

Cryptography with Elliptic Curves: Enhancing Security through Advanced Mathematical Techniques

Dr. G. Archana Alias Gurulakshmi*

*Assistant Professor, Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Email Id: drarchanag@veltech.edu.in, Scopus Id : 57822786800
Orcid Id: 0009-0002-7623-1334

Abstract

Elliptic curve cryptography (ECC) has now gained widespread acceptance as an encryption protocol of choice in the public-key cryptographic model since it can provide better security with considerably smaller key sizes and comparatively lower computation cost than most of the standard algorithms. This review discusses the mathematical ideas applied to the elliptic curves and how the elliptic curve discrete logarithm problem has been employed to offer a guarantee of cryptographic security. Key exchange, authentication and secure data transmission functions of major ECC algorithms, such as ECDH, ECDSA, ECIES and EdDSA, are discussed. More efficient methods of ECC performance and resilience, including efficient scalar multiplication, intelligent key generation schemes, pairing-based cryptography, and isogeny-based schemes, are also discussed. The review further evaluates common security threats affecting ECC implementations, including side-channel attacks, protocol-level vulnerabilities, hardware-related risks, and emerging quantum-computing challenges. Practical applications of ECC across secure communication protocols, blockchain systems, Internet of Things environments, and cloud platforms demonstrate its adaptability in modern digital infrastructures. Despite the fact that some implementation complexities and future quantum risks are still quite significant issues, ECC still provides a good balance between efficiency and security. The results underscore the current significance of the elliptic curve-based methods in modern cryptographic systems and their applicability to the creation of next-generation secure communication systems.

Keywords: elliptic curve cryptography, elliptic curve discrete logarithm problem, public-key cryptography, cryptographic security, post-quantum cryptography

How to cite this article: Gurulakshmi GA. Cryptography with Elliptic Curves: Enhancing Security through Advanced Mathematical Techniques. *Int J Drug Deliv Technol.* 2026;16(10s): 365-374; DOI: 10.25258/ijddt.16.10s.48.

1. Introduction

Cryptography is another indispensable aspect of the current information protection that enables it to protect sensitive data that is transmitted via digital networks. Since internet services, cloud computing, and mobile technologies have been increasing at a very high rate, the security of data exchange has become even more significant. Cryptographic systems assist in maintaining the confidentiality, integrity, authentication and non-repudiation by transforming readable data into unreadable data to ensure that the wrong entry or manipulation of the data during transit will not occur (Qadir and Varol, 2019). The introduction of cryptography systems that aided in the development of modern cryptography played a significant role in the evolution of cryptography. The asymmetric cryptography, which was pioneered by Diffie and Hellman, provides the concept of the key elements that enable two parties to share a common secret without exchanging keys across a sensitive communication line. This invention formed the basis of numerous secure communication standards applied in modern systems of digital infrastructure (Diffie and Hellman, 2022). As time goes by, a collection of cryptographic systems has been developed to address various security requirements in the computing environment. These are asymmetric cryptography, hybrid encryption and symmetric cryptography. Symmetric methods are usually used in regard to efficient encryption of information, but

asymmetric systems facilitate in disturbed dispensing of keys and authentication. Hybrid systems offer the benefits of both methods to enhance the general performance and security (Jain, 2021).

Complex mathematical principles and assumptions of computational hardness play a great role in determining the effectiveness of cryptographic systems. Other cryptographic algorithms are based on hard mathematical problems, like integer factorization and discrete logarithmic problems, which cannot be efficiently solved without secret parameters by classical computing machines (Pachghare, 2019). Nevertheless, these new technologies, like quantum computing, have cast doubt on the long-term security of some classical cryptographic methods, prompting efforts to develop more resistant security models (Portmann and Renner, 2022). Researchers have thus delved into the enhancement of the conventional cryptographic protocols, especially in key exchange protocols. Multi-cryptographic algorithm-based hybrid methods have been suggested to improve the security of communications and minimize the susceptibility in the contemporary network atmosphere (Hassan et al., 2025). In the same way, the upgrades to classical key exchange algorithms have also been created by integrating complementary cryptographic methods to enhance tools against adversarial attacks (Gupta and Subba Reddy, 2022). Elliptic curve cryptography (ECC) is among the most effective and secure modern systems of

*Author for Correspondence: drarchanag@veltech.edu.in

cryptography (including public-key cryptography). ECC depends upon the mathematical geometry of elliptic curves over finite fields and the intractability of the discrete logarithm problem of elliptic curves. ECC has similar security levels to the traditional algorithms, but with much smaller key sizes, which enhances the computational efficiency (Hankerson and Menezes, 2025a). Its general use in applications such as cloud computing, mobile security, and Internet of Things (IoT) systems, where strong encryption must be achievable with few computational resources, has been enabled by this performance (Deevi et al., 2023).

The analysis of the mathematics, algorithms and advanced techniques of the cryptography of elliptic curves is reviewed to enable an analysis of its contribution to improving the existing cryptographic security systems.

2. Review Methodology

A thorough review procedure was used to analyze the application of elliptic curve cryptography in contemporary security systems. The selection of the relevant literature was determined based on recent journal articles, conference papers, books, surveys, and dissertations of ECC foundations, algorithms, security concerns, applications, and developments in post-quantum. The found papers were filtered based on their direct relevance to the topic of the review, and summarized into the main themes, including mathematical background, cryptographic algorithms, optimization tools, attack models, practical implications, and research directions. The information from these sources was collected and merged to propose a clear and organized image of ECC. In this way, the review was able to integrate both theories and practice advancements and emphasize the changing role of ECC in safe online communication.

3. Mathematical Foundations of Elliptic Curves

The cryptography system based on elliptic curves is called elliptic curve cryptography (ECC). These mathematical entities form the foundation of the design of secure cryptography algorithms that are based on computationally challenging problems. Overall, the elliptic curve over a finite field can be defined by the Weierstrass equation:

$$y^2 = x^3 + ax + b,$$

The parameters that meet certain requirements to make the curve have no singularities. The elements of the curve, along with a predetermined point at infinity, create an algebraic group that permits well-defined arithmetical operations necessary to use cryptography applications (Yan, 2022). The elliptic curve group form allows performing such basic ECC-based operations as point addition and point doubling. These operations provide the possibility to generate new points on the

curve by means of algebraic manipulation of the old ones, as the foundation of scalar multiplication. Scalar multiplication, the repetition of adding a point to itself, is a key to the elliptic curve cryptography schemes, especially in the key generation processes and the encryption processes. The effectiveness and safety of ECC are highly reliant on the mathematical characteristics of these group tasks that are defined on the finite fields (Obukhov et al., 2024).

An important security feature of ECC is the elliptic curve discrete logarithm problem (ECDLP). Given two points on an elliptic curve,

P and $Q = kP$, computationally infeasibility to compute which integer k will give this relationship is possible in sufficiently large parameter sizes. This is the hardness assumption that is founded on the basis of ECC security, as well as ensures that the private keys are not easily obtained in accordance with the corresponding public keys through the classical computation methods. This is the main complication in the resolution of the ECDLP, which is therefore the main issue of security of elliptic curve-based cryptographic systems (Hankerson and Menezes, 2025b). Space Computational mathematics and quantum computing Studies have also explored how to solve discrete logarithm problems on elliptic and similar algebraic curves. There have been postulations of quantum algorithms that solve discrete logarithm problems more efficiently than classical algorithms. Based on these trends, it is evident that one can understand the mathematical complexity of the cryptographic systems of elliptic curves and determine how well they are tolerant to the new generation of computational models (Huang et al., 2020). Besides their direct use in cryptography, elliptic curves are rich mathematical objects whose study has been extensively used in number theory and also in the study of algebraic geometry. Mathematical subsystems associated with the distribution, classification, and interaction of elliptic curves have complicated mathematical processes and have led to current research in both theoretical mathematics and applied cryptography. These studies give a better understanding of the structural characteristics of elliptic curves and contribute to creating more viable cryptographic methods based on superior approaches to mathematics (He et al., 2025).

The combination of the mathematical concepts is the basis on which elliptic curve cryptography is made. Using the algebraic characteristics of elliptic curves and the computational hardness of the elliptic curve discrete logarithm problem, ECC offers a mathematically rigorous and efficient architecture of the cryptographic systems in the present day. Figure 1 provides a summary of the mathematical background of ECC, starting with the structure of elliptic curves and the difficulty of the ECDLP.

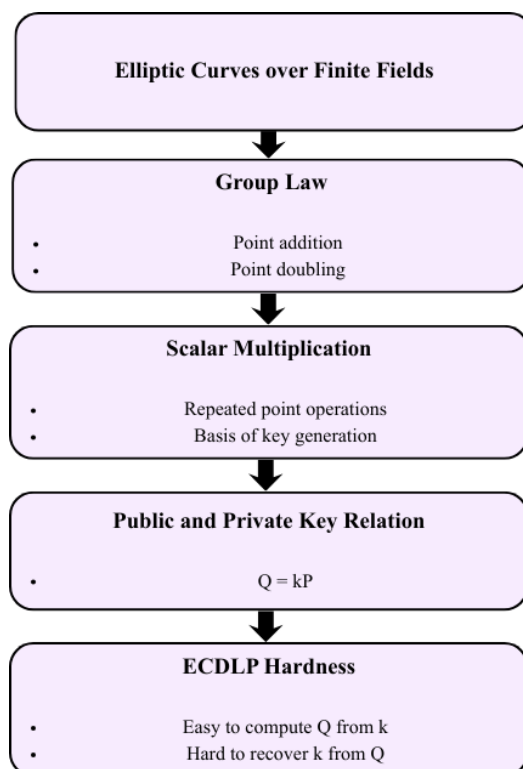


Figure 1. Mathematical foundation of ECC

4. Elliptic Curve Cryptographic Algorithms

Elliptic curve cryptography offers a design system to develop effective public-key cryptographic algorithms that rely on the mathematical properties of elliptic curves. Based on the elliptic curve discrete logarithm problem being computationally hard, these algorithms take advantage of this and guarantee security with relatively small key sizes and lower computational costs. The elliptic curve-based algorithms are more effective and more scalable than the traditional public-key cryptosystems, which is why they are especially applicable in the digital communication environment and resource-limited systems that are present nowadays (Diffie, 2019).

4.1 Elliptic Curve Diffie–Hellman

Elliptic Curve Diffie-Hellman (ECDH) is a key exchange protocol that has gained popularity in cryptography, and it enables two parties to agree on a common secret across an unsafe communication channel. Under this mechanism, every player creates their own key, which is the private key, and calculates a related key, which is the public key; this is performed through scalar multiplication on a chosen elliptic curve point. Through the exchange of public keys and other scalar multiplication actions, the two can manage to come up with the same shared secret that can later be utilized in performing a symmetric encryption. Its high efficiency and strong security features have seen the ECDH be used in other secure communication systems, such as wireless sensor networks and embedded devices (Aikins-Bekoe and Hayfron-Acquah, 2020).

4.2 Elliptic Curve Digital Signatures

Elliptic curve-based digital signature algorithms offer three cryptographic functions: authentication, integrity of data and non-repudiation of communication systems over the internet. One of the most popular ECC-based signature schemes, which is implemented most commonly, is the Elliptic Curve Digital Signature Algorithm (ECDSA). It works by creating a signature with the help of a private key and checking the authenticity of a message with the help of a relevant public key. ECDSA has been used extensively in infrastructures of secure communication, including authentication systems of smart grids and advanced metering systems, where the integrity of checking the information being sent is of paramount importance (Farooq et al., 2019).

4.3 Elliptic Curve Integrated Encryption

Elliptic Curve Integrated Encryption Scheme (ECIES) is an integrated encryption scheme, a hybrid encryption scheme that combines elliptic curve cryptography and symmetric encryption. The process that is used under this setup is that ECC is used to derive encryption keys safely, and then the actual data payload is encrypted using symmetric algorithms. It is an efficient combination and possesses high security properties. ECIES has been applied to various areas, including safe transmission of information systems in multimedia and medical information systems, where confidential information is vital (Benssalah et al., 2021).

4.4 Modern Elliptic Curve Signatures

Events in the recent history of the theory of elliptic curve cryptography have led to the creation of modern signature schemes such as EdDSA, and in particular, the Ed25519 one. These algorithms are supposed to provide

enhanced performance, simpler implementation and resistance to certain cryptographic attacks than the old signature schemes. One of them is Ed25519, which features deterministic signatures and a carefully selected set of curve parameters to render it highly efficient and provide a high security level. These elliptic curve signature systems in the modern age have been demonstrated to provide adequate security to the formal security analysis of the modern digital communication protocols (Brendel et al., 2021).

Most of the existing cryptographic infrastructures are made up of these elliptic curve-based algorithms. Enabling the secure exchange of keys, authentication and encryption of data with quite low computing power, ECC algorithms remain essential to the enhancement of the security of modern-day communication systems. Figure 2 defines the key ECC algorithms and their functionality roles. The main ECC algorithms described in this paper and their main cryptographic operations are summarized in Table 1.

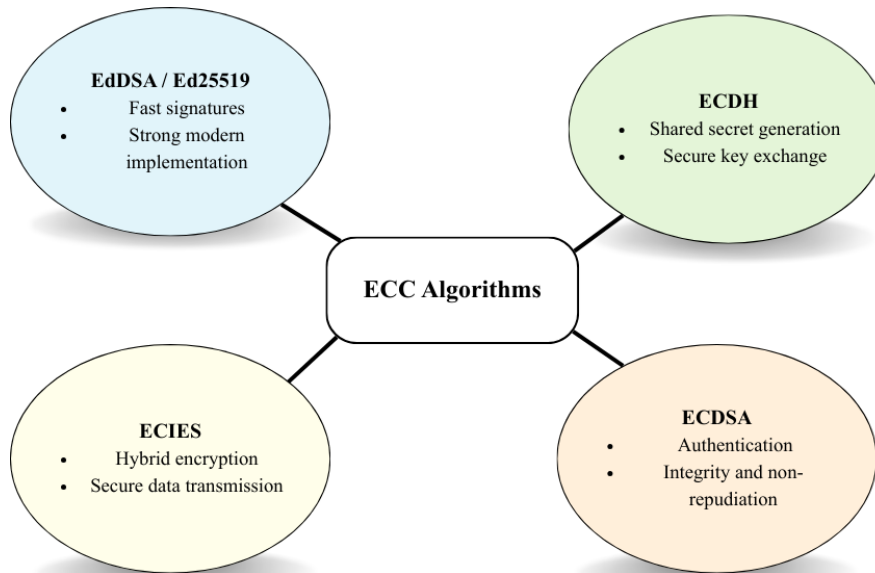


Figure 2. ECC algorithm ecosystem

Table 1. Core ECC algorithms and functions

Algorithm	Main Function	Security Role	Typical Use
ECDH	Key exchange	Shared secret establishment	Secure session setup
ECDSA	Digital signature	Authentication and integrity	Certificates, smart grids
ECIES	Hybrid encryption	Confidential data transfer	Secure messaging, medical data
EdDSA (Ed25519)	Modern digital signature	Fast and reliable signing	Secure protocols, modern applications

5. Advanced Mathematical Techniques for ECC Security

5.1 Efficient Scalar Multiplication

One of the fundamental operations in ECC is scalar multiplication, which consists of point addition and doubling on an elliptic curve repeated. As a lot of ECC algorithms depend on this operation extensively, scalar multiplication optimization is crucial to enhance the performance and lower the computational cost. Different mathematical techniques have been designed to speed up this process without compromising high security properties. The resource-constrained resource-using Internet of Things (IoT) devices, where energy consumption and computational efficiency are vital factors, are of particular significance (Kumar and Sukumar, 2019).

5.2 Intelligent Key Generation

There are also sophisticated approaches to key generation that have been considered to enhance the cryptography systems based on ECC. The application of optimization methods like the genetic algorithms to the

elliptic curve keys generation can increase their randomness and strengthen the cryptographic keys. These methods are used to implement evolutionary computer techniques in the quest to find optimal cryptographic parameters, hence enhancing the overall security of key generation processes within contemporary cryptographic systems (Kumar & Sharma, 2023).

5.3 Isogeny-Based Techniques

The isogeny-based cryptography is an important contribution towards the mathematical underpinnings of ECC. Isogenies are algebraic maps between elliptic curves which preserve the group structure but allow complex changes to be affected within elliptic curve systems. Isogenous cryptographic protocols take advantage of the computational complexity of locating such mappings between curves, and offer good security properties. Such methods have received much interest as possible candidates to post-quantum cryptography, because they are resistant to some quantum attacks (Mishra et al., 2025).

5.4 Advanced Algebraic Structures

ECC is also developed based on general progress in algebraic structures and number theory. Contemporary studies in algebraic geometry and group theory have helped to gain a better understanding of the properties of elliptic curves, allowing cryptographic systems to be designed to provide more security. Through these mathematical lessons, researchers can design curves that have favorable security properties and are able to study the possible weaknesses of elliptic curve-based algorithms (Shahid, 2024).

5.5 Pairing-Based Cryptography

The cryptography based on pairings is an expansion of the classic elliptic curve techniques that include bilinear pairings between elliptic curve group elements. These combinations allow the building of more complex cryptography applications, including identity-based encryption, functional encryption and short digital signatures. Pairing-based systems offer the ability to adapt cryptographic systems to complex security protocols by using bilinear maps on elliptic curves to develop flexible frameworks and support more advanced communication systems in the current world (Riyal et al., 2021).

5.6 Algorithmic Optimization Strategies

Besides the theoretical developments, the comparison of cryptographic algorithms has also revealed that optimization strategies are important in implementing ECC. These methods aim at providing the balance between the efficiency of computations, the level of security and the use of resources when implementing cryptography algorithms in real life. As the ECC has been compared to other public-key systems, such as RSA and Diffie-Hellman, it is revealed that ECC can readily attain the same security (with reduced key sizes) and reduced computing costs and thus is highly suited to the current secure communication infrastructures (Dalal et al., 2024).

All these advanced mathematical techniques combined render elliptic curve cryptography more secure, efficient and scalable. With the synthesis of recent improvements in algebraic theory, computational optimization and cryptographic protocols, ECC has continued to evolve as a highly secure and efficient technique of providing secure digital communication systems to this day. Table 2 provides a comparative summary of ECC and other popular public-key algorithms to show the differences in key size, performance, and ability to be used in applications.

Table 2. Comparison of ECC with classical public-key algorithms

Cryptographic Algorithm	Key Size Requirement	Computational Efficiency	Security Basis	Typical Applications
RSA	Large (2048–4096 bits)	Moderate to high computational cost	Integer factorization problem	Secure email, digital certificates
Diffie–Hellman	Large (2048+ bits)	Moderate computation	Discrete logarithm problem	Secure key exchange
ECC	Small (256–521 bits)	High efficiency with lower computation	Elliptic curve discrete logarithm problem	IoT, mobile security, TLS
Post-Quantum Algorithms	Large and complex parameters	Currently higher computational overhead	Lattice / code-based problems	Future quantum-resistant systems

6. Security Analysis and Cryptographic Attacks

Elliptic curve cryptography (ECC) security does not solely rely on the mathematical basis of cryptography, but also on the accuracy and strength of its implementation. Despite the high theoretical security of ECC that is smaller compared to many conventional public-key schemes, real-world implementation of ECC-based systems is susceptible to various hardware-, protocol-, and computation-level attacks. To effectively learn of the implementation vulnerabilities which may work against otherwise strong elliptic curve-based systems, however, a stringent security review is essential. The belief that memory corruption attacks are automatically resisted by hardware-level protection mechanisms is also one significant issue in the context of secure computing environments. It has been demonstrated that research on error-correcting code memory-based protections might not be entirely helpful in preventing attacks that cause faults, especially in Rowhammer-style exploitation. The findings introduce a bigger cryptographic security lesson. Implementation environments can introduce vulnerabilities that are not dependent on the mathematical strength of the

cryptographic algorithm, and hence system-level security analysis is required (Cojocar et al., 2019). The other major weakness of ECC is the passive side-channel attacks, in which an attacker measures physical leakage to steal secret data, e.g., timing, consumption or electromagnetic emissions. As the elliptic curve business is based on scalar multiplication, any minor variations during the implementation can reveal sensitive patterns of keys. According to the current surveys, the variety of suggested countermeasures may involve the performance, cost, and security trade-offs, meaning that side-channel resistance remains one of the largest concerns of ECC implementation (Abarzúa et al., 2021). Systems based on elliptic curves are also vulnerable to protocol-level attacks. Specifically, small subgroup attacks and invalid curve attacks take advantage of the incomplete verification of the public parameters in the process of key exchanges. In case of failure of a system to confirm that the received points belong to the relevant group and are of the right order, an attacker can exploit the protocol to divulge information regarding secret keys. Those attacks show that the deployment of secure ECC is to be supported by rigorous parameter checking

and close protocol design, along with a mathematically sound choice of curves (Cremers & Jackson, 2019). The advent of quantum computing has further added to the ECC security concerns. Particularly, Shor’s algorithm poses a theoretical threat since it is possible to use it to solve discrete logarithm problems on any sufficiently powerful quantum computer. Because the hardness of the elliptic curve discrete logarithm problem is the core of the security of ECC, the emergence of large-scale quantum computing might pose a major threat to existing ECC-based systems. The threat has inspired the deepening of interest in quantum-resistant cryptography methods and in the reevaluation of the existing security assumptions (Mohammed, 2024). Systems based on ECC made in the lightweight resource-constrained environment, e.g. RFID applications, are further compromised. They may be cost and power-efficient and

thus can restrict the development of robust security controls. This can lead them to be more vulnerable to wireless attacks and side-channel exploitation. Low-cost RFID protocols based on ECC Vulnerability analyses indicate that the practicality of security can rely on the effectiveness of balancing protocol efficiency with practical attack surface resistance (Gabsi et al., 2021). In general, security analysis of ECC should not only be confined to abstract mathematical hardness, but also to implementation integrity, protocol validation, physical leakage resistance and threats of future computations. These attack vectors require a complete study in order to develop elliptic curve cryptographic systems that can be secure in the present and future threat environment. Figure 3 shows the key attack surfaces and security threats to ECC implementations.

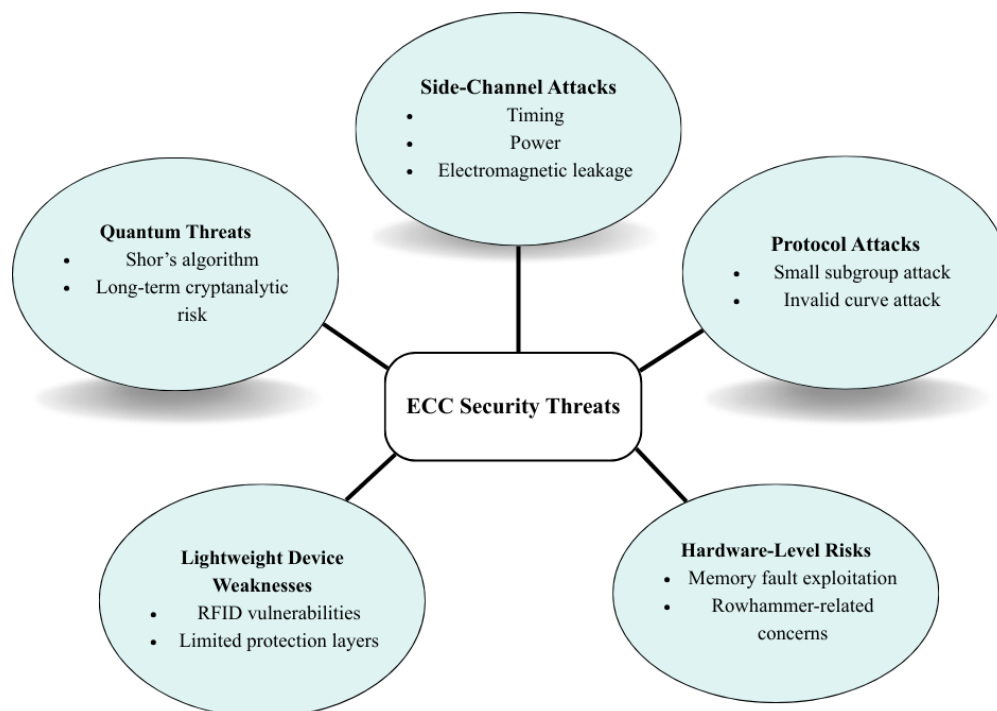


Figure 3. ECC threat landscape

7. Applications of Elliptic Curve Cryptography

7.1 Secure Communication Protocols

ECC has found application in authenticated communication systems, especially in the SSL/TLS systems that authenticate data transfer across the internet. The protocols use key exchange, authentication, and session establishment based on the premise of public-key cryptography and are provided as an alternative to the traditional algorithms, which are efficient using ECC because it reduces the number of bits in key size without compromising security. This benefit is especially applicable to the contemporary network settings, which necessitate fast and safe handshake systems for encrypted communication (Kumar et al., 2024). Furthermore, analysis of the performance of using SSL/TLS has demonstrated that cryptographic efficiency is significant in minimizing the latency and responsiveness of a secure communication system as a whole, which further demonstrates the

significance of ECC in the protocol design in optimized usage (Saranya, 2025).

7.2 Blockchain and Cryptocurrencies

ECC finds its basis in blockchain systems and cryptocurrency systems as well. In decentralized financial networks, elliptic curve-based digital signatures are typically applied in authenticating transactions, ensuring ownership of wallets, and non-repudiation. These characteristics are needed to ensure trust and integrity in the blockchain ecosystems, in which transactions cannot be validated by a centralized authority. The popularity of the elliptic curve mechanism in these systems can be explained by the fact that ECC is an appropriate tool to ensure secure, scalable, and distributed digital transactions (Chan et al., 2020).

7.3 Internet of Things

One of the most crucial application fields of ECC is the Internet of Things (IoT) due to the fact that most IoT

devices are limited to a rigid set of processing, memory, and power consumption. ECC-based authentication schemes that are lightweight have been suggested in order to provide security in communication between such devices and reduce computational overhead. These solutions prove that ECC is capable of offering practical protection to limited networked settings where other public-key algorithms might be less efficient (Hammi et al., 2020). Additional comparative assessments of ECC libraries to embedded devices also indicate the applicability of the scheme as they demonstrate that implementation and library architecture have a massive impact on the cryptographic performance of low-resource systems (Silde, 2019).

7.4 Edge-IoT Security

Besides the conventional IoT setting, ECC has been applied on edge-IoT setting, where data is computed by distributed nodes that are significantly closer to the place of generation. Such architectures also need secure authentication as the edge devices are likely to be in a heterogeneous and dynamic environment. The ECC-based models of authentication have been used to improve the establishment of trust and secure flow of information within these decentralized ecosystems and have cemented their relevance in new edge-based infrastructures (Alzahrani, 2025).

7.5 Cloud Authentication

Another significant area where ECC can be used to enable secure access control and user authentication is

cloud computing. Due to the fact that cloud services presuppose the safe exchange of credentials and the safety of remote communications, ECC-based protocols can offer an effective authentication and session security method. Safe user authentication systems based on ECC have shown that an elliptic model can improve confidentiality and computing efficiency in a cloud system, and it can support a distributed service model on a large scale (Rangwani and Om, 2021).

7.6 Mobile Cloud Security

Mobile cloud computing has also implemented ECC, where the mobile computers access common resources using the mobile devices, which have low processing power. In such an environment, safe sharing and access control systems take advantage of ECC due to its smaller key size and lower computation cost. ECC-based designs enable sharing of resources in a way that is elastic and secure, with protection against unauthorized access in the context of mobile cloud infrastructure (Hamad et al., 2023).

The use of ECC is very diverse, including internet communication and blockchain networks, IoT, edge computing, and cloud platforms. Its efficiency in implementation and high level of security have made it one of the most viable and flexible cryptographic strategies to be used in contemporary information systems. Table 3 highlights the key areas of application of ECC and why it is appropriate in any of these environments.

Table 3. Application domains of ECC

Application Domain	ECC Role	Key Advantage	Example Context
SSL/TLS	Key exchange and authentication	Reduced handshake overhead	Secure web communication
Blockchain	Transaction signing	Strong integrity with compact keys	Cryptocurrencies
IoT / Edge-IoT	Device authentication	Low computational burden	Smart connected devices
Cloud computing	User authentication	Efficient secure access	Distributed cloud services
Mobile cloud	Secure sharing and access control	Small key size and speed	Mobile resource access

8. Emerging Trends and Post-Quantum Considerations

The development of hybrid classical-post-quantum constructions occurs as one of the most significant new directions. These techniques use hybrid structures of classical cryptographic tools, e.g. ECC and post-quantum tools, to create layered security frameworks. Such hybrid designs are being considered in smart consumer and connected electronic environments, to preserve interoperability with the existing infrastructure, and to be more resilient to threats in the quantum era. This trend is the indicator of a feasible transition plan according to which ECC will continue to play an important role during the transition process through the adoption of the post-quantum transition (Yang et al., 2025). The applied use of hybrid keying mechanisms, via a mixture of classical as well as quantum and post-

quantum elements of cryptography, is also a relative advancement. These methods are directed to the purpose of strengthening the key establishment, by taking several security assumptions and moving them into a single system rather than simply replacing the current cryptosystems in a single leap. The strategies can especially be applied in the real-life communication systems where compatibility, migration cost and continuity of operations are very crucial. In such aspects, ECC can be regarded as a considerable classical aspect because of its maturity, efficiency and extensive coverage of its implementation (Ricci et al., 2024).

Isogeny-based cryptography is also an important mathematical direction in post-quantum cryptography. Isogeny-based constructions, based on mappings between elliptic curves, are extensions of the algebraic basis of ECC into new security models that are resistant

to quantum attacks. Studies in this field have considered how to trade off concrete security and computational efficiency, with both isogeny-based systems and elliptic curve-based systems being promising and complex as potential successors or complements to classical elliptic curve security systems (Corte-Real Santos, 2024). Meanwhile, ECC is still being developed in terms of the lightweight and mobile security environment, in which efficiency is one of the main demands. Mobile environment authentication protocols are becoming sensitive to lower computational requirements, low latency, and high security levels. Such environments give ECC a close operational edge due to its small key sizes and minimal operations that are suited to limited environments, despite more comprehensive post-quantum migration plans being underway (Garg et al., 2019).

The other trend, which is important, relates to the establishment of efficient algorithms, protocols and hardware architectures of next-generation cryptography in embedded systems. Since future cryptographic systems will have to be created to work on constrained and heterogeneous devices, there is increased discussion in creating architectures capable of efficiently implementing both classical and post-quantum primitives. Such a direction supports the transitional significance of ECC, as a contemporary standard of embedded security, as well as a standard of measuring the efficiency and deployability of future-generation cryptographic solutions (Banerjee, 2021)

9. Challenges, Limitations, and Future Research Directions

Despite the sound security concepts and efficiency advantages, elliptic curve cryptography (ECC) also has several problems that affect the extent of its further implementation and its usability in the future. Although ECC provides a great level of security with smaller key sizes compared to most conventional public-key schemes and indeed smaller key sizes, it is not a compact system and needs a prudent selection of parameters, implementation and adaptation to application environments. The studies of ECC utilization and application indicate that these remain the strongholds and the weaknesses of the cryptography systems to this day (Vijay Nikhil et al., 2025). One of the largest limitations, compared with more traditional algorithms, is the complexity of the mathematical implementation of ECC. Even though ECC provides all the advantages of elliptic curve arithmetic in terms of key size and processing requirements, the arithmetic on which it is built can be more difficult to implement with adequate and comprehensive security. This makes it more difficult to have software bugs, unsafe choice of parameters and misconfigurations of protocols, in particular in systems that do not have ideal cryptographic knowledge. The comparative analyses of ECC and RSA point to the fact that, regardless of the high efficiency of the former, which may be much higher than the latter, implementation hardship is a serious practical factor when dealing with ECC (Khan et al., 2023). The other problem is implementation in application specific

environment, such as cloud computing and secure data sharing platforms. The cryptographic functionality in these environments is not about the algorithm, and it is also about the interaction of the algorithm with the distributed structures, access-control systems and with large-scale service architectures. The systematic reviews relating to ECC in cloud data-sharing applications suggest that the problems of such issues, including interoperability, scalable key management, and protocol design with respect to security, remain in the list of issues. All these constraints imply that the feasibility of ECC in reality is founded on the cryptographic strength, as well as architectural flexibility (Alagarsundaram, 2023).

Future research would be focused on improving the safety of implementation, deployment simplicity in a complex digital ecosystem and improving ECC to new threats to computation. Further work is needed on the following areas: secure choice of curves, design of lightweight and strong protocols, resistance to implementation level attacks and integration in hybrid post-quantum. Considerable advancements in these directions will be needed to keep the practical significance of ECC, and to increase its use in the systems of secure communication of the following generation.

10. Conclusion

Cryptography is a security technique important to modern public-key security, both by offering powerful mathematical underpinnings and practical (and efficient) implementation, elliptic curve cryptography has become essential. The hardness of the elliptic curve discrete logarithm problem, its core algorithm efficiency, and its applicability to a wide variety of applications, including secure communication, IoT, cloud computing, blockchain, and embedded systems, are its strengths as have been observed in this review. At the same time, its practical security is not merely pegged to its theoretical validity, but also to its wise implementation, parameter verification and side channel and protocol level oral and novel quantum resistance. Recent advances in scalar multiplication, key generation, pairing constructions and isogeny constructions demonstrate that ECC is in its infancy as a fully-fledged classical cryptosystem, and as the foundation of future cryptographic development. Although there are still some challenges in the implementation complexity, interoperability and post-quantum transition, ECC has a lot to offer because of its security cost of computation balance. Its future development will therefore remain significant to the next-generation digital system security architecture design, which is resilient, efficient, and marketable.

References

1. Abarzúa, R., Valencia, C., & Lopez, J. (2021). Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC. *Journal of Cryptographic Engineering*, 11(1), 71-102.
2. Aikins-Bekoe, S., & Hayfron-Acquah, J. B. (2020). Elliptic curve diffie-hellman (ECDH) analogy for

- secured wireless sensor networks. *International Journal of Computer Applications*, 176(10), 1-8.
3. Alagarsundaram, P. (2023). A systematic literature review of the Elliptic Curve Cryptography (ECC) algorithm for encrypting data sharing in cloud computing. *International Journal of Engineering and Science Research*, 13(2).
 4. Alzahrani, N. (2025). Security importance of edge-IoT ecosystem: An ECC-based authentication scheme. *PLoS one*, 20(6), e0322131.
 5. Banerjee, U. (2021). *Efficient algorithms, protocols and hardware architectures for next-generation cryptography in embedded systems* (Doctoral dissertation, Massachusetts Institute of Technology).
 6. Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, 80(2), 2081-2107.
 7. Brendel, J., Cremers, C., Jackson, D., & Zhao, M. (2021, May). The provable security of ed25519: theory and practice. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 1659-1676). IEEE.
 8. Chan, S., Chu, J., Zhang, Y., & Nadarajah, S. (2020). Blockchain and cryptocurrencies. *Journal of Risk and Financial Management*, 13(10), 227.
 9. Cojocar, L., Razavi, K., Giuffrida, C., & Bos, H. (2019, May). Exploiting correcting codes: On the effectiveness of ecc memory against rowhammer attacks. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 55-71). IEEE Computer Society.
 10. Corte-Real Santos, M. (2024). *The design, concrete security and efficiency of isogeny-based cryptography* (Doctoral dissertation, UCL (University College London)).
 11. Cremers, C., & Jackson, D. (2019, June). Prime, order please! Revisiting small subgroup and invalid curve attacks on protocols using Diffie-Hellman. In *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)* (pp. 78-7815). IEEE.
 12. Dalal, Y. M., Supreeth, S., Amuthabala, K., Satheesha, T. Y., Asha, P. N., & Somanath, S. (2024, September). Optimizing security: A comparative analysis of rsa, ecc, and dh algorithms. In *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)* (pp. 1-6). IEEE.
 13. Deevi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2023). Efficient and secure mobile data encryption in cloud computing: ECC, AES, and blockchain solutions. *International Journal of Engineering Research and Science & Technology*, 19(2), 155-166.
 14. Diffie, W. (2019). Conventional versus public key cryptosystems. In *Secure communications and asymmetric cryptosystems* (pp. 41-72). Routledge.
 15. Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In *Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman* (pp. 365-390).
 16. Farooq, S. M., Hussain, S. S., & Ustun, T. S. (2019, March). Elliptic curve digital signature algorithm (ecdsa) certificate based authentication scheme for advanced metering infrastructure. In *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)* (Vol. 1, pp. 1-6). IEEE.
 17. Gabsi, S., Beroulle, V., Kieffer, Y., Dao, H. M., Kortli, Y., & Hamdi, B. (2021). Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks. *Sensors*, 21(17), 5824.
 18. Garg, S., Kaur, K., Kaddoum, G., Ahmed, S. H., Gagnon, F., & Guizani, M. (2019, April). ECC-based secure and lightweight authentication protocol for mobile environment. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-6). IEEE.
 19. Gupta, C., & Subba Reddy, N. V. (2022, January). Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. In *Journal of Physics: Conference Series* (Vol. 2161, No. 1, p. 012014). IOP Publishing.
 20. Hamad, A. H., Dawod, A. Y., Abdulqader, M. F., Al Barazanchi, I., & Gheni, H. M. (2023). A secure sharing control framework supporting elastic mobile cloud computing. *International Journal of Electrical and Computer Engineering*, 13(2), 2270.
 21. Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal*, 14(3), 3440-3450.
 22. Hankerson, D., & Menezes, A. (2025a). Elliptic curve discrete logarithm problem. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 784-787). Cham: Springer Nature Switzerland.
 23. Hankerson, D., & Menezes, A. (2025b). Elliptic curves. In *Encyclopedia of cryptography, security and privacy* (pp. 801-805). Cham: Springer Nature Switzerland.
 24. Hassan, S., Faridi, A. R., Shibli, A. R., & Srivastava, S. K. (2025). A novel approach to key exchange: dual-secured Diffie-Hellman with RSA integration. *International Journal of Information Technology*, 1-12.
 25. He, Y. H., Lee, K. H., Oliver, T., & Pozdnyakov, A. (2025). Murmurations of elliptic curves. *Experimental Mathematics*, 34(3), 528-540.
 26. Huang, Y., Su, Z., Zhang, F., Ding, Y., & Cheng, R. (2020). Quantum algorithm for solving hyperelliptic curve discrete logarithm problem: Y. Huang et al. *Quantum Information Processing*, 19(2), 62.
 27. Jain, V. (2021). A review on different types of cryptography techniques. *ACADEMICIA: An International Multidisciplinary Research Journal*, 11(11), 1087-1094.
 28. Khan, M. R., Upreti, K., Alam, M. I., Khan, H., Siddiqui, S. T., Haque, M., & Parashar, J. (2023). Analysis of elliptic curve cryptography & RSA. *Journal of ICT Standardization*, 11(4), 355-378.
 29. Kumar, D. D., Mukharzee, J. D., Reddy, C. V. D., & Rajagopal, S. M. (2024, March). Safe and secure communication using SSL/TLS. In *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 1-6). IEEE.

30. Kumar, K. S., & Sukumar, R. (2019). Achieving energy efficiency using novel scalar multiplication based ECC for android devices in Internet of Things environments. *Cluster Computing*, 22(Suppl 5), 12021-12028.
31. Kumar, S., & Sharma, D. (2023). Key generation in cryptography using elliptic-curve cryptography and genetic algorithm. *Engineering Proceedings*, 59(1), 59.
32. Mishra, S., Mondal, B., & Jha, R. K. (2025). A survey on isogeny-based cryptographic protocols. *Wireless Networks*, 31(3), 2993-3024.
33. Mohammed, A. (2024). Cyber security implications of quantum computing: Shor's algorithm and beyond. *Innov. Comput. Sci. J*, 10, 1-23.
34. Obukhov, V., Qadamova, Z., Sobirov, M., Ergashev, O., & Nabijonov, R. (2024). Methods for using elliptic curves in cryptography. In *E3S Web of Conferences* (Vol. 508, p. 05009). EDP Sciences.
35. Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd..
36. Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, 94(2), 025008.
37. Qadir, A. M., & Varol, N. (2019, June). A review paper on cryptography. In *2019 7th international symposium on digital forensics and security (ISDFS)* (pp. 1-6). IEEE.
38. Rangwani, D., & Om, H. (2021). A secure user authentication protocol based on ECC for cloud computing environment. *Arabian Journal for Science and Engineering*, 46(4), 3865-3888.
39. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. *IEEE Access*, 12, 23206-23219.
40. Riyal, A., Kumar, G., & Sharma, D. K. (2021). Pairing-based cryptography. In *Functional Encryption* (pp. 79-101). Cham: Springer International Publishing.
41. Saranya, N. (2025). Secure Communication Performance: Multidisciplinary Perspectives on SSL/TLS Latency and Optimization Strategies. *Bridge: Journal of Multidisciplinary Explorations*, 1(2), 31-36.
42. Shahid, A. (2024). ADVANCES IN ALGEBRAIC STRUCTURES AND THEIR APPLICATIONS. *Scientific Insights and Perspectives*, 1(01), 36-54.
43. Silde, T. (2019). Comparative study of ECC libraries for embedded devices. *Norwegian University of Science and Technology, Tech. Rep.*
44. Vijay Nikhil, U., Stamenkovic, Z., & Raja, S. P. (2025). A study of elliptic curve cryptography and its applications. *International Journal of Image and Graphics*, 25(06), 2550062.
45. Yan, Y. (2022, December). The overview of elliptic curve cryptography (ECC). In *Journal of Physics: Conference Series* (Vol. 2386, No. 1, p. 012019). IOP Publishing.
46. Yang, J., Govindarajan, V., Xu, X., Khan, M. A., Shaikh, Z. A., Ayouni, S., ... & Por, L. Y. (2025). Enhancing Cryptographic Security in Smart Consumer Electronics with a Hybrid Classical–Post-Quantum Framework. *IEEE Transactions on Consumer Electronics*.