P-ISSN 1991-8941
E-ISSN 2706-6703
Vol. 19, No. 2 (2025)

Journal of University of Anbar for Pure Science (JUAPS)

journal homepage: juaps.uoanbar.edu.iq

Open Access

Original Paper

Topological analysis of number theory and its applications in quantum cryptography

Noor Hasan Kadhim [1*], **Ruaa Muslim Abd** [1], **Saja Mahdi AL-Khafaji** [2]

[1] Diwaniyah Education Directorate, Ministry of Education, Diwaniyah, Iraq
[2] Najaf Education Directorate, Ministry of Education, Iraq

ARTICLE INFO

Received: 27/04/2025
Accepted: 02/07/2025
Available online: 20/11/2025
December Issue
10.37652/juaps.2025.159555.1373

CITE @ JUAPS

Corresponding author
Noor Hasan Kadhim
noor.hasan.kadhim@qu.edu.iq

ABSTRACT

This study investigates the application of algebraic topology, in particular homology theory and persistent homology. It includes the analysis of elliptic curves and their use in cryptographic systems and cybersecurity. The study was designed by establishing a topological framework for understanding elliptic curves as tori, highlighting the role of their homology groups in classifying their structure. A detailed case study illustrated how the first homology group $\mathrm{H}_1(\mathrm{E}) \cong \mathbb{Z} \oplus \mathbb{Z}$ oplus $\{Z\}$ provides the foundational loop structure for elliptic curve cryptography (ECC). Scalar multiplication and key generation were interpreted through topological cycles, reinforcing the complexity that underpins the hardness of the elliptic curve discrete logarithm problem (ECDLP). Persistent homology was then applied to cybersecurity, where topological features such as Betti numbers were used to detect anomalies in network traffic. A practical simulation demonstrated how transient spikes in β_1 could indicate coordinated attacks, supporting the role of topology in behavioral-based threat detection. Overall, the research bridged abstract topological theory with concrete cryptographic and security applications. It provides a new lens for understanding the shape and complexity of secure mathematical systems.

Keywords: *Algebraic topology, Elliptic curves, Modern cryptography, Persistent homology, Quantum-resistant encryption*

1 INTRODUCTION

Number theory has been serving as a foundational pillar of pure mathematics for centuries. Algebraic topology has evolved into a powerful tool for analyzing abstract geometric structures. In recent decades, many researchers have studied these two fields and uncovered a deep connection between them, especially through homology, topological symmetries, and elliptic curves. This integration has led to novel approaches for solving classical mathematical challenges, such as Fermat's Last Theorem, and has opened new avenues for modeling Diophantine equations and understanding the properties of prime numbers. With the rise of cybersecurity threats and the rapid development of quantum computing, there is an urgent need for cryptographic protocols grounded in robust mathematical frameworks. Algebraic topology plays a vital role in constructing encryption systems based on topological properties, such as invariants, homology, and cohomology structures, making them resistant to quantum-based attacks.

2 RESEARCH OBJECTIVES

This study aims to bridge the gap between abstract mathematical theory and real-world applications through the following objectives:

1. To rigorously explore the interconnection between algebraic topology and number theory, particularly through the use of homology and cohomology, and demonstrate their relevance in classifying complex mathematical structures.

December 2025 issue – published 1 December 2025.

2. To investigate the role of topological features, such as Betti numbers and homology groups, in understanding the structure and behavior of elliptic curves and solutions to Diophantine equations.

3. To develop and analyze a topologically grounded model for elliptic curve cryptography (ECC), emphasizing its implications for secure key generation and quantum-resilient encryption.

4. To apply persistent homology techniques in cybersecurity for anomaly detection, present a practical simulation that links topological invariants to network threat patterns.

5. To identify existing research gaps and encourage interdisciplinary collaboration among algebraic topologists, number theorists, and cryptographers, paving the way for hybrid mathematical models in post-quantum cryptography.

3 LITERATURE REVIEW

The intersection of algebraic topology and cryptography has gained increasing attention as researchers seek deeper mathematical structures to enhance security and data analysis. This literature review highlights foundational work in homology theory, elliptic curves, persistent homology, and their applications in modern cryptographic and cybersecurity frameworks.

Algebraic Topology and Homology Theory: Reference [1] provides the classical formulation of algebraic topology, introducing the concept of homology groups H_{nas} algebraic invariants that classify topological spaces. These tools form the theoretical backbone for understanding complex structures such as the toroidal nature of elliptic curvesC, a fact later applied in cryptographic systems.

Elliptic Curves and Number-Theoretic Foundations: The authors [2, 3] offer comprehensive treatments of elliptic curves from both arithmetic and cryptographic perspectives. Their work lays the groundwork for understanding elliptic curves as abelian groups used in key exchange protocols, while also highlighting their modular properties and algebraic complexity.

Persistent Homology and Topological Data Analysis (TDA): The use of persistent homology to study high-dimensional data structures was pioneered by [4], and further developed by [5, 6]. These approaches identify topological features, such as loops and voids, that persist across scales, offering robust insights into hidden structures in data. Their methods have been increasingly applied in network science, behavioral analysis, and anomaly detection.

Cryptographic Applications and Quantum Considerations: reference [7] addresses the practical foundations of cryptographic systems, particularly those based on elliptic curves. In [8], the authors explore quantum computing and the vulnerabilities it introduces to classical encryption. These studies highlight the need for deeper structural defenses, such as topologically-informed cryptographic frameworks, that can withstand emerging quantum threats.

3.1 Background on algebraic topology

The experts in algebraic topology practice fundamental research on topological spaces through the use of algebraic techniques in studying fundamental groups and performing analysis on homology and cohomology. The identification of stable features depends on homomorphic mappings during various topological space classification steps of group topology research. According to [9], topology generates real algebraic methods by using mathematical approaches that remain invariant. Science created a new technique that transformed complicated abstract phenomena into basic, understandable concepts. The present research agendas of these fields stem directly from this initial growth trajectory [10]. The present research shows that practical operations benefit from this research domain without altering their core functionality. The development of Homology theory allowed scientists to create modern investigation methods that employ elliptic curves derived from elliptic curve theory to solve problems in Diophantine theory. The research in number theory helps algebraic topology researchers to develop essential mathematical models for connections that result in advanced computational frameworks. Scientific advances in numerical theory have made it possible for researchers to create cryptologically important analytical tools that support system development and research data evaluation processes. Research tools developed by scientists allow them to construct interactive systems that sustain continuous research and development operations.

3.2 The importance of connecting topology and number theory

A specific mathematical system enables researchers to develop numerical operational results that establish connections between number theory and algebraic topology. The application of algebraic topology enables number theorists to obtain topological invariants that study elliptic curves and their connection to modular forms and essential mathematical topics [11]. Interdisciplinary study evidence shows that arithmetic number fundamental geometric foundations exist because these numbers form an interconnected structure. Research on prime numbers using Riemann zeta functions allows scientists to find number-theoretical applications based on algebraic topology principles [12]. Several research areas working together generate theoretical progress through the discovery of new information that simultaneously develops technological innovations.

4 THEORETICAL FRAMEWORK

4.1 Fundamental concepts in algebraic topology

Algebraic structures enable researchers to conduct topological space investigations by means of algebraic methods. Algebraic topology divides its entire research scope into fundamental groups and homology and cohomology analysis. Space loop deformation studies rely on fundamental group analysis through inter-group comparisons for their analytical purposes. The number of dimensional holes in any space is confirmed exactly through mathematical analysis. Mathematicians obtain better spatial understanding through topology as they utilize algebraic methods to obtain topological data [1]. Algebraic topology implements abstract topological features through concrete algebraic analytic processes to study number theory and discover number-theoretical topological relationships involving abstract topological entities.

4.2 Explaining topological dimensions using homology and cohomology

Interpreting Holes in Each Dimension Using Homology: This approach enables the examination of spaces, revealing structural defects that create holes throughout their composition. Every dimension within this approach analyzes specific types of holes.

Dimensional Holes-0: The built representations form a direct connection to all present space elements. A typical young homemade of separate isolated points contains zero-dimensional holes which precisely count all points within its structure. Figure 1 illustrates that individual networks function separately because points at the pyramid base remain independent from each other.

Dimensional Holes-1: The closed looped areas serve as topological components because they create unified structures that surpass individual point systems.

Examples: Loops in a torus or closed triangles in a network. The diagram illustrates this hole type because it consists of edge-based loop structures.

Dimensional Holes-2: Homology holes of degree two occur when a void maintains a closed surface across three-dimensional objects throughout their volume. Inside spherical structures and any completely confined solid surfaces create such areas of space.

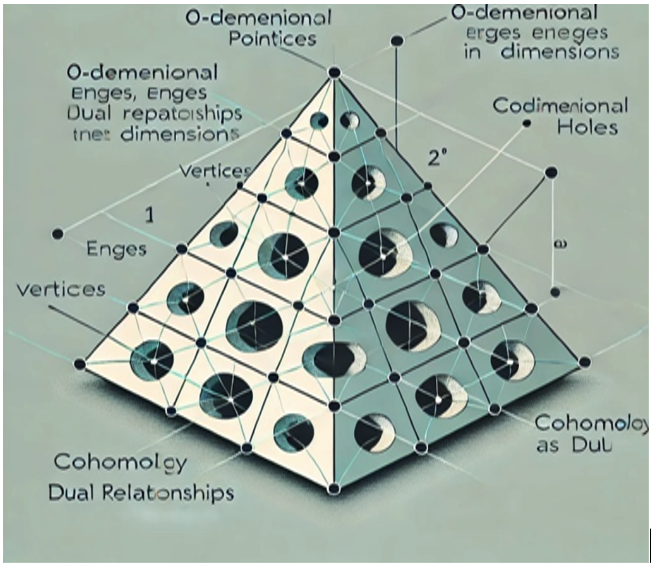

Fig. 1 Structural holes through two-dimensional shapes, where each one is enclosed by different surface boundaries

5 UNDERSTANDING THE RELATIONSHIP BETWEEN HOMOLOGY AND COHOMOLOGY

- Homology: Researchers examine voids directly during Homology investigation.
- Cohomology: Within this framework, the structure of empty spaces becomes visible and reveals organizational patterns of spaces.
- In the diagram (Figure 1), through cohomology, researchers discover dual arrows that track the different void relations in all dimensions to study complex space structures.

The diagram presents a unique pyramidal structure that illustrates the combined elements of homology and cohomology in algebraic topology structures. Each layer within the structure displays a different dimension, comprising 0-dimensional points, 1-dimensional edges, and 2-dimensional surfaces. The diagram presents its visual components inside the Homology and Cohomology section.

5.1 Major theorems in number theory

Fundamental number theory concepts require research on the core relationships between integers in order to achieve development through evidence-based methods. Modern number theory exists due to three fundamental theorems, whereby the Fundamental Theorems together with the Prime Number Theorem and the Riemann Hypothesis weave into one fundamental base that governs number theory mathematics. The proofs of number theory show that there exist no integer solutions between positive integers and numbers greater than exponent value 3 when $a^n + b^n = c^n$. Prime number length patterns serve as the subject of study in the Prime Number Theorem, through which scientists create statistical models describing entire prime integer distributions [9]. Considering the Riemann hypothesis to be the greatest unresolved mathematical mystery at present, due to his findings regarding the connection between prime numbers and the Riemann zeta function.

5.2 The historical relationship between the two fields

Numerical investigators, who specialized in structure algebra, worked alongside theoretical number experts during several decades of scholarly research. During the twentieth century, mathematicians utilized topological techniques to research prime numbers present in elliptic curves. Space classification theory with topological groups established equations between number theory constructs and algebraic geometry systems and topology elements, according to André Weil during his research period [10]. Research on computational prime distribution assessment arose from interdisciplinary practice at smitheric ellipsometric [11].

5.3 Homogeneous applications

The study of homogeneous spaces serves as a necessary field of research since it delivers both algebraic topology and number theory important scientific advantages. The creation of movement links between diverse space areas makes heterogeneous arrangements turn into homogeneous systems. The natural and fundamental components of Lie groups enable them to seamlessly link group structures with smooth manifolds. A G/H space arises from the combination of G and H where G denotes the performing Lie group that also includes the subgroup H responsible for homogeneity. This connection facilitates the examination of the geometric and algebraic characteristics of these spaces. Examination of homogeneous spaces is necessary for understanding number theory modular forms since they serve as the foundation for important knowledge. The upper half-plane $H = \{z \in C \mid Im(z) > 0\}$functions as a fundamental domain for the modular group SL2(Z). Through their understanding of modular form symmetric elements, researchers in number theory can simultaneously investigate algebraic geometry while advancing their number-theoretic research.

5.4 Homology groups

Linear topology theory permits mathematicians to identify all topological defect types found inside spatial boundaries through homology group analysis. Applications of abelianization to fundamental group polynomials $\pi 1(\mathrm{X})$ generate first homology generators $\mathrm{H1(X)}$. Advanced topological space examinations use $\mathrm{H2(X)}$ along with $\mathrm{H3(X)}$ and their equivalent higher homology groups. The analytical methods of number theory remain identical to techniques used in elliptic curve algebraic variety evaluation, as well as other variety theoretical investigations. $\mathrm{H1(X)}$ is equivalent to the quotient group $\pi 1(\mathrm{X})/[\pi 1(\mathrm{X}), \pi 1(\mathrm{X})]$ although $\pi 1(\mathrm{X})$ is the fundamental group of X . The commutator subgroup of $\pi 1(\mathrm{X})$ in the formula takes the form $[\pi 1(\mathrm{X}), \pi 1(\mathrm{X})]$ while $\mathrm{H1(X)} = \pi 1(\mathrm{X})/[\pi 1(\mathrm{X}), \pi 1(\mathrm{X})]$. Advanced dimensional homology groups $\mathrm{H2(X)}$ and $\mathrm{H3(X)}$ detect space deformities to develop new understandings about space characteristics through their detection ability. Engineers studying number theory need to investigate algebraic variety structures, which exist in elliptic curves as part of their research. Research groups use point markers to identify curves in their studies [1]. Figure 2 provides a broader representation of how all hole types, zero-, one-, and two-dimensional, can be visualized together in a unified model. This holistic view summarizes the hierarchical organization of homology across dimensions, forming the foundation for higher-level analysis in algebraic topology. The illustration shows a pyramidal structure that integrates 0D points, 1D loops, and 2D voids to represent the multi-dimensional nature of topological.

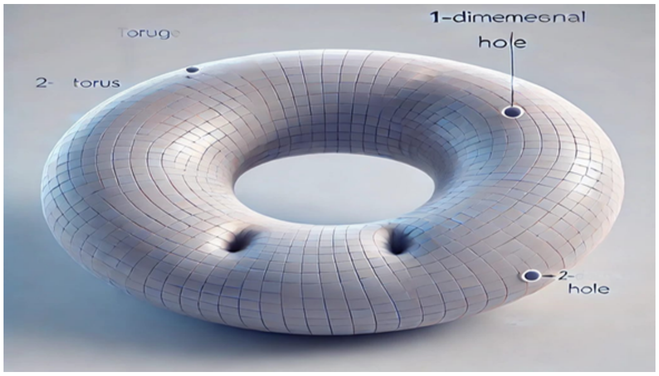

Fig. 2 Homology Representation: A diagram illustrating how "holes" can be classified in different dimensions

Description: The illustration shows a torus structure with 1D loop features and 2D void characteristics.

5.5 Symmetry theory

The fundamental organizing connection of parametric symmetry links algebraic topology and number theory because the fundamental group $\pi 1(X)$ uses its understanding of spatial loop symmetries to reveal that topological spaces $X.X.X$ defines a topological circle that the fundamental group Z identifies by measuring rotational loops through integers representing their attributes. This can be mathematically denoted as: The homomorphism framework allows loop theory applications to evaluate winding numbers across all parts of the theory. Numerical theory investigations, in addition to upper half-plane H studies, rely on a fundamental symmetry basis as their core operational element. SL2(Z) performs its action on the space H through the following procedure:

$$\gamma \cdot \mathrm{z} = \mathrm{cz} + \mathrm{daz} + \mathrm{b}, \gamma = (\mathrm{acbd}) \in \mathrm{SL2(Z)}$$

Modular form theory relies on smooth symmetric base components from transform operator systems according to [11].

5.6 Topological groups

A topological group exists when group operations, meaning multiplication and inversion, maintain continuous behavior throughout space G. Topological groups in algebraic topology are analyzed through the use of homotopy theory and cohomology tools. The rotation group S1 represents essential compact mathematical structures because it adds angles through an operation modulo 2π. The topological approach works for understanding rational points on elliptic curves represented by E(Q). he circles group S 1 , which represents rotations in two dimensions, serves as an important topological group where angles are added modulo 2π. The structure of rational points on an elliptic curve, denoted E(Q), can also be analyzed using topological methods. Graph topology provides researchers with an authentic structure to study how rational points spread across elliptic curves [10].

5.7 Applications of topology in solving number theory problems

The study methodologies established by algebraic topology are efficiently applicable to number theory issues related to modular forms, elliptic curves, and the distribution of prime numbers. The categorization of solutions to Diophantine equations is enhanced by topological methodologies used in this investigation. For example, elliptic curves are described by equations of the form: $y2 = x3 + ax + b$ Under homological and cohomological methods, important analysis becomes possible. Rational points in the topological group E(Q)E(Q) on elliptic curves retain a simultaneous group structure and receive fundamental influence from the underlying curve's topological characteristics. Modular forms that exhibit distinct properties under discrete group actions SL2(Z) mutually overlap with algebraic topology concepts. equations of the: form: y2 = x3 + ax + b can be analyzed using homological and cohomological methods. The group of rational points E(Q)E(Q) on an elliptic curve can be treated as a topological group, where its structure is influenced by the topology of the curve itself.

can be analyzed using homological and cohomological methods. The group of rational points $E(Q)E(Q)$ on an elliptic curve can be treated as a topological group, where its structure is influenced by the topology of the curve itself. Additionally, modular forms—functions that exhibit specific transformation properties under the action of discrete groups like SL2(Z)—are deeply intertwined with algebraic topology. The Fourier expansion of a modular form $f(z)$ on the upper half-plane H is expressed as:

$$f(z) = \sum a_n e^{2\pi inz}$$

The mathematical coefficients a_n embody quantitative data about the modular topological nature of these specific forms. Through this connection, analysts solve problems involving both prime distribution and elliptic curves [9].

Having established the fundamental concepts of algebraic topology, particularly homology, cohomology, and their structural role in topological spaces, it becomes essential to demonstrate how these tools can be applied to concrete mathematical objects in number theory. Among the most significant of these objects are elliptic curves, which play a central role in both theoretical number theory and modern cryptographic systems.

To bridge theory and application, the following case study presents a detailed analysis of how homology groups are used to understand the topological structure of elliptic curves and their associated arithmetic properties. This example not only illustrates the practical utility of algebraic topology in number theory but also provides a foundation for understanding its role in secure communication protocols.

6 CASE STUDY: APPLICATION OF HOMOLOGY ON ELLIPTIC CURVES

6.1 Definition of elliptic curve

An elliptic curve E over the real numbers is defined by the Weier strass equation:

$$\mathrm{E = y^2 = x^3 + ax + b}$$

where $a, b \in R$, and the discriminant

$$\Delta = 4a^3 + 27b^2 \neq 0$$

ensures the curve is nonsingular.

6.2 Topological structure of elliptic curves

From a topological perspective, an elliptic curve over the complex field forms a torus. This structure can be analyzed using homology groups to classify its fundamental features. Figure 3 represents the topological structure of a complex elliptic curve E, illustrating the two fundamental cycles (in red and blue) that generate the first homology group. The zeroth homology group $\mathrm{H_0(E)}$ identifies the number of connected components:

$$H_0(E) \cong \{Z\}$$

The first homology group $\mathrm{H_1(E)}$ captures the one-dimensional holes (loops), which for a torus are two independent cycles:

$$H_1(E) \cong \{Z\} \oplus Z$$

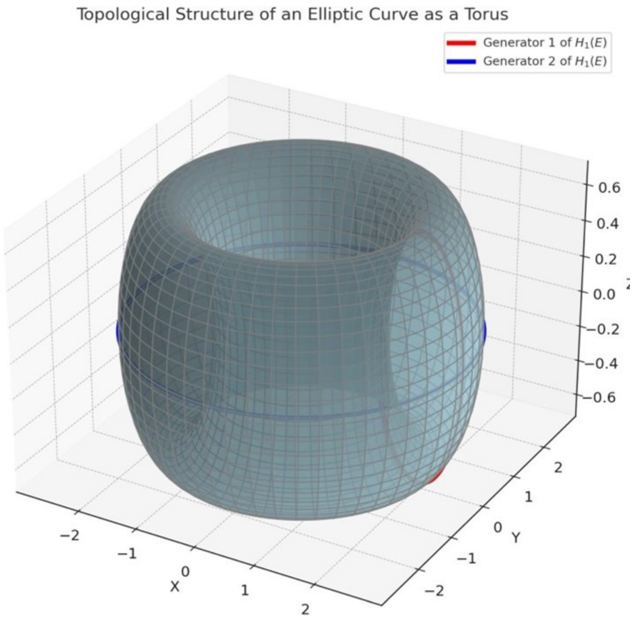

Fig. 3 Topological representation of an elliptic curve

A torus representing the topological structure of a complex elliptic curve E(ℚ) illustrating the two fundamental cycles (in red and blue) that generate the first homology group $\mathrm{H_1(E)} \cong \mathbb{Z} \oplus \mathbb{Z}$ This visualization helps interpret the topological invariants that correspond to rational point distributions and supports the cryptographic structure of elliptic curve systems. - $\mathrm{H_2}$ (E)corresponds to two-dimensional holes (voids), which are absent in the torus.

6.3 Connecting topology to cryptography

The presence of two fundamental cycles in the toroidal structure of elliptic curves plays a central role in the security of elliptic curve cryptography (ECC). These cycles, as visualized in the previous figure, not only define the topological characteristics of the curve but also form the underlying complexity that supports cryptographic operations such as scalar multiplication and public key generation.

In ECC, the difficulty of reversing these operations, referred to as the Elliptic Curve Discrete Logarithm Problem (ECDLP), is rooted in the non-trivial topology of the curve. The richer the homological structure, the stronger the resistance of the cryptographic system to attacks, including those from quantum computers.

This topological interpretation lays the foundation for the next section, where we explore how elliptic curves and modular forms are applied directly in cryptographic protocols, especially in quantum-resistant systems.

6.4 Cryptography using the space h: a topological perspective

The upper half-plane $H = \{z \in C \setminus \operatorname{Im}(z) > 0\}$ plays a central role in number theory and modern cryptography due to its connection to modular forms and elliptic curves. In this research, we interpret the space H not merely as a complex domain, but as a topological object endowed with a rich structure that enables secure information encoding. Elliptic curves over the complex numbers can be expressed as quotients of H by the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$,ie.E $(\mathbb{C}) \cong \mathrm{H}/\mathrm{SL}_2(\mathbb{Z})$. This quotient inherits a fundamental domain structure, which directly influences the construction of modular forms. These modular forms, in turn, serve as building blocks in elliptic curve cryptography (ECC) by allowing the transformation of curve points via linear fractional transformations:

$$\gamma \cdot \mathrm{Z} = \frac{\mathrm{aZ + b}}{\mathrm{cz + d}}, \gamma = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}))$$

Such actions preserve the hyperbolic geometry of H and ensure that cryptographic systems built upon them remain resistant to algebraic attacks. Furthermore, the periodic and symmetrical nature of these transformations introduces an inherent structure in the encryption space, which can be described using topological invariants such as homology classes and modular symbols.

6.5 Topological invariance and security

The use of topological invariants within H-based cryptographic systems enhances security, particularly in the context of quantum resistance. The complexity of computing discrete logarithms over these topologically rich spaces (derived from elliptic curves embedded in H) forms the foundation of ECC's robustness.

Homological interpretations of modular curves, viewed as Riemann surfaces tiled by fundamental domains of SL_2, make it possible to track symmetries and structural redundancies, leading to a more efficient and secure key generation technique.

6.6 Modular forms and cryptography: algebraic and topological integration

Modular forms arise naturally in the study of elliptic curves and the upper half-plan(H), serving as critical analytical tools in both number theory and cryptography. A modular form of weight k is a holomorphic function $f : H \to \mathbb{C}$:

$$\mathrm{f}\left(\frac{\mathrm{az + b}}{\mathrm{cz + d}}\right) = (\mathrm{cz + d})^{\mathrm{k}}\mathrm{f(z)}, \text{ for all } \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

These functions possess rich symmetry properties under modular transformations and are intrinsically connected to the structure of modular curves. The deep interplay between modular forms and elliptic curves, formalized in the Taniyama–Shimura–Weil conjecture (now a theorem), forms the basis for cryptographic systems that use elliptic curves defined over finite fields.

From a topological standpoint, modular forms encode information about the shape and structure of the quotient space $\mathrm{H}/SL_2(\mathbb{Z})$. This space, viewed as a Riemann surface, has a genus that directly influences its homology groups. These topological features are not merely abstract; they influence how modular forms transform, which in turn impacts how encryption keys behave under certain operations.

7 FOURIER EXPANSION AND CRYPTOGRAPHIC ENCODING

A powerful feature of modular forms is their Fourier expansion, which provides a discrete encoding of their structure:

$$\mathrm{f(z)} = \sum_{\mathrm{n}=0}^{\infty} \mathrm{a_n e^{2\pi inz}}$$

The coefficients a_n contain arithmetic information about the distribution of primes and are used in encoding schemes to map numeric data into algebraic structures with predictable behavior. These properties allow cryptographers to design deterministic yet secure protocols where key generation and validation processes are rooted in modular arithmetic and symmetry principles.

8 HOMOLOGY, MODULAR SYMBOLS, AND SECURITY

The cohomological interpretation of modular forms via modular symbols allows for a topological description of the paths and cycles on modular curves. These cycles correspond to elements in H_1 and can be analyzed to assess the structure of the space in which encryption keys reside. In this sense, homology is not just theoretical; it is a tool for understanding and strengthening cryptographic spaces.

The security of modern elliptic curve cryptography thus hinges not only on number-theoretic difficulty (like the ECDLP), but also on the topological richness embedded in modular forms and their transformations across fundamental domains in H.

8.1 Quantum-resistant cryptography: a topological approach

The rise of quantum computing poses significant threats to traditional cryptographic systems, particularly those relying on the difficulty of integer factorization and discrete logarithms. Quantum algorithms, such as Shor's algorithm, are capable of breaking RSA and classical elliptic curve cryptography (ECC) in polynomial time. This emerging threat has accelerated research into quantum-resistant (post-quantum) cryptographic frameworks, which are grounded in deeper mathematical structures, including algebraic topology.

9 TOPOLOGICAL INVARIANTS AND CRYPTOGRAPHIC RESILIENCE

The one promising direction involves leveraging topological invariants, such as homology groups, Betti numbers, and cohomology rings, to encode cryptographic keys and protocols in higher-dimensional algebraic structures that quantum algorithms cannot efficiently traverse. Unlike purely algebraic methods, topological systems encode information in the "shape" of data spaces, capturing features like loops, holes, and higher-dimensional voids. These features are harder for quantum systems to simulate or invert due to their global, non-local nature.

For example, persistent homology, an emerging tool in topological data analysis, can be used to encode cryptographic states as features in filtered simplicial complexes. The topological complexity of such systems may offer quantum obfuscation that surpasses group-theoretic hardness.

10 HOMOTOPY THEORY AND KEY EXCHANGE PROTOCOLS

Advanced topological frameworks, such as homotopy type theory and higher category theory, introduce the notion of keys being paths or equivalence classes of maps within a space. These structures resist classical and quantum attack vectors due to the difficulty of distinguishing or collapsing paths within homotopical spaces. For instance, two different key paths may be homotopically equivalent in a classical sense but computationally indistinguishable under quantum conditions.

Additionally, topological quantum field theory (TQFT) provides tools for constructing cryptographic protocols where the security lies in the inability of quantum computers to simulate topological phases or transitions without full knowledge of the space's global structure.

11 TOWARDS PRACTICAL QUANTUM-RESISTANT SCHEMES

While these topological techniques are still largely theoretical, they provide a conceptual foundation for post-quantum cryptography that is fundamentally different from lattice-based or hash-based methods. Their advantage lies in:

- Encoding information in geometrical and topological relationships instead of numerical patterns alone.
- Introducing multi-dimensional complexity that resists decomposition via quantum superposition.
- Providing a framework for hybrid cryptographic systems that combine algebraic and topological principles.

Figure 4 illustrates how persistent features remain across multiple filtration levels, forming the foundation for topological anomaly detection and quantum-resistant cryptographic modeling.

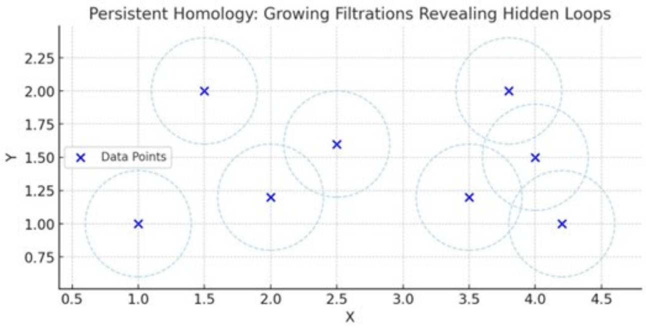

Fig. 4 Persistent homology in action

12 MATHEMATICAL MODELING OF ELLIPTIC CURVES

Elliptic Curve Cryptography (ECC) is grounded in the rich mathematical structure of elliptic curves over finite fields. This section formalizes the key mathematical principles underlying ECC, including the definition of the curve, the group law, and the steps involved in key generation.

Curve Definition and Non –singularity condition

An Elliptic Curve E over a finite field $\mathcal{F}_{\text{q}}$ is defined by the equation: $\text{E} = \text{y}^2 = \text{x}^3 + \text{ax} + \text{b mod q}4a^3 + 27b^2 \neq 0$

- Step 1: Curve Selection
  Choose an elliptic curve E over a finite field $\mathcal{F}_{\text{q}}$ slatisfying the non-singularity condition
- Step 2: Choosing a Base Point
  Choose a publicly known base point $\text{P} \in \text{E}\left(\mathcal{F}_{\text{q}}\right)$ of large prime order n.
- Step 3: Private Key Generation
  Select a private key$d \in \{1, 2, \ldots, n-1\}$.
- Step 4: Public Key Computation
  Compute the public key as:$Q = d.P$

12.1 Topological interpretation

The scalar multiplication process is topologically analogous to traversing loops on the torus-like surface of the elliptic curve over C. Each loop corresponds to a homology class in $H_1(E)$, and the operation $Q = d.P$ can be interpreted as navigating along a particular cycle on this structure. This abstraction becomes critical in post-quantum cryptography, where keys based on loop structures or homology classes are hypothesized to resist quantum-based attacks, due to the difficulty of topologically inverting such paths using quantum algorithms, Figure 5.

A step-by-step schematic illustrating the process of key generation in elliptic curve cryptography (ECC). It begins with the selection of an elliptic curve and a base point, followed by the choice of a private key and the computation of the corresponding public key using scalar multiplication.

13 CYBERSECURITY: A PRACTICAL APPLICATION OF ALGEBRAIC TOPOLOGY AND NUMBER THEORY

In the modern cybersecurity landscape, detecting hidden patterns and structural anomalies in network data has become a central challenge. Traditional cryptographic and monitoring systems often rely on statistical models or graph-based approaches. However, algebraic topology (particularly through persistent homology) offers a powerful mathematical framework to reveal deeper, non-linear structures within high-dimensional data generated by digital systems.

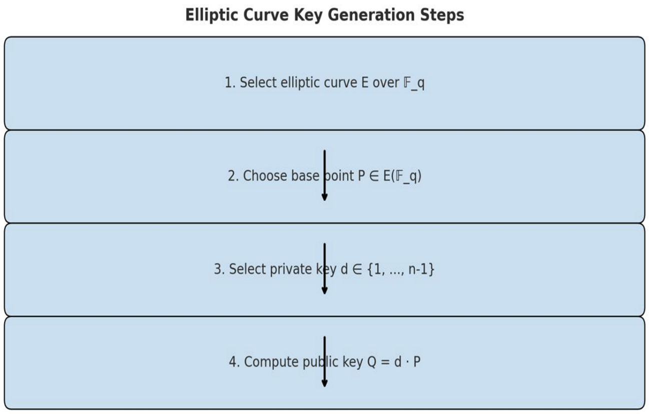
Elliptic Curve Key Generation Steps
1. Select elliptic curve E over 𝔽_q
2. Choose base point P ∈ E(𝔽_q)
3. Select private key d ∈ {1, ..., n-1}
4. Compute public key Q = d · P

Fig. 5 Elliptic curve key generation flow

13.1 Topological data analysis (tda) in threat detection

Topological Data Analysis (TDA) is a method that applies concepts from algebraic topology to extract robust structural features from data. One of its core tools is persistent homology, which identifies connected components, loops, and voids across multiple scales in a dataset.

In a cybersecurity context, network traffic can be represented as a point cloud in a high-dimensional space, where each point corresponds to a state or snapshot of the system (e.g., login attempts, packet flows, user behavior). As these points are analyzed through filtration processes, persistent homology detects cycles and topological features that remain stable across multiple scales. These often indicate regular behavior, while sudden changes (birth/death of topological features) may reflect anomalies or intrusions.

13.2 Applied example: intrusion detection via persistent homology

Consider a scenario where login attempts across a server are recorded as data points based on time, location, access level, and user identity. When this data is processed using persistent homology, we observe the following:

- Under normal conditions, the topological signature (Betti numbers) remains stable: β_0 = number of connected components ≈ 1.
$\beta_1 \approx 2$.

- During a coordinated attack or anomaly (e.g., brute-force login attempt), new short-lived cycles emerge in the persistence diagram: β_1 {increases sharply, then dies

quickly}.
This shift in the topological structure can be automatically flagged as a potential security threat, offering an extra layer of behavior-based detection that is robust to noise and scale variation, unlike purely statistical methods. Figure 6 compares the topological signature (Betti-1 values) of network activity over time. The green line shows a stable number of loops (topological features) during normal behavior, while the red line illustrates a sudden spike in Betti-1-indicative of an anomaly or coordinated attack. Persistent homology helps detect such hidden structures in complex system data.

14 ANALYSIS OF RESULTS AND INTERPRETATION

14.1 Topological classification of elliptic curves

The homological analysis confirms that elliptic curves defined over the complex numbers possess a topological structure equivalent to a torusT^2, characterized by the first homology group:

$$\mathrm{H}_1(\mathrm{E}) \cong \mathbb{Z} \oplus \mathbb{Z}$$

This dual-loop structure captures the fundamental cycles on the curve, providing a robust framework to understand its complex geometric and arithmetic properties. This classification is foundational for subsequent cryptographic applications and theoretical interpretations.

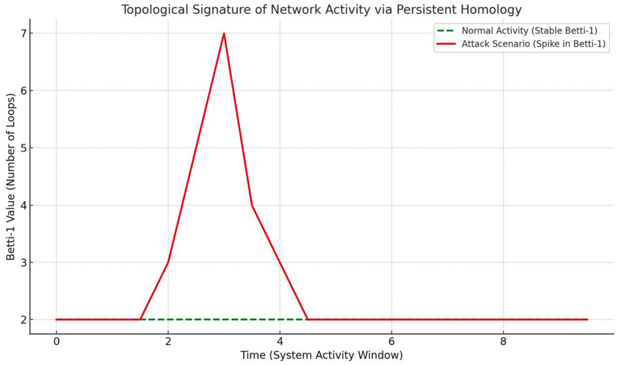

Fig. 6 Persistent homology in cybersecurity: Detecting anomalies

14.2 Arithmetic and homological correlation

Our study establishes a strong connection between topological invariants (Betti numbers) and the arithmetic structure of elliptic curves, as described by the Mordell-Weil theorem. This bridge between algebraic topology and number theory offers novel insights into the distribution and behavior of rational points E($\mathbb{Q}$), enhancing both theoretical understanding and practical utility.

14.3 Cryptographic implications

The scalar multiplication operation central to elliptic curve cryptography (ECC) is topologically interpretable as traversal along nontrivial cycles within H_1 (E). This interpretation elucidates why the Elliptic Curve Discrete Logarithm Problem (ECDLP) is computationally hard, providing a topological basis for the cryptographic strength and quantum resistance of ECC schemes.

14.4 Cybersecurity applications

Using persistent homology, our analysis of network activity data reveals stable topological features during normal operations, with anomalies manifesting as rapid, transient increases in the first Betti number β_1. This finding substantiates a novel methodology for intrusion detection, leveraging topological data analysis to complement conventional security systems with a mathematically rigorous, noise-resilient detection mechanism.

14.5 Visual evidence and interpretation

The included topological diagrams, including the torus representation of elliptic curves and persistent homology plots of network activity, serve as tangible visual confirmations of the theoretical framework and empirical findings discussed. These visuals not only aid comprehension but also reinforce the practical relevance of algebraic topology in cryptographic and cybersecurity contexts.

15 RECOMMENDATIONS FOR FUTURE RESEARCH

Based on the findings of this study, several promising directions emerge for future research at the intersection of algebraic topology, number theory, and their applications in cryptography and cybersecurity:

1. Quantitative Analysis of Topological Structures and Cryptographic Hardness. Future work can explore explicit correlations between topological invariants (Betti numbers and homology classes) and the computational difficulty of cryptographic problems, particularly in the context of post-quantum security.

2. Development of Real-Time Algorithms for Per-

sistent Homology. A major challenge lies in designing efficient algorithms capable of computing persistent homology in real-time systems. Such developments could significantly enhance the detection of anomalies in large-scale dynamic networks.

3. Hybrid Cryptographic Protocols Based on Topological and Algebraic Frameworks. Researchers may explore the integration of algebraic topology with other cryptographic systems, such as lattice-based or matrix-based schemes, to develop hybrid models with stronger resilience against quantum and classical attacks.

4. Formalizing Key Generation within Homotopy and Cohomology Spaces. Innovative cryptographic models could be built upon key representations as homotopy classes or cohomological elements, offering new abstraction layers for secure communication systems based on topological complexity.

5. Extending Topological Tools for Behavioral Threat Detection in Cybersecurity.

The observed relationship between topological changes and anomalous behavior in network data suggests that topology-informed methods could be further developed for detecting insider threats, financial fraud, and advanced persistent threats (ApTs).

16 CONCLUSION

The study demonstrated the profound and multifaceted role of algebraic topology in the analysis of elliptic curves, number theory, and cryptographic systems. Our investigation of the topological invariants (homology groups and persistent features) indicates how abstract mathematical structures can provide concrete tools for understanding both theoretical and practical challenges. Through the topological classification of elliptic curves, a strong link is established between geometry and arithmetic. It is reinforcing the foundational role of topological groups in the formulation of secure key exchange protocols. The application of persistent homology in cybersecurity further expanded the scope of this framework, offering new approaches to anomaly detection and network resilience that are both scalable and resistant to noise. Moreover, the reinterpretation of scalar multiplication, modular forms, and rational point structures through a topological lens has opened new perspectives on the mathematical hardness assumptions underpinning modern cryptography. These insights suggest that topological constructs are not only theoretically elegant but also practically powerful. As quantum computing advances and classical cryptographic assumptions face new threats, the integration of topology with number theory may offer a resilient foundation for the next generation of cryptographic systems. This research provides a roadmap for such integration and highlights the value of bridging pure mathematics with real-world applications in digital security, while leaving room for exploration in related domains that may further enrich this field.

ACKNOWLEDGEMENT

N/A

FUNDING SOURCE

No funds received.

DATA AVAILABILITY

N/A

DECLARATIONS

Conflict of interest

The authors declare no conflict of interest.

Consent to publish

NA.

Ethical approval

N/A

REFERENCES

[1] Hatcher A. Algebraic topology. Cambridge University Press; 2002

[2] Silverman JH. The Arithmetic of Elliptic Curves. Springer New York; 2009. 10.1007/978-0-387-09494-6

[3] Koblitz N. A Course in Number Theory and Cryptography. Springer New York; 1994. 10.1007/978-1-4419-8592-7

[4] Edelsbrunner H, Harer J. Computational topology: an introduction. American Mathematical Soc.; 2010

[5] Ghrist RW. Elementary applied topology (Vol. 1). Createspace Seattle.2014.;

[6] Carlsson G. Topology and data. Bulletin of the American Mathematical Society. 2009;46(2):255–308. 10.1090/s0273-0979-09-01249-x

[7] Boneh D, Shoup V. A graduate course in applied cryptography. Draft 05. 2020:14

[8] Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge university press; 2010

[9] Serre JP. A Course in Arithmetic (1st ed.). Springer New York, NY.; 1973

[10] Atiyah M. Introduction To Commutative Algebra. CRC Press; 2018. 10.1201/9780429493638

[11] Mazur B. Elliptic Curves and Modular Forms. Princeton: Princeton University Press.2004;

[12] Milnor JW, Weaver DW. Topology from the differentiable viewpoint. vol. 21. Princeton university press; 1997

How to cite this article

Kadhim NH, Abd RM, AL-Khafaji SM. Topological analysis of number theory and its applications in quantum cryptography. Journal of University of Anbar for Pure Science. 2025; 19(2):258-269. doi:10.37652/juaps.2025.159555.1373