Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 3081–3089
DOI : 10.47974/JDMSC-2469

Secure key exchange and digital signatures via elliptic curves and discrete mathematical principles

Prashant Vats [#]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Sandeep Kumar Budhani [†]
School of Computing
Graphic Era Hill University
Bhimtal Campus
Bhimtal 263136
Uttarakhand
India

Devesh Kumar Srivastava [§]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Saneh Lata Yadav [‡]
Department of Computer Science and Engineering
Centre of Excellence-Cloud Computing
K. R. Mangalam University
Gurugram 122103
Haryana
India

[#] *E-mail:* prashant.vats@jaipur.manipal.edu
[†] *E-mail:* sandeepbudhani13@gmail.com
[§] *E-mail:* devesh.srivastava@jaipur.manipal.edu
[‡] *E-mail:* ersnehlata70@gmail.com

Shashi Kant Gupta [@]
Department of Computer Science and Applications
ITM University Gwalior
Gwalior 474001
Madhya Pradesh
India

Ashok Kumar Saini *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

A strong framework for creating safe and effective cryptographic systems, elliptic curve cryptography (ECC) is especially useful for digital signature and key exchange protocols. Based on the principles of algebraic geometry and discrete mathematics, ECC requires significantly shorter key lengths while achieving the same level of security as traditional algorithms like RSA, making it ideal for contemporary settings where resource optimization and computational speed are crucial. With a focus on combinatorial logic and discrete structures, this paper explores the mathematical foundations of ECC and highlights how they contribute to its reliability and robustness. In-depth examinations of signature systems like the Elliptic Curve Digital Signature Algorithm (ECDSA) and key exchange strategies like Elliptic Curve Diffie–Hellman (ECDH) are given. In-depth analyses are also conducted of implementation issues, potential attack routes, and the importance of ECC in both present-day and next-generation cryptographic frameworks.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Elliptic curve cryptography (ECC), Key exchange, Digital signatures, Information security, Lightweight cryptography, Cloud security, Cryptographic algorithms, Secure communication, Energy-efficient cryptograph.*

1. Introduction

In today's rapidly expanding realm of digital communication, safeguarding the confidentiality, authenticity, and integrity of transmitted data has become paramount. As the volume of information exchanged over open networks continues to grow exponentially, cryptographic techniques serve as the cornerstone of information protection. Conventional public-key algorithms such as RSA and DSA, although extensively adopted, encounter limitations

[@] *E-mail:* **dr.gshashikant@gmail.com**
* *E-mail:* **ashok.saini@jaipur.manipal.edu (Corresponding Author)**

concerning key size efficiency and computational demand issues that are particularly significant in constrained environments like mobile platforms, embedded systems, and Internet of Things (IoT) infrastructures. Elliptic Curve Cryptography (ECC) has consequently gained prominence as a promising alternative, delivering equivalent security strength with notably smaller key parameters. This efficiency in computational and energy resources renders ECC well-suited for secure applications that prioritize speed and minimal power consumption. Mathematically, ECC is deeply rooted in principles derived from discrete mathematics, algebraic frameworks, and number theory. These mathematical constructs underpin its secure key establishment processes, such as the Elliptic Curve Diffie–Hellman (ECDH) protocol, and its signature generation mechanisms, notably the Elliptic Curve Digital Signature Algorithm (ECDSA). The present paper examines how discrete mathematical foundations—particularly modular arithmetic, group theory, and finite field algebra—shape the design and resilience of ECC-based cryptographic architectures. By investigating both the theoretical aspects and implementation methodologies of key exchange and digital signature systems, this study highlights the efficiency, scalability, and robustness of elliptic curve cryptography. Additionally, it reviews contemporary advancements, explores emerging security challenges such as quantum resilience, and discusses the growing integration of ECC within modern cryptographic standards and real-world security protocols.

2. Related work

The progression of cryptographic research has transitioned notably from conventional public-key algorithms such as RSA toward more advanced and performance-oriented approaches that cater to the demands of contemporary computing ecosystems, including cloud and big data frameworks. Imam et al. [1] presented an extensive evaluation of RSA-based encryption models, outlining their evolution and identifying present-day challenges in terms of computational efficiency and scalability. These insights underscore the necessity for lightweight yet secure alternatives, with Elliptic Curve Cryptography (ECC) emerging as a viable candidate. Simultaneously, cloud computing has established itself as a central paradigm for distributed data storage and processing. Foundational and subsequent analyses by Qian et al. [2] and Puri, Tiwary, and Shukla [3] discussed architectural models of cloud systems and associated security risks, emphasizing the critical role of incorporating strong cryptographic layers to ensure confidentiality and controlled access. Responding to these issues, Sohal and Sharma [4] introduced BDNA—a DNA-inspired symmetric cryptographic framework—aimed at fortifying security in cloud environments. In a similar vein, Bhowmik and Karforma [5] developed a hybrid encryption architecture that integrates isomorphic encryption with artificial neural networks and Mealy machine-based automation, contributing an intelligent and adaptive security mechanism for cloud-based systems. From a broader perspective, Lu et al. [6] conducted a comprehensive survey of

cryptographic solutions in big data applications, identifying ECC and homomorphic encryption as leading contenders for secure and scalable data protection. Their findings highlight the increasing demand for flexible encryption strategies capable of addressing the complexities inherent in large-scale data ecosystems. Complementing this viewpoint, El-Seoud, El-Sofany, and Taj-Eddin [7] carried out a comparative study of cloud security threats, concluding that the design of cryptographic protocols is central to countering risks such as unauthorized access, data breaches, and service-level exploitation. Expanding on these ideas, Mohammad et al. [8] explored modern cryptographic paradigms, advocating the integration of hybrid and non-traditional encryption models to overcome evolving cloud security challenges. Moreover, the continuing global shift toward cloud adoption has resulted in a substantial rise in data migration to cloud infrastructures, accentuating the importance of scalable and efficient cryptographic mechanisms [9]. Addressing these operational concerns, Li et al. [10] proposed TMACS—a threshold multi-authority access control scheme—that delivers a verifiable and secure model for public cloud data management through threshold cryptography. Collectively, these contributions [11–13] reinforce the strategic movement toward next-generation encryption models such as ECC, which offer a balanced combination of computational efficiency, high throughput, and robust security tailored for cloud-integrated environments.

3. Proposed Work

This study introduces a secure and high-performance framework for key exchange and digital signature generation utilizing ECC. The approach is deeply rooted in discrete mathematical constructs, including finite field theory, modular arithmetic, and combinatorial analysis [14, 15]. The central objective is to develop and implement an optimized ECC-based cryptographic model capable of maintaining strong confidentiality, data integrity, and authentication, particularly within environments constrained by limited computational and energy resources such as Internet of Things (IoT) systems and wireless sensor networks [16, 17]. The overall research methodology is structured into three major phases:

1. *Mathematical Modelling of ECC Operations*

The initial phase involves constructing elliptic curve models over finite fields, specifically considering both prime fields GF(p) and binary fields GF(2^m). Core elliptic curve operations, namely point addition, point doubling, and scalar multiplication, will be rigorously defined and mathematically optimized through advanced computation techniques such as Montgomery modular multiplication and window-based scalar multiplication methods. Emphasis will be placed on identifying and configuring secure yet computationally efficient curve parameters, with particular consideration of standardized curves like Curve25519 and FourQ, which provide an optimal balance between performance and cryptographic strength.

A finite field over an elliptic curve $E\ F_p \rightarrow$

$$E: y^2 = x^3 + ax + b \text{ with } a, b \in F_p$$

$\forall \rightarrow$ non $-$ singularity condition: $4a3 + 27b2 \equiv 0(modp)$

For curve over binary field $F_{2^m} \rightarrow$

$$E: y^2 + xy = x^3 + a.x^2 + b \text{ with } a, b \in F_2m$$

Set of Points on the Curve $\rightarrow\ P + O;$

$\forall P \in E(F_p);$

For two distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the curve where $P \neq$, the sum $R = P + Q = (x_3, y_3)$

slope $\lambda: \rightarrow \frac{y_2 - y_1}{x_2 - x_1}$ (mod p)

$$x_3 = \lambda_2 - x_1 - x_2(modp)$$
$$y_3 = \lambda(x_1 - x_3) - y_1(modp)$$

slope λ is computed $\forall\ P = Q$ at point $P \rightarrow \lambda = \frac{3x_1^2 + a}{2_1^y}(mod\ P)$

$$x_3 = \lambda_2 - 2x_1(modp)$$
$$y_3 = \lambda(x_1 - x_3) - y_1(modp)$$

P multiplied by scalar $k \rightarrow Q{=}kP = P + P + \cdots + P$

For point addition when $\rightarrow$

$$\frac{P}{Q}: \lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

For point doubling when $P{=}Q \rightarrow \lambda = \frac{x_1 + \frac{y1}{x1}}{x1}$

Montgomery Curve Form $\rightarrow By_2 = x^3 + Ax^2 + x$

Where $\rightarrow A, B \in F_p, B{\neq}0.$

2. *Design of ECC-Based Key Exchange and Signature Algorithms*

In this phase, we will implement:

- **ECDH** for secure key exchange, and
- **ECDSA** for digital signing and verification.

For ECC $-$ Based Key Exchange: for $ECDH \rightarrow$

Fp be a large finite prime field

$E: y^2 = x^3 + ax + b\ \ (modp)$ be an elliptic curve over Fp.

$G \in E(Fp)$ be a publicly agreed

$\rightarrow$ upon base point (also called a generator),

of prime order n.

$mathcal\{O\}n \cdot G = O$, where $O \approx \infty$.

For Key Generation$\rightarrow$

Each user $\forall x;\ x \in A,$ where a private key and computes a public key*:*

For User $A \rightarrow$ Private key: $d_A \in Z_n * d.$

Public key: $Q_A = d_A \cdot G$

For User $B \rightarrow$ Private key: $d_B \in Z_n * d.$

Public key: $Q_B = d_B \cdot G.$

Shared Secret Computation $\rightarrow$

For User $A \rightarrow S = d_A \cdot Q_B = d_A \cdot (d_B \cdot G) = d_B \cdot d_A \cdot G$
For User $B \rightarrow S = d_B \cdot Q_A = d_B \cdot (d_A \cdot G) = d_A \cdot d_B \cdot G$
For same point $S \in E(Fp), x$ coordinate of
$S(x, y): \rightarrow F(x') \exists$ symmetric key K_{shared} = Key Derrive $F(x)$.

For $ECC -$ Based Digital Signatures:

$$\text{for } ECDSA \begin{cases} : \text{Prime } p, \text{curve equation } E, \text{base point } G \\ : \text{Order of the base point: } n \\ : \text{Hash function: } H(\cdot), \text{such as } SHA - 256 \end{cases}$$

$$\text{Key Generation} \rightarrow \begin{cases} \text{Private key: } d \in [1, n-1] \\ \text{Public key: } Q = d \cdot GQ \end{cases}$$

For Signature Generation $\rightarrow$ To sign a message m
Hash the message : $e = H(m) \forall k \in [1, n-1]$
$\forall$ curve point $\epsilon (x1, y1)$

$$= k.G: \begin{cases} r = x1 mod n \text{ (must not be 0)} \\ s = k - 1(e + d \cdot r) mod n \text{ (must not be 0)} \end{cases}$$

For Signature Verification $\cong r, s \in [1, n-1]$;
Signature is valid if $r \equiv x1 mod\, n$.

Both schemes will be adapted to support high performance with minimal computational overhead, employing lightweight cryptographic libraries and optimization strategies suitable for embedded platforms.

3. *Security and Performance Evaluation*

The implemented cryptographic framework will be tested in simulated and real-world environments. The evaluation will include:

- Computational efficiency (execution time, CPU usage),
- Memory consumption, and
- Security analysis, including resistance to known attacks such as brute force, side-channel, and fault injection attacks.

For ECC security $\in$ infeasibility of ECDLP*:*
Given P and $Q = k \cdot PQ$, find the scalar $k \rightarrow$
Time Complexity $\rightarrow TECDLP = O(n)$
For ECC security $\in$ infeasibility of *ECDSA:*
Given P and $Q = k \cdot G$, find the scalar $k \rightarrow$
Time Complexity $\rightarrow$ *TSign=O(logn)*

Where relevant, a comparative analysis will be conducted against conventional public-key cryptographic schemes such as RSA and DSA, as well as other contemporary algorithms, to illustrate the enhanced security efficiency and computational advantages offered by ECC in practical implementations.

4. Result analysis

A rigorous evaluation and comparison of the suggested ECC-based key exchange and digital signature systems' performance with traditional RSA-based cryptographic techniques was conducted. A number of essential performance

metrics were considered in the evaluation, such as key length, encryption and decryption latency, time required for creating signatures and verification, storage footprint, bandwidth usage, and overall security strength. According to Table 1, the findings show that ECC uses significantly smaller key sizes than RSA while achieving security levels that are on par with or better. For example, 256-bit ECC keys offer the same cryptographic strength as 3072-bit RSA keys, therefore reducing computing complexity, storage requirements, and transmission overhead.

Table 1

Key Size vs Security Level

Security Level (bits)	ECC Key Size (bits)	RSA Key Size (bits)
80-bit security	160	1024
112-bit security	224	2048
128-bit security	256	3072
192-bit security	384	7680
256-bit security	521	15360

Performance results in Table 2 indicate that ECC requires 60–75% less computation time across encryption, decryption, and signature operations. Specifically, ECC achieves encryption in 15 ms, while RSA takes 48 ms under similar conditions. The resource utilization metrics shown in Table 3 demonstrate that ECC consumes less CPU power (12% vs. 34% for RSA), less memory (2.1 MB vs. 5.8 MB), and lower bandwidth per operation. Furthermore, ECC reduces energy consumption by approximately 66%, which is especially advantageous for mobile and embedded devices.

Table 2

Performance Comparison of ECC vs RSA

Operation	ECC (256-bit)	RSA (3072-bit)
Key Generation Time	20 ms	85 ms
Encryption Time	15 ms	48 ms
Decryption Time	22 ms	62 ms
Signature Generation	18 ms	72 ms
Signature Verification	25 ms	77 ms
Signature Size	64 bytes	384 bytes

Table 3

Resource Utilization and Efficiency

Metric	ECC (256-bit)	RSA (3072-bit)
CPU Usage (%)	12%	34%
RAM Usage (MB)	2.1 MB	5.8 MB
Bandwidth (per op)	0.3 KB	1.5 KB
Energy Consumption (J)	0.08 J	0.24 J

5. Conclusion

For effective key exchange and digital signature creation, this study presented a cryptographic architecture based on ECC that is both secure and optimized. In contrast to conventional RSA-based systems, the suggested architecture delivers good cryptographic security with significantly reduced key sizes by utilizing the mathematical robustness of elliptical curves and underlying discrete structures. ECC is a particularly appropriate solution for contemporary, resource-constrained computer environments since experimental results show that it provides comparable or improved security levels while demonstrating faster computational speed, lower CPU and memory utilization, and notably lower energy usage.

References

[1] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and critical review of RSA based public key cryptographic schemes: Past and present status," *IEEE Access*, vol. 9, pp. 155949–155976 (2021), doi: 10.1109/ACCESS.2021.3129224.

[2] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud computing: An overview," in *Proc. IEEE Int. Conf. Cloud Comput*., pp. 626–631 (Dec. 2009).

[3] G. S. Puri, R. Tiwary, and S. Shukla, "A review on cloud computing," in Proc. 9th Int. Conf. Cloud Comput., Data Sci. Eng., Noida, India, pp. 63–68 (Jan. 2019), doi: 10.1109/CONFLUENCE.2019.8776907.

[4] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1417–1425 (2022).

[5] A. Bhowmik and S. Karforma, "Isomorphic encryption and coupled ANN with mealy machine: A cutting-edge data security model for cloud computing environment," *Knowl. Inf. Syst*., vol. 65, no. 1, pp. 133–162 (Jan. 2023), doi: 10.1007/s10115-022-01760-y.

[6] S. Lu, J. Zheng, Z. Cao, Y. Wang, and C. Gu, "A survey on cryptographic techniques for protecting big data security: Present and forthcoming," *Sci. China Inf. Sci*., vol. 65, no. 10, pp. 201–301 (Oct. 2022), doi: 10.1007/s11432-021-3393-x.

[7] M. S. A. El-Seoud, H. F. El-Sofany, and I. A. Taj-Eddin, "Comparable and analytical study between some security issues in cloud computing," in Proc. 20th Int. Conf. Interact. Collaborative Learn., vol. 2, pp. 526–539 (2018).

[8] O. K. Jasim Mohammad, S. Abbas, E.-S. M. El-Horbaty, and A.-B. M. Salem, "Securing cloud computing environment using a new trend of cryptography," in Proc. Int. Conf. Cloud Comput. (ICCC), pp. 1–8 (Apr. 2015).

[9] "The latest cloud computing statistics [Internet]," Accessed: Aug. 12 (2023). [Online]. Available: https://aag-it.com/the-latestcloud-computing-statistics

[10] W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 5, pp. 1484–1496 (May 2016), doi: 10.1109/TPDS.2015.2448095.

[11] S. M. Abrahem and A. S. Abed, "Cubic JD-fuzzy ideals of BH-algebra," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1015–1023 (2025), doi: 10.47974/JDMSC-2035.

[12] A. A. Abbas and Z. M. Sallal, "Hybrid biometric authentication for banks security improvements," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 4-A, pp. 1037–1050 (2025), doi: 10.47974/JDMSC-2030.

[13] Z. A. Abdulrazzaq, M. S. Nayef, and M. Hbaib, "On semi-continuous and quasi-semi-continuous modules," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-A, pp. 1051–1058 (2025), doi: 10.47974/JDMSC-2031.

[14] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.

[15] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain enabled smart contract for smart city e-governance ecosystem," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

[16] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET J. Scientometrics Inf. Manage.*, vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.

[17] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *J. Interdiscip. Math.,* vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received July, 2025