International Conference on Engineering, Applied Science And Technology

Systematic Analysis of Mathematical Fundamentals in Elliptic Curve Cryptography: Concepts, Applications, and Challenges

Miftah Sigit Rahmawati[1*], **Ierasath Bin Yousuf**[2]
[1]*Universitas Muhammadiyah Sorong, Sorong 58416 , Indonesia*
[2]*An-Nikmah Al-Islamiyah Institute, Malaysia*

ARTICLE INFO

JASAT use only:
Received date :
Revised date :
Accepted date :

Keywords:
Elliptic Curve
Cryptography
Encryption
Algebra

ABSTRACT

This study aims to systematically analyze the mathematical fundamentals underpinning Elliptic Curve Cryptography (ECC) by reviewing its key concepts, applications, and challenges. Utilizing literature from Springer, Sagepub, and Mendeley databases, several essential mathematical concepts, such as the basic operations in ECC, including addition and multiplication. This article categorizes previous research into three main areas: (1) ECC concepts covering discussions on elliptic curves, cryptology, and pre-cryptological operations, (2) ECC applications in various encryption methods and models, such as the ECC encryption model, ECDSA, and ECDH, and (3) challenges in ECC implementation as a computational model. The results show that while the foundational algebraic theories supporting ECC have been developed, further research is required to enhance the effectiveness and efficiency of ECC in the future. This study serves as a groundwork for more in-depth research on algebraic structures in the formation of ECC.

Introduction

Cryptography plays a crucial role in securing digital communications, safeguarding sensitive information from unauthorized access and ensuring data integrity. As the digital landscape evolves, so do the methods employed to protect data. Among these methods, Elliptic Curve Cryptography (ECC) has emerged as a powerful tool due to its ability to provide robust encryption with relatively small key sizes. This efficiency is particularly important in an era where computational resources are often limited, such as in mobile devices and Internet of Things (IoT) applications. ECC's strength lies in its mathematical foundation, which leverages the properties of elliptic curves over finite fields, making it a preferred choice in various sectors, including finance, telecommunications, and cybersecurity [1]. The growing reliance on ECC is evidenced by its adoption in widely used security protocols, including Transport Layer Security (TLS) and Secure Socket Layer (SSL), which underpin secure communications on the internet. The National Institute of Standards and Technology (NIST) has also recognized ECC as a viable alternative to traditional public key cryptosystems like RSA, particularly for securing transactions and communications in environments where performance and resource efficiency are paramount [2]. As digital threats continue to evolve, the need for advanced cryptographic methods becomes increasingly critical, positioning ECC at the forefront of modern cryptography.

The purpose of this article is to systematically analyze the mathematical foundations of ECC by reviewing existing literature. This analysis aims to categorize previous research on ECC's algebraic structures, its applications in encryption methods, and the challenges encountered in its implementation. By doing so, the article seeks to provide a comprehensive understanding of how ECC operates within the broader context of cryptography and to highlight areas where further research and development could enhance its effectiveness. Specifically, the article will explore the algebraic principles as [3], [4] that form the basis of ECC, including the group law associated with elliptic curves and how these principles contribute to the security and efficiency of cryptographic operations. Finally, the article will address the current challenges faced in ECC implementation, including computational

[*] Corresponding author.
E-mail address: miftahsigit.rahmawati@gmail.com

complexity and security vulnerabilities, which are critical for ensuring its continued relevance in an evolving digital landscape.

Conducting a literature review is essential for gaining a comprehensive understanding of how ECC has evolved over time and how its mathematical foundations contribute to its performance. By analyzing studies that explore the algebraic principles underlying elliptic curves, this review will help identify key areas where ECC’s mathematical foundation has enhanced its efficiency in encryption processes. For instance, research has shown that ECC can provide equivalent security to RSA with significantly smaller key sizes, which is a crucial advantage in resource-constrained environments [5]. Furthermore, the literature review allows us to pinpoint areas where ECC's performance can be further improved through refined algebraic models. Understanding these foundational elements not only contributes to the theoretical framework of ECC but also informs practical implementations that could lead to advancements in security, scalability, and applicability across a broader range of technological solutions. By synthesizing existing research, this article aims to illuminate the intricate relationship between ECC's mathematical principles and its practical applications, thereby setting the stage for future innovations in the field.

Methods

1. Data Sources.

To ensure a thorough and credible analysis, sources were selected from reputable academic databases such as Springer, Sagepub, and Mendeley. These platforms were chosen for their extensive collections of peer-reviewed journals and publications that cover a wide range of topics in cryptography and mathematics. The credibility of these journals is paramount, as they often feature cutting-edge research and contributions from leading experts in the field. For instance, Springer hosts numerous journals dedicated to applied mathematics and cryptography, providing access to high-quality studies that can enhance our understanding of ECC [6]. The selection of these databases also facilitates access to interdisciplinary studies that may incorporate insights from fields such as computer science, information security, and algebraic geometry. This multidisciplinary approach is essential for comprehensively analyzing the mathematical foundations of ECC, as it allows for the integration of various perspectives and methodologies. Consequently, the choice of data sources reflects a commitment to rigor and depth in the literature review process.

2. Selection Criteria

The literature included in this review was selected based on specific inclusion criteria to ensure relevance and quality. Key terms such as "elliptic curve cryptography," "elliptic curve," and "algebra structure of cryptology" were utilized to guide the search process. Additionally, a time frame for publication was established, focusing on studies published between 2015 and 2024. This period was chosen to capture the most recent advancements and trends in ECC research, reflecting the rapid evolution of the field. The filtering process involved conducting keyword searches across the selected databases, followed by a review of abstracts and full texts to assess the relevance of each study. Articles that provided significant insights into the mathematical foundations, applications, or challenges of ECC were prioritized. This systematic approach to selection ensures a comprehensive and focused literature review that accurately represents the current state of research in ECC.

3. Categorization Process

Once the relevant articles were identified, they were categorized into three main areas: ECC concepts, applications, and challenges. This framework serves to guide the analysis and ensure a systematic approach to the literature review. Under the first category, ECC concepts, the focus will be on the mathematical principles and algebraic structures that underpin elliptic curves, exploring their implications for cryptographic security. The second category, applications, will delve into how ECC is utilized in various encryption methods, highlighting specific algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie-Hellman (ECDH) protocol. Finally, the challenges category will address the computational and security-related issues that practitioners face when implementing ECC in real-world scenarios. By organizing the literature in this manner, the review aims to provide a clear and coherent analysis of ECC's mathematical fundamentals and their practical implications.

Results and Discussions

The literature reviewed provides key insights into the mathematical fundamentals and practical applications of ECC. It systematically addresses the foundational concepts, the core cryptographic operations, and the challenges associated with ECC implementations.

Table 1. Concepts in Elliptic Curve Cryptography

Reff	**Elliptic curve**	**Cryptology**	**Pre-cryptological operations**
[7]		Classic	Algebraic binary relations
[8]	ECSM (elliptic curve scalar multiplication)	ECC	Point addition (PA) and point doubling (PD) methods
[9]	Elliptic curves are defined over finite fields	ECC	Point addition and the construction of cyclic subgroups from elliptic curves
[10]	Elliptic curves over finite rings		Elliptic curves and their properties
[11]	Construction and selection of pairing-friendly elliptic curves	Cryptographic systems	
[12]	Group of points on the elliptic curve of Montgomery's shape	ECC	Algebraic operations related to groups and fields
[13]	Overview of elliptic curves over prime fields	El Gamal	Encoding and decoding algorithms
[5]	ECC as an asymmetric scheme based on elliptic curves	ECC	
[1]	Fundamental theory of elliptic curves	ECC	Point addition, scalar multiplication, and point doubling
[14]	The application of elliptic curves in cryptography	ECC	How complete addition formulas can optimize these processes for better performance
[15]	Relation to mathematical properties		Mathematical formulation
[16]	The implementation of a new mapping technique	ECC	Scalar multiplication, point addition, and point doubling
[17]	Weierstrass equation	ECC	Scalar multiplication, point addition, and point doubling
[18]	Tangen of Elliptic curve		
[19]	Highlights the non-linear nature and large group order of elliptic curves	Elliptic curves Max-Plus algebra-based wavelet transforms	Encoding and diffusion

The conceptual framework of elliptic curve cryptography has evolved significantly since its inception, with key historical developments shaping the field. The mathematical theory of elliptic curves dates back to the 19th century, when mathematicians like Niels Henrik Abel and Carl Friedrich Gauss explored their properties. However, it was not until the late 20th century that elliptic curves found their application in cryptography. In 1985, Neal Koblitz and Victor Miller independently proposed the use of elliptic curves for public-key cryptography, marking a pivotal moment in the field [20], [21]. This standardisation was crucial in legitimising ECC for use in government and commercial applications [22]. As research continued, various advancements in ECC algorithms and implementations emerged. In particular, the introduction of efficient scalar multiplication techniques, such as the double-and-add algorithm and the Montgomery ladder, significantly improved the performance of ECC operations. These developments were instrumental in demonstrating ECC's viability for resource-constrained environments, such as mobile devices and embedded systems [11].

Several papers [7], [8] discuss the mathematical structure of elliptic curves and their role in cryptography. The focus is placed on essential operations such as elliptic curve scalar multiplication (ECSM) and point addition/doubling, which are crucial for establishing secure cryptographic systems. These operations leverage the algebraic properties of elliptic curves defined over finite fields or rings, as emphasized in the work by Sanjeewa et al. The exploration of algebraic structures, including binary relations and cyclic groups, provides a robust theoretical foundation for ECC.

A. Elliptic Curve and Algebraic Structures

Elliptic curves arise from the study of cubic equations in two variables, typically expressed in the Weierstrass form

$$y^2 = x^3 + ax + b \qquad (1)$$

where a and b are coefficients that satisfy the condition

$$4a^3 + 27b^2 \neq 0 \qquad (2)$$

to ensure no singular points exist on the curve. These curves possess a rich algebraic structure, forming a group under a well-defined addition operation. The group law, which allows for the addition of two points on the curve to yield a third point, is foundational to elliptic curve cryptography (ECC). This operation is geometrically realised by drawing a line through two points on the curve, finding the intersection with the curve, and reflecting that point across the x-axis [7]. The algebraic properties of elliptic curves confer significant advantages for cryptographic applications. One notable feature is the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is the basis for the security of ECC. This contrasts sharply with traditional systems like RSA, where the security relies on the difficulty of factoring large integers. Research shows that ECC can achieve comparable levels of security with significantly smaller key sizes; for example, a 256-bit key in ECC provides a security level equivalent to a 3072-bit RSA key [1]. Moreover, the efficiency of ECC is further enhanced by its algebraic structure, which permits faster computations. Various algorithms, such as the double-and-add method and the Montgomery ladder, exploit these properties to perform scalar multiplication operations efficiently. These optimisations are crucial in resource-constrained environments, such as mobile devices and embedded systems, where processing power and memory are limited [8]. The lightweight architecture developed for elliptic curve scalar multiplication over prime fields exemplifies this efficiency, enabling rapid computations without compromising security.

B. Cryptology and Pre-cryptological Operations.

Cryptology, the science of secure communication, encompasses two main branches: cryptography, which focuses on the creation of secure communication systems, and cryptanalysis, which deals with breaking these systems. Within this broader field, elliptic curve cryptography (ECC) serves as a powerful tool for ensuring data integrity and confidentiality. ECC operates on the principles of algebraic structures and finite fields, allowing for the secure exchange of information through public-key cryptographic methods [11]. A significant portion of the literature delves into pre-cryptological operations, such as point addition and point doubling, which are vital for constructing cryptographic protocols. These operations, highlighted in the works of [8], [11], [23], form the basis of secure key generation and encryption methods within ECC. The studies identify how these mathematical operations underpin the cryptographic strength of ECC and ensure the generation of secure and reliable encryption keys. Before any encryption takes place, several pre-cryptological operations must be executed. Key generation is one of the most critical processes, involving the creation of a public-private key pair.

Scalar Multiplication

Scalar multiplication on an elliptic curve is a key operation in classical asymmetric cryptography (Benjamin smith). This operation is the basis of modern cryptographic operations, especially ECC. Take the point P on the elliptic curve and multiply it by the scalar number k. Then, the new point Q which is the result of multiplying the point P for k times as $Q = P + P + \cdots + P$ (k times)

$$Q = kP \qquad (3)$$

If $k = 3$ then, $Q = 3P$ etc.

The Elliptic Curve Discrete Logarithm Problem (ECDLP) as the problem of determining scalar k, given P and Q is a source of ECC security.

Scalar multiplication (3) directly depends on operations over points on the elliptic curve. In general, traditional methods to compute the scalar multiplication rely on the execution of a given sequence of point doubling $(2P)$ and point addition $(P + Q)$ operations, where P and Q are points on the elliptic curve. Formulae to compute the pre-cryptological operations are derived according to what is known as group law.

Group Law

The points on an elliptic curve form a group structure, these basic group operations form the basis of ECC . Elementary point operations are typically described geometrically to best understand how point formulae are derived. The following description is based on the natural representation of points using x and y coordinates, which is called affine coordinate representation in the context of ECC.

a. Point Addition

Point addition is one of the basic operations that allows determining the result of two points P and Q on an elliptic curve. If a straight line is drawn through two points P and Q, it will intersect the elliptic curve at one additional point R.

Supposed $P = (x_1,y_1)$ dan $P = (x_2,y_2)$ with $P \neq Q$ then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \ mod\ P \qquad (4)$$

λ as gradient trough P and Q

From (2) so that $R = (x_3,y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \quad mod\ P$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \quad mod\ P$$

b. Point Doubling

Point doubling is the process of calculating the result of adding the point P to the elliptical curve by itself $(2P)$. Geometrically, this involves tangent at point P and finding an intersection with a curve.

$$\lambda = \frac{3{x_1}^2 + a}{2y_1} \qquad (5)$$

From (5), so that $R = (x_3,y_3)$ where

$$x_3 = \lambda^2 - 2x_1 \quad mod\ P$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \quad mod\ P$$

Establishing cryptographic protocols is another essential pre-cryptological operation. Protocols such as the Elliptic Curve Diffie-Hellman (ECDH) allow two parties to securely share a secret over an insecure channel. In the ECDH protocol, both parties generate their public-private key pairs and exchange their public keys. Each party then computes the shared secret independently using their private key and the other party's public key. This process ensures that the shared secret remains confidential, even if an adversary intercepts the public keys [5]. The integration of ECC into broader cryptographic frameworks also necessitates the development of secure hashing algorithms. Hash functions, which convert input data into fixed-size output, play a vital role in ensuring data integrity and authenticity. When combined with ECC, these hash functions can enhance the security of digital signatures, providing non-repudiation and authenticity in electronic transactions [2]. For instance, the Elliptic Curve Digital Signature Algorithm (ECDSA) employs a combination of ECC and secure hash functions to produce digital signatures that are both compact and secure. The pre-cryptological operations in ECC, including key generation and protocol establishment, are fundamental to the secure exchange of information. The interplay between these operations and the underlying mathematics of elliptic curves highlights the sophistication of ECC as a modern cryptographic solution. In conclusion, the mathematical foundation of elliptic curves, characterised by their group law and algebraic properties, plays a pivotal role in the effectiveness of ECC. The combination of strong security assurances with efficient computational methods positions ECC as a leading choice in contemporary cryptographic practices.

Table 2. Application of ECC

Ref	Categorization	Encryption
[7]	Clarifications on Ciphers	Symmetric and asymmetric encryption, and block and stream ciphers.
[8]	The importance of ECSM in ECC	
[9]	Public key systems	ECDSA (Elliptic Curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman)
[13]		ElGamal encryption
[5]		ECC encryption
[1]	Secure key exchange and digital signatures	
[14]		ECC encryption
[16]		ECC encryption and

		description
[17]		ECC encryption and description
[18]	Geometry	
[19]		A novel encryption algorithm

ECC has found widespread application in public key encryption systems, such as Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH), as described in the literature by [10]. The lightweight nature of ECC, which offers high security with relatively small key sizes, makes it suitable for constrained environments like IoT devices and mobile communications. ECC has emerged as a pivotal method for securing digital communications, primarily due to its unique mathematical properties that facilitate robust encryption processes. ECC employs elliptic curves defined over finite fields, allowing for the creation of secure public-key cryptographic systems. Among the most significant applications of ECC are ECDSA and ECDH protocols. ECDSA is widely used for digital signatures, providing authenticity and integrity for messages, while ECDH enables two parties to establish a shared secret over an insecure channel, thus facilitating secure communication [11]. For instance, the use of ECC in contactless payment systems allows for quick and secure transactions. This efficiency not only enhances user experience but also strengthens security against potential attacks, thus fostering greater consumer trust in digital payment methods. In the realm of IoT, where devices often have limited processing power and battery life, ECC provides an optimal solution for secure communication. The lightweight nature of ECC algorithms enables secure data transmission between devices without overwhelming their resources. This also illustrates how ECC is implemented in smart home devices, allowing for secure control and monitoring via mobile applications. This highlights the versatility of ECC in enabling secure interactions in an increasingly interconnected world.

When comparing ECC with traditional cryptographic methods such as RSA, the advantages of ECC become apparent. RSA relies on the difficulty of factoring large prime numbers, which necessitates larger key sizes to maintain security. For instance, a 2048-bit RSA key is generally considered secure, whereas a mere 256-bit ECC key offers equivalent security, as demonstrated by [1]. This disparity in key size translates to significant computational efficiency; ECC operations require fewer resources in terms of processing power and memory, making it particularly advantageous for devices with constrained capabilities, such as mobile phones and Internet of Things (IoT) devices. Moreover, the mathematical foundation of ECC allows for faster computations, particularly in scalar multiplication, which is the core operation in ECC-based algorithms. Research by [8] highlights lightweight architectures designed for efficient elliptic curve scalar multiplication, demonstrating that these methods can perform operations significantly quicker than their RSA counterparts. This efficiency is crucial in real-time applications where speed is essential, such as in secure financial transactions or real-time data encryption. The application of ECC is not limited to secure communications; it also extends to various encryption models that enhance security across different platforms. This showing how elliptic curve methods are applied in encryption schemes, ensuring data protection in resource-limited devices. For instance, ECDSA is widely adopted in blockchain technologies, ensuring the integrity of transactions in cryptocurrencies like Bitcoin. The integration of ECC into these platforms exemplifies its versatility and robustness in modern cryptographic applications, as noted by [2]. As the demand for security increases in digital transactions, the adoption of ECC is expected to rise, further solidifying its role in contemporary cryptography.

the systematic analysis of encryption methods and models within ECC illustrates its superiority over traditional cryptographic systems. The combination of smaller key sizes, enhanced computational efficiency, and broad applicability positions ECC as a cornerstone of modern cryptographic practices. As digital security continues to evolve, ECC will likely play an increasingly prominent role in safeguarding sensitive information across various domains. The practical implementation of ECC has been transformative across several sectors, particularly in enhancing the security of financial transactions, data protection in smart cards, and secure communication in IoT devices. One notable example is the use of ECC in securing online banking transactions. Financial institutions leverage ECC to authenticate users and encrypt sensitive data, ensuring that transactions remain confidential and tamper-proof. A study by [2] indicates that the adoption of ECC in banking has reduced fraud rates significantly, demonstrating the effectiveness of this cryptographic approach in real-world scenarios. Smart cards, which are ubiquitous in various applications such as payment systems and identification, also benefit from ECC. These cards often operate under stringent resource constraints, making ECC's smaller key sizes and lower computational requirements particularly advantageous. Case studies further illustrate the effectiveness of ECC in enhancing security. For example, in a recent implementation within a smart grid system, ECC was employed to secure communication between grid management systems and consumer devices. The results indicated a marked improvement in the resilience of the system against cyber threats, as reported by [13]. Such case studies underscore the practical benefits of ECC, showcasing its ability to protect sensitive data in various real-world applications.

Table 3. Challenges of ECC

Reff	Computation	Implementation
[7]		Encryption modalities used in digital communications.
[8]	Computational efficiency	Cryptographic attack
[9]		An awareness of potential challenges in implementation
[10]		Security against various attacks (linear, differential, and statistical)
[11]	New TNFS attacks that affect the security of elliptic curves with composite embedding degrees	
[1]	Computational efficiency, potential cryptographic attacks	Difficulties in hardware or software implementation
[14]	Computational efficiency, potential cryptographic attacks	Difficulties in hardware or software implementation
[16]	Faster process	
[17]		Implementation and performance of ECC in the context of chat applications
[18]		The understanding of geometric properties of ellipses and the behavior of tangents from external points.
[19]	Computational Complexity	

Computational Challenges

One of the primary challenges in implementing Elliptic Curve Cryptography (ECC) lies in computational complexity, particularly with elliptic curve scalar multiplication (ECSM). Although ECC offers reduced key sizes compared to RSA, the scalar multiplication operation remains computationally expensive as it involves a series of point additions and doublings. This challenge becomes more critical in environments with limited processing power, such as smart devices and IoT platforms [11]. To enhance computational efficiency, the choice of the algebraic structure of elliptic curves is critical. Different forms, such as Weierstrass, Montgomery, and Edwards curves, offer unique properties that impact the speed of cryptographic operations. Montgomery curves, for example, allow for faster scalar multiplication due to their coordinate system, making them advantageous for high-speed applications [16]. The choice between prime fields and binary fields also plays a crucial role. Prime fields provide more efficient point operations for software implementations, while binary fields are often preferred for hardware implementations due to their simpler arithmetic [7]. Algorithmic improvements, such as precomputed tables for point addition and doubling, can reduce the number of operations required [17].

Challenges in Implementation

Addressing the challenges in ECC's computation and implementation is crucial to improving its performance and security. Ongoing research into optimization techniques for scalar multiplication, hardware acceleration, and lightweight algorithms will play a key role in ensuring ECC's efficiency in real-world applications. The adoption of post-quantum cryptography will also ensure resilience against future threats. With its smaller key sizes, enhanced computational efficiency, and ability to operate in resource-constrained environments, ECC remains a leading choice for secure digital communications [2], [11]. Continued efforts to enhance ECC's security and efficiency will cement its role in financial transactions, IoT communications, and other critical applications in the evolving digital landscape.

Although significant progress has been made in understanding the algebraic structures that underpin ECC, further optimization is necessary. The reviewed studies suggest that refining these structures could lead to more efficient implementations of ECC, particularly in resource-constrained environments. For instance, the mathematical efficiency of ECSM and other elliptic curve operations must be improved to reduce computational overhead without compromising security.

While ECC provides strong protection against current cryptographic attacks, new threats, especially from quantum computing, require enhanced defense mechanisms. The literature suggests that ECC needs to evolve to address these future challenges, making it essential for future research to focus on developing quantum-resistant variants of ECC. The bar chart below visually represents the findings from a comprehensive literature study on the mathematical fundamentals of elliptic curve cryptography, organized into five key categories. Each category reflects the frequency with which it is addressed in existing research, highlighting the areas of focus and significance within the field.

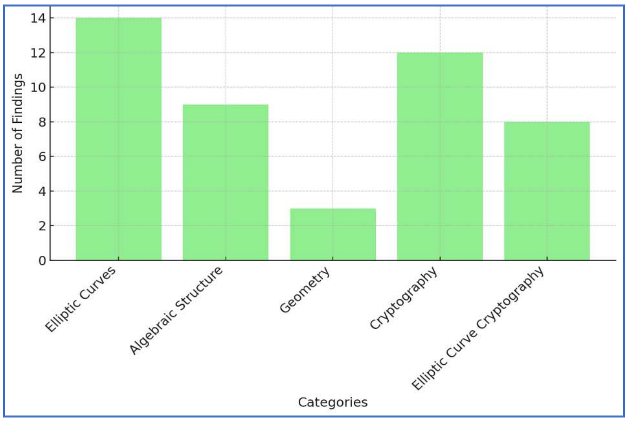

Figure 1. Findings Field

The systematic literature study reveals a strong emphasis on elliptic curves, which holds the highest number of references (14). This suggests that the foundational mathematics behind elliptic curves remains a primary focus of research in this field. It is likely that further advancements will continue to explore the intricate properties of elliptic curves. Following this, cryptography is another area receiving significant attention with 12 references. This indicates that practical applications of elliptic curves in securing data, particularly in cryptographic algorithms, are a key area of development. As more industries adopt cryptographic methods like ECC, this may see further research in improving security and efficiency. The presence of algebraic structure with 9 references highlights ongoing interest in the underlying mathematical structures supporting elliptic curves, emphasizing the theoretical side of the topic. Interestingly, elliptic curve cryptography appears as a new, focused category with 8 references, showing how specialized the application of elliptic curves has become within cryptography. This may point to future research in optimizing ECC protocols for specific use cases like blockchain and secure communications. Finally, geometry shows fewer references (3), but its inclusion suggests that the geometric interpretation of elliptic curves, while less explored, is still relevant for certain niche applications.

Conclusions

This article makes a significant contribution to the field of Elliptic Curve Cryptography (ECC) by providing a systematic analysis of its mathematical fundamentals. The review has highlighted the importance of pre-cryptological operations, which form the foundation for secure key generation and encryption methods. Through a comprehensive literature review, we have identified key algebraic structures such as law group with elliptic curve scalar multiplication (ECSM) and point addition that play a crucial role in the cryptographic strength of ECC. By categorizing previous research into concepts, applications, and challenges, this study has offered valuable insights into how algebraic theories can be leveraged to enhance the effectiveness and efficiency of ECC, particularly in resource-constrained environments. However, despite the progress made, there is a clear need for further research into the algebraic foundations of ECC. Optimizing the mathematical operations that underpin ECC is essential for improving its computational efficiency, especially in environments with limited processing power. Additionally, research must continue to address emerging security threats, such as those posed by quantum computing, which could potentially undermine the robustness of current ECC implementations. By advancing the algebraic theories supporting ECC, researchers can further strengthen its encryption model, ensuring that it remains a viable solution for securing communications in the future. Looking ahead, future research should focus not only on theoretical developments but also on practical implementations of ECC. As the demand for secure and efficient cryptographic methods continues to grow, particularly in industries like finance, IoT, and mobile communications, it is critical that ECC evolves to meet these challenges. Developing quantum-resistant variants of ECC, refining its algebraic models, and improving computational efficiency are key areas where further exploration is needed. By addressing these challenges, ECC can maintain its position as a leading cryptographic method in an increasingly digital world.

Conflicts of Interest

The authors declare no conflict of interest

References

[1] M. R. Khan *et al.*, “Analysis of Elliptic Curve Cryptography & RSA,” *J. ICT Stand.*, vol. 11, no. 4, pp. 355–378, 2023. doi: 10.13052/jicts2245-800X.1142.

[2] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, “Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey,” *Comput. Sci. Rev.*, vol. 47, p. 100530, 2023. doi: 10.1016/j.cosrev.2022.100530.

[3] R. Soekarta and M. Sigit, “Implementation of Affine Group Algebra on Digital Image Security,” vol. 1, no. 1, pp. 137–146, 2020. doi: 10.12928/mf.v1i1.XXX

[4] M. S. Rahmawati and R. Soekarta, “Penerapan aljabar linear pada transformasi Wavelet Diskrit dalam program aplikasi keamanan citra digital,” 2019. doi: 10.21831/pspmm.v1i0.15

[5] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, “Cryptography: A Comparative Analysis for Modern Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 442–448, 2017. doi: 10.14569/ijacsa.2017.080659.

[6] K. L. Tan, A. K. S. Sim, S. S. N. Yap, S. Vithayaporn, and A. W. Rachmawati, “A systematic review of meaningful work unifying 20 years of theoretical and substantive contributions (2000–2020),” *J. Adv. Manag. Res.*, vol. 20, no. 3, pp. 462–512, 2023. doi: 10.1108/JAMR-11-2022-0225.

[7] V. Jara-Vera and C. Sánchez-ávila, “Some notes on a formal algebraic structure of cryptology,” *Mathematics*, vol. 9, no. 18, 2021, doi: 10.3390/math9182183.

[8] Y. Hao *et al.*, “Lightweight Architecture for Elliptic Curve Scalar Multiplication over Prime Field,” *Electron.*, vol. 11, no. 14, pp. 1–24, 2022. doi: 10.3390/electronics11142234.

[9] R. Sanjeewa and B. A. K. Welihinda, “Elliptic Curve Cryptography and Coding Theory,” *Int. J. Multidiscip. Stud.*, vol. 3, no. 2, p. 99, 2017. doi: 10.4038/ijms.v3i2.12.

[10] U. Hayat, I. Ullah, N. A. Azam, and S. Azhar, “A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings,” *Entropy*, vol. 24, no. 5, pp. 1–24, 2022. doi: 10.3390/e24050571.

[11] G. Favre *et al.*, “Elliptic Curve Cryptography and Coding Theory,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11, no. 1, pp. 1–24, 2022. doi: 10.4038/ijms.v3i2.12.

[12] Y. B. W. Tama and M. F. Fahmi, “Sistem Kriptografi Klasik Dengan Memanfaatkan Orde Dari Grup Titik Pada Kurva Eliptik Bentuk Montgomery,” *Euler J. Ilm. Mat. Sains dan Teknol.*, vol. 11, no. 2, pp. 361–371, 2023. doi: 10.37905/euler.v11i2.23009.

[13] D. Krenn *et al.*, “Definition and Implementation of an Elliptic Curve Cryptosystem using a New Message Mapping Scheme,” *Semigr. Forum*, vol. 104, no. August 2021, pp. 58–71, 2020. doi: 10.1145/3386723.3387893.

[14] J. Renes, C. Costello, and L. Batina, “Complete addition formulas for prime order elliptic curves,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9665, pp. 403–428, 2016. doi: 10.1007/978-3-662-49890-3_16.

[15] D. J. Unger, “Yield criteria representable by elliptic curves and Weierstrass form,” *Procedia Struct. Integr.*, vol. 35, no. C, pp. 2–9, 2021. doi: 10.1016/j.prostr.2021.12.041.

[16] K. Keerthi and B. Surendiran, “Elliptic curve cryptography for secured text encryption,” *Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2017*, no. March, 2017. doi: 10.1109/ICCPCT.2017.8074210.

[17] D. Natanael, Faisal, and D. Suryani, “Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC),” *Procedia Comput. Sci.*, vol. 135, pp. 283–291, 2018. doi: 10.1016/j.procs.2018.08.176.

[18] A. Pakapongpun and S. Srisuk, “On the Problem of Tangency of Ellipse Curve,” *Asian J. Appl. Sci.*, vol. 6, no. 6, pp. 542–546, 2018. doi: 10.24203/ajas.v6i6.5534.

[19] K. A. Sattar, T. Haider, U. Hayat, and M. D. Bustamante, “An Efficient and Secure

Cryptographic Algorithm Using Elliptic Curves and Max-Plus Algebra-Based Wavelet Transform," *Appl. Sci.*, vol. 13, no. 14, 2023.
doi: 10.3390/app13148385.

[20] B. N. Koblitz, "Elliptic Curve Cryptosystems," vol. 4, no. 177, pp. 203–209, 1987.

[21] V. S. Miller, "Elliptic Curves and their use in Cryptography," *Communications*, pp. 1–14, 1997.
doi: 10.2307/2007884

[22] N. Sendrier, *Code-Based Cryptography Post-Quantum Cryptography*, no. February 2009. 2014.
doi: 10.20944/preprints202104.0734.v1

[23] R. Sanjeewa and B. A. K. Welihinda, "Elliptic Curve Cryptography and Coding Theory," *Int. J. Multidiscip. Stud.*, vol. 3, no. 2, p. 99, 2017.
doi: 10.4038/ijms.v3i2.12.