Journal of Mathematical Problems, Equations and Statistics

**E-ISSN:** 2709-9407
**P-ISSN:** 2709-9393
Impact Factor (RJIF): 5.94
JMPES 2025; 6(2): 657-660

www.mathematicaljournal.com
Received: 04-07-2025
Accepted: 07-08-2025

**Rukmani Devi**
Research Scholar (Mathematics), Bhagwant University, Ajmer, Rajasthan, India

**Dr. Jyoti Gupta**
Research Guide, Bhagwant University, Ajmer, Rajasthan, India

**Dr. BK Chaturvedi**
Research Guide, Bhagwant University, Ajmer, Rajasthan, India

**Corresponding Author:**
**Rukmani Devi**
Research Scholar (Mathematics), Bhagwant University, Ajmer, Rajasthan, India

# Trends in algebraic structures and their applications in cryptography

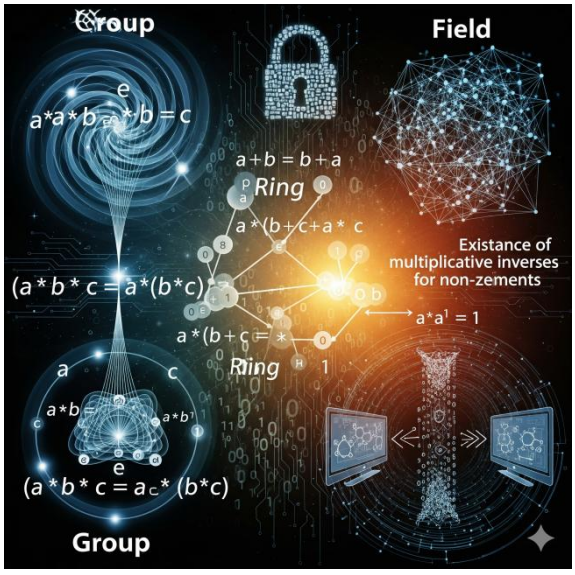
**Rukmani Devi, Jyoti Gupta and BK Chaturvedi**

**DOI:** https://www.doi.org/10.22271/math.2025.v6.i2d.255

**Abstract**
This research paper discusses the recent discoveries and the new trends in the use of algebraic structures in cryptography and how it has helped to enhance the security of digital information in the age of fast growing and changing technology. Encryption has historically been based on algebraic structures, including groups, rings, fields, lattices and so on, in which security communication over global networks is achieved. Modular arithmetic-based systems such as RSA, DiffieHellman, and ElGamal, information security revolutionaries, have become more vulnerable to attack under the rise of quantum computing. Equally, Elliptic Curve Cryptography (ECC) based on the difficulty of the Elliptic Curve Discrete Logarithm Problem, provides compact key sizes and efficiency, but is quantum-sensitive. The recent trends point to a paradigm shift to post-quantum cryptography. Lattice-based cryptography with the Learning With Errors (LWE) problem and its structures have become the top contenders to long-term security, and algorithms like CRYSTALS-Kyber and Dilithium are on the road to becoming international standards. Another potential post-quantum solution is isogeny-based cryptography, which is based on algebraic geometry and has compact key sizes, only requiring additional development to be resilient. Also, new innovations like homomorphic encryption and coding-theoretic methods broaden the usage of algebra in cloud and distributed systems by providing the ability to perform secure computations and data privacy. Based on a qualitative review of the recent literature and cryptographic standards, the paper can prove that algebraic structures are not only the theoretical foundation of cryptography but also are developing as the tools that cannot be dismissed to meet the new challenges. The results confirm that the multiplicity of algebra is the factor that guarantees its long-term relevance in protecting the digital communication against classical and quantum attacks.

**Keywords:** Algebraic structures, Cryptography, Modular arithmetic, Elliptic Curve Cryptography (ECC), Lattice-based cryptography, Post-quantum cryptography, Isogeny-based cryptography, Homomorphic encryption, Learning With Errors (LWE), Cybersecurity

## Introduction



Algebraic structures have traditionally been considered the foundation of modern mathematics: they are abstract structures, e.g. a group, a ring, a field, a lattice, which allow a systematic approach to solving problems in a variety of fields. Cryptography, the science of secure communication is one of the most important fields of application of algebra which has undergone profound and radical application. Cryptographic systems since the inception of digital communication use algebraic principles, which play a central role in guaranteeing confidentiality, integrity and authentication of information. Early encryption algorithms relied on basic modular arithmetic and number theory, although as large-scale computing became possible, more complex tools of algebra were needed.

Intersection The combination of algebra and cryptography has introduced potent systems which include the RSA algorithm whose construction relies on modular arithmetic and Elliptic Curve Cryptography (ECC) whose construction uses the structure of elliptic curve over finite field to achieve high levels of security with relatively small key sizes. The last few years have seen the fast development of technologies, and the imminent danger of quantum computing has redirected the cryptography research, requiring novel methods based on novel algebraic frameworks. New methods, like lattice-based cryptography, isogeny-based cryptography, and homomorphic encryption, demonstrate the role that algebra is playing in the development of strong, post-quantum cryptographic designs. This paper attempts to delve on such new developments and trends in algebraic structures in their applications in cryptography, and with particular attention to their qualitative value. The paper will focus on the development of algebra, and the needs of the field of cybersecurity by identifying the transition of classical systems to post-quantum models. Finally, this investigation illustrates that algebra is not an abstract concept, but a living and breathing framework of ensuring the safety of the digital world today and tomorrow.

**Objectives**

The main aim of the research study is to examine the current trends and advancements in algebraic structures and applications in cryptography with specific views on how they have been used to provide secure digital communication. The study aims to:

1. Examine the role of classical algebraic structures.
2. Analyze the significance of Elliptic Curve Cryptography (ECC).
3. Explore emerging post-quantum cryptographic methods.
4. Investigate other innovative algebraic approaches.
5. Provide a comparative understanding of classical and modern approaches.

**Background of Algebraic Structures**

Abstract algebra builds up around algebraic structures, which consist of sets, possibly endowed with one or more operations that are defined to satisfy certain axioms. These are structures, including groups, rings, fields, and lattices, that give a systematic structure to generalise and extend the arithmetic of numbers. The concept dates back to the 19th century when mathematicians, such as Évariste Galois and Carl Friedrich Gauss, formalized the group theory, whose work on symmetry and number theory has influenced the direction of modern mathematics. An example of this is how a group can be used to get the flavour of symmetry and invertibility, and rings and fields are used to generalise arithmetic operations, necessary to polynomial equations, codes, and cryptography.

Algebraic structures are important in the sense that they are universal. They do not only apply to pure mathematics but also to computer science, physics and engineering. Finite groups and finite fields are used in cryptography to create algorithms like RSA, the Diffie-Hellman algorithm and Elliptic Curve Cryptography. More recent developments in lattice theory and isogeny based systems are another indication of the way in which abstract algebra is adapting to modern challenges, especially the threat of quantum computing. Algebraic structures can therefore be considered as a theoretical framework and a practical tool which has continuously translated the abstract based reasoning to a problem solving in the real world.

**Importance of Algebra in Cryptography**

Cryptographic systems heavily depend on algebra to design and develop their cryptography systems and as such, data security is based on the mathematical underpinnings of algebra. Cryptography is the technique of designing protection for information against unauthorized access and algebraic constructs like groups, rings, and fields give the form of designing such protection. The RSA algorithm, one of the most popular algorithms, is an implementation of modular arithmetic and prime number theory based on properties of prime numbers and great depth in number theory and abstract algebra. Likewise, DiffieHellman key exchange and Elliptic Curve Cryptography (ECC) use group operations in finite field to create secure lines of communication.

The security of cryptographic systems is determined by the complexity of the computational problems in the algebraic number theory, including the factoring of large numbers, breaking discrete logarithms, or breaking lattice-based algorithms. The problems are analytically easy to specify but computationally impossible to solve efficiently so that they are perfect to use in encryption and security. The value of algebra has increased with the emergence of quantum computing, with some scientists considering post-quantum cryptographic algorithms, such as lattice-based and isogeny-based cryptography, also relying heavily on complex algebra.

**Research Methodology**

The research is the qualitative research and is based on the descriptive and analytical research approach, where the study investigates the recent progressions in the field of algebraic structures and their use in cryptography. The main purpose is to generalize tendencies, determine new trends and analyze their relevance to the future of safe communication. The data is gathered by means of secondary sources, such as peer-reviewed journal articles, books about abstract algebra and cryptography, as well as conference papers and technical reports of organizations, including the National Institute of Standards and Technology (NIST). Specific attention is paid to recent publications (20152024) in order to make sure that the results present the newest development, especially in the field of post-quantum cryptographics.

Their methodology is thematic analysis, according to which the information is classified into major fields of group theory, elliptic curves, lattice-based systems, and isogeny-based cryptography. The comparison against classical methods of encryption, which often rely on algebra (e.g. RSA, ECC), and new state-of-the-art post-quantum methods is conducted. With this approach, it becomes possible to gain a better insight into the way algebraic structures are modified to meet new challenges, such as quantum computational challenges.

Through a systematic qualitative system to the degree to which the study registers and elucidates developments, it suffers credibly to give useful information regarding

mathematicians, cryptographers, and policymakers with cybersecurity interests.

**Trends in Algebraic Structures and Cryptography**

***Group Theory and Number Theory***

Group theory and number theory provide the foundation for classical cryptosystems. The concept of modular arithmetic underlies RSA encryption:

$$C \equiv M^e \pmod{n}, \quad M \equiv C^d \pmod{n}$$

where $M$ is plaintext, $C$ is ciphertext, and $n = pq$ (product of two large primes). Its security rests on the difficulty of factoring $n$. Similarly, the Discrete Logarithm Problem (DLP) in cyclic groups supports protocols like Diffie-Hellman and ElGamal. If $g$ is a generator of a cyclic group $G$, given $g^a$ and $g^b$, it is computationally hard to find $g^{ab}$. These problems remain central to public-key cryptography.

**Elliptic Curve Cryptography (ECC)**

ECC is increasingly adopted due to high security with smaller keys. An elliptic curve over a finite field $F_p$ is defined as:

$$E: y^2 \equiv x^3 + ax + b \pmod{p}, \quad \Delta = 4a^3 + 27b^2 \neq 0$$

The group law allows point addition and scalar multiplication. For example, Elliptic Curve Diffie-Hellman (ECDH) computes a shared secret:

$$K = n_A(n_B P) = n_B(n_A P)$$

where $P$ is a base point, and $n_A, n_B$ are private keys. Recent trends include pairing-based cryptography, which enables identity-based encryption (IBE). Bilinear pairings $e: G_1 \times G_2 \to G_T$ allow new cryptographic primitives like short signatures and attribute-based encryption.

**Lattice-Based Cryptography**

Lattices are multi-dimensional grids defined as:

$$L = \left\{ \sum_{i=1}^{n} z_i \, b_i \mid z_i \in \mathbb{Z} \right\}$$

where $\{b_1, b_2, \ldots, b_n\}$ is a basis. The hardness of problems like Shortest Vector Problem (SVP) and Learning With Errors (LWE) provides security. For example, in LWE, given $(\mathrm{a}, b = \langle \mathrm{a}, \mathrm{s} \rangle + e)$, recovering secret s is computationally hard when error $e$ is added. NIST's post-quantum cryptography program has selected lattice-based algorithms such as CRYSTALS-Kyber (encryption) and Dilithium (digital signatures) for standardization.

**Isogeny-Based Cryptography**

Isogeny-based schemes rely on algebraic geometry, particularly isogenies morphisms between elliptic curves preserving group structures. The Supersingular Isogeny Diffie-Hellman (SIDH) protocol constructs shared secrets from isogenies between elliptic curves. Its security lies in the hardness of finding isogeny paths between given supersingular curves. While promising for compact key sizes, it remains under active research after recent cryptanalysis challenges.

**Other Emerging Algebraic Structures**

Homomorphic Encryption (HE) allows computation on encrypted data. In schemes like the Brakerski-Gentry-Vaikuntanathan (BGV) model, operations are performed using rings with error terms, based on Ring-Learning With Errors (RLWE). For example:

$$c_1 = Enc(m_1), \; c_2 = Enc(m_2), \quad Dec(c_1 + c_2) = m_1 + m_2$$

Coding theory also leverages algebraic structures such as polynomial rings and finite fields for error correction and cryptography. For instance, McEliece cryptosystem uses generator matrices of error-correcting codes, relying on the difficulty of decoding random linear codes.

These trends highlight a shift from classical number-theoretic methods like RSA to modern algebraic frameworks ECC for efficiency, lattices for quantum resistance, isogenies for compactness, and homomorphic encryption for secure computation. Algebra thus continues to be the dynamic engine driving cryptographic innovation.

**Discussion**

The comparative analysis of algebraic structures in cryptography highlights both their enduring significance and evolving challenges. Classical methods like RSA rely on modular arithmetic in number theory:

$$C \equiv M^e \pmod{n}, \quad M \equiv C^d \pmod{n}$$

where $n = pq$. While secure for decades, RSA's reliance on integer factorization makes it vulnerable to Shor's quantum algorithm, which can factor large $n$ efficiently, undermining its security.

Elliptic Curve Cryptography (ECC) introduced more compact security. Its security depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP): given $P$ and $Q = kP$, find $k$. This problem is computationally infeasible for classical computers, allowing ECC to provide strong encryption with smaller keys (e.g., 256-bit ECC ≈ 3072-bit RSA). However, like RSA, ECC would be broken by quantum algorithms.

To address this, lattice-based cryptography has emerged as a post-quantum solution. In the Learning With Errors (LWE) problem, one must solve equations of the form:

$$b = \langle \mathbf{a}, \mathbf{s} \rangle + e \pmod{q}$$

where it is difficult to recover s because of error term e. The issue is also high-level even with quantum computers and lattice-based schemes such as CRYSTALS-Kyber and Dilithium are good candidates to be standardized.

Algebraic geometry based cryptography Isogeny-based cryptography is also promising based on isogenies between elliptic curves, but more reinforcement is needed following recent attacks.

Accordingly, the discussion presents a shift: between number-theoretic systems susceptible to quantum-attacks to lattice and isogeny-based models that reincarnate the future of a secure communication.

**Conclusion**

The study of algebraic constructions in cryptography shows that it plays the pivotal role in ensuring digital communication and that the field is still developing. Modular arithmetic-based classical algorithms like RSA, DiffieHellman and ElGamal, form the backbone of the cryptography of the public key, but are susceptible to attacks during the quantum era. The Elliptic Curve Cryptography enhanced efficiency and security to the modern applications and is quantum-sensitive.

The most recent developments indicate a clear change towards post-quantum cryptography, where lattice-based methods provide high protection against the classical and quantum attacks. On the same note, isogenous based techniques and homomorphic encryption enhance the power of cryptography, responding to new requirements including secure computation and data privacy in the cloud.

Finally, the versatility of algebraic structures highlights their continued significance. Algebra is still used to determine the future of the cryptography field by connecting abstract theory with practical use to provide resistance to changing technological threats and keep information safe despite the digital age.

## References


1. Jyothi A, Lakshmi SM, Jyothi G. Applications of *algebraic structures* in modern cryptography: A comprehensive overview. Journal of Emerging Technologies and Innovative Research (JETIR). 2025;12(3):b201-b212. https://www.jetir.org/view?paper=JETIR2503122
2. Balamuralitharan S, Venmani R, Arulprakasam R, Murthy CSSN, Prabhakar MB, Ramana GV. *Algebraic structures* in cryptography: Applications and challenges. Communications on Applied Nonlinear Analysis. 2024;31(1):354-366. https://internationalpubls.com
3. Annu. *Algebraic structures* and their applications in modern cryptography. Shodh Sagar: Innovative Research Thoughts. 2024;10(3):52-60. https://doi.org/10.36676/irt.v10.i3.1433
4. Jara-Vera V, Sánchez-Ávila C. Some notes on a formal *algebraic structure* of cryptology. Mathematics. 2021;9(18):2183. https://doi.org/10.3390/math9182183
5. Katz J, Lindell Y. Introduction to modern cryptography. 3rd ed. CRC Press; 2020.
6. Agarwal S. Encryption and decryption using linear algebra: Advancement in public key cryptography. Indian Journal of Economics and Business. 2019;19(1):167-180.
7. Arora P. Use of group theory in cryptography. International Journal of Advance Research and Innovative Ideas in Education. 2016;2(6):1767-1772.
8. Agarwal S, Uniyal AS. Prime weighted graph in cryptographic system for secure communication. International Journal of Pure and Applied Mathematics. 2015;105(3):325-338.