, BLS, and KSS families) are selected

VI. ISOGENY-BASED AND CLASS GROUPS

6.1 Cryptography and class groups

Class groups with imaginary quadratic orders, which often have non-cyclic structures and offer various hardness assumptions, have been suggested as group platforms for cryptography.

6.2 Cryptography based on isogeny

The group-like action of class groups on isogeny graphs of elliptic curves is used by isogeny-based schemes (e.g., SIDH/SIKE historically, and more contemporary schemes using CSIDH-style methods). Although these architectures can be difficult to build and analyze, they are appealing for small key sizes and small ciphertexts in post-quantum situations.

6.3 Security

The most well-known quantum algorithms for isogeny problems are now worse than those for factoring/DLP, although research is moving quickly. The necessity for careful investigation is highlighted by the failure of certain early isogeny concepts (such as SIKE). Structure of Mathematics: The elements of an abelian group formed by an elliptic curve E over a finite field Fq are points (x,y) that fulfill the curve equation plus a point at infinity. A cyclic subgroup of big prime order points is used in cryptography.

- Bandwidth: Perfect for IoT and mobile devices. Examples of systems include EdDSA, ECDSA (signatures), and ECDH (key exchange). Benefits Compared to Finite Cyclic Groups
- Signatures and keys are smaller.
- Quicker computation.
- Less power is used.

One of its limitations is that it is not quantum resistant.

- Implementation hazards, such as invalid curve attacks and side channels

VII. ALGEBRAIC STRUCTURES: LATTICES AND RINGS IN POST-QUANTUM CRYPTOGRAPHY

7.1 Lattices

Instead of using traditional group-theoretic discrete-log hardness, lattice-based systems (such as NTRU, Kyber, and Dilithium) rely on module/lattice and ring structures. They use algebraic structures (modules over rings) that enable signatures, key exchange, and trapdoor functions, even though they are not groups in the same sense.

7.2 Usefulness as a benchmark

Even though these are not group-based constructions, they are the main post-quantum alternative to traditional group-based cryptography and should be taken into account when comparing algebraic platforms. Leading prospects for post-quantum cryptography (PQC) are lattice-based groups and structures.

7.3. Other Post-Quantum Group Structures: These include multivariate polynomial systems and isogeny-based (commutative supersingular elliptic curve groups). The underlying hard problem, asymptotic security parameters, computing efficiency, key/ciphertext sizes, and quantum resistance are the axes along which we assess these groups. Structure of Mathematics: Structured infinite groups, or lattices, that are formed from high-dimensional geometry problems are used in lattice cryptography. A discrete subgroup of Rn is called a lattice. Typically, cryptosystems employ quotients of polynomial rings, such as Rq=Zq[x]/(f(x)), which are finite modules whose security is related to the lattice structure but not strictly groups in the sense of cryptographic operations.

7.4. Ring-LWE (RLWE)

A structured, effective variation that makes use of polynomial rings.

Security: • Classical & Quantum: For both classical and quantum computers, the most well-known attacks (which use lattice reduction techniques like BKZ) are exponential. Shor's algorithm is the only known polynomial-time quantum algorithm.

- Efficiency: Polynomial convolutions or linear algebra operations may be quick, but they are frequently slower than ECC.
- Versatility: Enables key exchange, encryption, signatures, FHE, and more.

Systems include Kyber (KEM, NIST PQC standard), NTRU, and Dilithium (signatures, NIST standard).

Comparing Cyclic/ECC Groups:

- Advantage: Very adaptable and quantum-resistant.
- Drawback: New and less studied than ECC/DLP, with larger keys and ciphertexts.

7.5. Additional Group Structures After Quantum

- One challenging problem is the Supersingular Isogeny Diffie-Hellman (SIDH) problem.. The original SIDH has been compromised by recent assaults (2022) employing the "GLV/GLS endomorphism". Variants like SQISign (signatures) and CSIDH (using commutative class groups) are still being researched.
- Features: Slow operations and continuous security analysis, but very short keys (competing with ECC).

7.6. Cryptography Using Multivariate Polynomials

- Structure: Predicated on how challenging it is to solve nonlinear polynomial problems over finite fields. The trapdoor is a well-organized collection of maps that are simple to flip.
- The Multivariate Quadratic (MQ) problem is a hard problem (NP-hard in general).
- Features include big public keys (tens to hundreds of kilobytes), tiny signatures, and extremely quick operations. For instance, GeMSS and Rainbow (signature, certain parameter settings broken).

Efficiency vs. Security Trade-off Groups with the most compact representations and fastest operations (ECC) are quantum-vulnerable, as the table shows a fundamental tension. Larger data overheads are usually associated with quantum-resistant groups (Lattice, Multivariate). Although isogeny-based cryptography made an effort to close this gap, it has serious security flaws.

7.7 Quantum Impact

Groups based on factoring (RSA's Z*n) and discrete logarithms (both finite field and elliptic curve) are no longer viable for long-term security due to the threat of quantum computing. This has accelerated the transition to groups and problems—mostly those based on lattices—that are not known to be amenable to Shor's technique.

VIII. FINAL THOUGHTS AND PROSPECTS

The ongoing arms race between cryptanalysis and the need for effective, secure communication is reflected in the development of cryptographic group structures. The discipline was founded by finite cyclic groups, which are now outdated against quantum threats and ineffective for classical security. Although elliptic curve groups share the fatal quantum weakness, they represent an ideal point in the classical world, providing an extraordinary blend of security, efficiency, and compactness.

More sophisticated algebraic structures are becoming more popular in the post-quantum age. As the most adaptable and promising foundation, lattice-based groups—formalized through problems such as LWE and RLWE—were standardized by NIST. In many applications, their primary disadvantage—larger key sizes—is a reasonable trade-off for quantum resistance.

While multivariate systems might be useful in some situations needing quick verification, other structures like isogeny-based groups offer intriguing compactness but call for more cryptanalytic assurance.

IX. FUTURE RESEARCH WILL FOCUS ON THREE AREAS

1) improving lattice-based cryptography implementations for practical applications;

2) delving deeper into the cryptanalysis of recently suggested structures; and

3) creating hybrid systems that combine PQC and ECC to guarantee security during the transition phase. The comparative analysis emphasizes that there isn't a "perfect" group for every situation; instead, the decision is still based on context-dependent optimization of threat models, performance needs, and security assumptions.

REFERENCES

[1] N. Koblitz (1987). cryptosystems with elliptic curves. Computational mathematics.

[2] O. Regev (2005). on lattices, cryptography, random linear codes, and learning with errors. STOC 2005.

[3] Lange, T., and D. J. Bernstein (2017). post-quantum cryptography. Nature.