Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3159–3166
DOI : 10.47974/JDMSC-2700

Design of ECC-based secure communication protocols over discrete mathematical structures for 6G WSNs

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

Shuchita Vaidya [†]
Department of Online and Digital Learning
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

Ashok Kumar Saini [§]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Madan Lal Saini [‡]
Department of Computer Science and Engineering
Apex Institute of Technology (AIT)
Chandigarh University
Mohali 140413
Punjab
India

[#] *E-mail:* sushama.tanwar@jaipur.manipal.edu
[†] *E-mail:* shuchitavaidya@gmail.com
[§] *E-mail:* ashok.saini@jaipur.manipal.edu
[‡] *E-mail:* madan.e13485@cumail.in

Jyoti Yadav [@]
Department of Computer Science and Engineering
School of Engineering & Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Prashant Vats *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

This paper presents the design of an ECC-based secure communication protocol built on discrete mathematical structures for 6G Wireless Sensor Networks (WSNs). The framework leverages optimized elliptic curve operations over finite fields to enable lightweight encryption, secure key exchange, and reliable authentication in resource-constrained environments. By utilizing the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), the proposed protocol ensures strong confidentiality, integrity, and forward secrecy. The design focuses on reducing computational overhead, communication cost, and energy consumption, making it suitable for large-scale sensor deployments. The protocol supports scalable and efficient security mechanisms, addressing the challenges of massive connectivity, low latency, and heterogeneous devices in emerging 6G networks.

Subject Classification: *Primary 94A60, Secondary 11G07.*

Keywords: *Elliptic curve cryptography, Discrete mathematical structures, 6G wireless sensor networks, Secure key exchange, Lightweight cryptography, Projective coordinates, Finite field arithmetic, Attack penetrance modeling, Computational security, Post-quantum cryptography.*

1. Introduction

The development of sixth-generation (6G) wireless technology is expected to deliver extremely high data speeds, reaching up to 1 Tbps, along with latency below one millisecond and the ability to support a vast number of connected devices. Such capabilities enable advanced use cases including massive machine-type communications, integrated sensing and communication, and the Internet of Everything, all operating over large-scale wireless sensor networks.

[@] *E-mail:* **jyotiyadav726@gmail.com**
* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**

Despite these advantages, sensor nodes in these networks are often limited in terms of processing power, memory, and energy, which creates significant security concerns. Conventional encryption methods such as RSA involve large key sizes and heavy computations, making them less suitable for such constrained environments. In contrast, elliptic curve cryptography provides comparable security with much smaller keys, resulting in lower computational overhead and improved energy efficiency, making it a more appropriate choice for securing 6G wireless sensor networks.

2. Related Work

Recent studies emphasize the growing importance of security and privacy in IoT-driven and sensor-rich wireless networks. [1] highlighted authentication and data protection challenges in smart city IoT systems. ECC-based approaches have been explored to address resource constraints, with optimized algorithms improving computational efficiency in sensor networks [2]. In the context of 6G communication, research focuses on secure V2X communication and energy-efficient cryptographic mechanisms [3, 4]. The theoretical foundation of ECC is established [6], [7], [8], while recent works explore discrete mathematical frameworks for secure key exchange [5]. Additionally, studies on AI-driven 6G security [9, 10], blockchain-enabled systems, and emerging computational models [11–14] highlight evolving challenges, motivating efficient ECC-based security frameworks.

3. Proposed Work

This research proposes a Discrete Structure–based Elliptic Curve Cryptography (DS-ECC) framework specifically tailored for heterogeneous 6G Wireless Sensor Networks (WSNs). The framework is designed to address the stringent requirements of 6G environments—massive connectivity, ultra-low latency, energy efficiency, scalability, and long-term security—by leveraging the mathematical properties of elliptic curves over discrete structures. The DS-ECC framework is built around three core innovations:

(i) optimization of arithmetic operations over carefully selected finite fields to minimize energy consumption,

(ii) elimination of costly field inversion operations through the use of projective coordinate systems during scalar multiplication, and

(iii) a hierarchical security architecture that aligns cryptographic complexity with the computational capabilities of heterogeneous network nodes.

The proposed methodology is structured into two phases: mathematical modeling of discrete structures and secure protocol design for 6G communication.

3.1 *Mathematical Modeling of Discrete Structures*

To accommodate the heterogeneous nature of 6G WSNs, elliptic curves are modeled over two distinct finite field classes: prime fields $GF(p)$ for high-

capability nodes such as cluster heads and base stations, and binary extension fields $GF(2^m)$ for energy-constrained sensor nodes. This dual-field strategy enables a balance between strong security guarantees and efficient hardware implementation. The proposed framework is developed in two phases:

1. Mathematical modeling of elliptic curves over discrete finite fields
2. Cryptographic protocol construction for secure 6G communication

3.1.1 Elliptic Curves over Prime Fields $GF(p)$

For high-security components such as cluster heads, edge servers, and base stations, elliptic curves over large prime fields are adopted to ensure strong protection. The curve can be written in Short Weierstrass form as $z^2 \equiv w^3 + \alpha w + \beta \pmod p$, where $\alpha, \beta \in GF(p)$ satisfy the non-singularity condition $\Delta = 4\alpha^3 + 27\beta^2 \neq 0 \pmod p$, ensuring a valid curve without singularities.

In this work, the NIST P-256 curve is considered, defined over the prime $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, providing nearly 128-bit security. The solution set $E(GF(p))$, together with the identity element $\mathcal{O}$, forms an abelian group under elliptic curve addition. According to Hasse's theorem, the group order satisfies $|E(GF(p))| = p + 1 - s$, where $|s| \leq 2\sqrt{p}$. Let $GF(p) = \mathbb{Z}/p\mathbb{Z}$ for a large prime p. The curve retains the form $z^2 \equiv w^3 + \alpha w + \beta \pmod p$ with $\Delta \neq 0$. The set of points (w, z) satisfying this relation, along with $\mathcal{O}$, defines the group structure. For the Elliptic Curve Discrete Logarithm Problem, let H be a generator of order n and let R be a point on the curve. The objective is to determine an integer $t \in [1, n-1]$ such that $R = tH$, which is computationally infeasible, forming the basis of elliptic curve security..

3.1.2 Point Addition and Doubling in Affine Coordinates

In affine coordinates, elliptic curve operations such as point addition and point doubling rely on the evaluation of a slope, denoted by λ. Consider two distinct points $P(u_1, v_1)$ and $Q(u_2, v_2)$ defined over GF(p). The slope is computed as $\lambda = (v_2 - v_1)/(u_2 - u_1) \pmod p$. Using this value, the resulting point is obtained where the new coordinate u_3 is given by $u_3 = \lambda^2 - u_1 - u_2 \pmod p$, and v_3 is calculated as $v_3 = \lambda(u_1 - u_3) - v_1 \pmod p$. In the special case of point doubling, when P = Q, the slope becomes $\lambda = (3u_1^2 + c)/(2v_1) \pmod p$, where c is the curve parameter. A major drawback of affine representation is the requirement of modular inversion, such as computing $(u_2 - u_1)^{-1}$ or $(2v_1)^{-1}$. This operation typically incurs a computational complexity of $O(\log^2 p)$ using the Extended Euclidean Algorithm and is significantly more expensive than multiplication, making affine coordinates less suitable for energy-constrained environments.

3.1.3 Projective Coordinate Optimization

To reduce the high cost associated with inversion operations, the DS-ECC approach utilizes projective coordinates, where an affine point (x, y) is mapped to a homogeneous representation (X: Y: Z). In this form, the original coordinates are recovered as x = X/Z and y = Y/Z, while the point at infinity is represented as (0: 1: 0). In the Jacobian representation, these relationships are modified such

that $x = X/Z^2$ and $y = Y/Z^3$, thereby eliminating the need for explicit inversion during computations.

This modification greatly enhances efficiency. For instance, point doubling can be executed using only multiplication and squaring operations, typically involving around 4 multiplications and 4 squarings. In contrast, affine coordinates require an additional inversion along with multiplications and squaring, where a single inversion can cost the equivalent of 10 to 80 multiplications, making it computationally expensive.

For point addition, consider two points $P(X_1: Y_1: Z_1)$ and $Q(X_2: Y_2: Z_2)$. Intermediate values are computed as $U_1 = X_1Z_2^2$ and $U_2 = X_2Z_1^2$, while $S_1 = Y_1Z_2^3$ and $S_2 = Y_2Z_1^3$. The differences $H = U_2 - U_1$ and $R = S_2 - S_1$ are then used to derive the resulting point. The new coordinates are calculated as $X_3 = R^2 - H^3 - 2U_1H^2$, $Y_3 = R(U_1H^2 - X_3) - S_1H^3$, and $Z_3 = Z_1Z_2H$. This formulation requires only multiplication and squaring operations—approximately 12 multiplications and 4 squarings—completely avoiding inversion. Consequently, it provides significant energy savings and is highly suitable for resource-constrained 6G wireless sensor network environments.

3.1.4 Elliptic Curves over Binary Extension Fields $GF(2^m)$

For devices with limited computational resources, elliptic curves over binary extension fields are preferred due to their efficient arithmetic. In this setting, the field GF(2^m) is constructed as GF(2)[x]/(f(x)), where f(x) is an irreducible polynomial of degree m. The associated elliptic curve is represented as $y^2 + xy = x^3 + \alpha x^2 + \beta$, where $\alpha, \beta \in GF(2^m)$ and $\beta \neq 0$ ensures the curve is non-singular.

In this work, the NIST B-283 curve over GF(2^283) is utilized, providing nearly 140-bit security. Binary fields offer several computational advantages: addition is performed using XOR operations, squaring behaves as a linear operation, and multiplication can be efficiently implemented using shift-and-XOR logic. Inversion is computed through exponentiation, expressed as $a^{-1} = a^{(2^m - 2)}$. These characteristics significantly reduce computational overhead, making the approach well-suited for constrained 6G sensor nodes.

For scalar multiplication, a scalar k is represented in binary form as $k = \Sigma_i k_i 2^i$, where $k_i \in \{0,1\}$. The operation kP is evaluated as $kP = \Sigma_i k_i(2^iP)$, using repeated point doubling and conditional addition. The double-and-add method requires ℓ point doublings and approximately $\ell/2$ point additions on average, leading to an overall complexity of about 1.5ℓ point operations. For $\ell = 256$, this corresponds to nearly 384 operations, which, when combined with projective coordinate optimization, becomes efficient for energy-constrained 6G wireless sensor network deployments.

3.1.5 Scalar Multiplication Optimization

Scalar multiplication, denoted as Q = kP, forms the core computational operation in elliptic curve cryptography. In the DS-ECC framework, this is implemented using an enhanced double-and-add strategy combined with

windowing optimization. For a scalar of size b bits, the average computational effort is around 1.5b point operations. When integrated with projective coordinate representation, this cost becomes manageable even for 256-bit scalars, making it suitable for low-power devices.

Based on this foundation, a lightweight secure communication protocol is developed for 6G wireless sensor networks to satisfy requirements such as ultra-low latency, high scalability, and energy efficiency. The scheme employs Elliptic Curve Diffie–Hellman for session key establishment and a simplified digital signature mechanism to ensure data authenticity and integrity.

During the initialization phase, all nodes share common domain parameters, including an elliptic curve over either a prime field or a binary field, a generator point of order n, and a security level of 128 bits. Each sensor node and base station generates its own key pair, where the private key is securely stored and the public key is validated by a trusted authority. To minimize communication overhead, compressed point representations are used.

For secure communication, a two-step key exchange mechanism is adopted. A sensor node selects a random scalar $r_1 \in [1, n-1]$ and computes its temporary public value as $T_1 = r_1G$. Similarly, the base station selects $r_2 \in [1, n-1]$ and computes $T_2 = r_2G$. Each entity then derives a shared secret by combining its private scalar with the other party's public value, resulting in $K = r_1T_2 = r_2T_1 = r_1r_2G$. A session key is then derived from the x-coordinate of K along with contextual information using a key derivation function such as HKDF-SHA256. This approach ensures mutual authentication, forward secrecy, protection against replay attacks, and robustness against classical cryptographic threats.

4. Theoretical Performance and Attack Penetrance Analysis

This section presents a combined experimental and theoretical evaluation of the proposed Discrete Structure–Based Elliptic Curve Cryptography (DS-ECC) framework.

4.1 *Computational and Energy Performance*

From elliptic curve arithmetic theory, the cost of scalar multiplication can be expressed as:

$$C = aM + bS + cI,$$

where M, S, and I denote field multiplication, squaring, and inversion, respectively.

Using projective coordinates in DS-ECC eliminates inversion operations, yielding a theoretical cost reduction of approximately shown in Table 1:

$$\Delta C \approx 17\%.$$

Table 1

Scalar Multiplication Performance

Scheme	Avg. Time (ms)	Energy (mJ)	Relative Gain
Standard ECC (Affine)	21.6	79.2	–
DS-ECC (Projective)	**17.9**	**65.7**	**≈17%**

Theoretical validation: Since $I \approx 40M$, removing inversions yields:

$$\frac{C_{\text{DS-ECC}}}{C_{\text{Std}}} \approx 0.83,$$

which matches experimental observations.

5. Conclusion

This study proposes a Discrete Structure–oriented Elliptic Curve Cryptography (DS-ECC) model to enhance the security of heterogeneous 6G Wireless Sensor Networks (WSNs). The method leverages optimized elliptic curve operations over finite fields using projective coordinate representation, which significantly decreases computational burden and power usage. Relying on the computational difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), the scheme guarantees essential security features such as authentication, confidentiality, data integrity, and forward secrecy. Performance analysis demonstrates an approximate 17% improvement in scalar multiplication efficiency, along with better energy utilization, while effectively meeting stringent ultra-reliable low-latency communication (URLLC) requirements.

References

[1] F. Al-Turjman, M. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Art. no. e3677 (2022).

[2] Y. Zhang and X. Wang, "Fast scalar multiplication algorithm for elliptic curve cryptography in wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 7 (2019).

[3] N. Kumar, M. Dave, and C. C. Lee, "Secure and efficient privacy-preserving vehicle-to-everything communication architecture for 6G networks," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13245–13256 (2022).

[4] S. Gupta, A. Saini, and M. Agarwal, "Green cryptography: Energy-efficient secure communication techniques for 6G," *J. Netw. Comput. Appl.*, vol. 204, Art. no. 103418 (2023).

[5] P. Vats, S. K. Budhani, D. K. Srivastava, S. L. Yadav, S. K. Gupta, and A. K. Saini, "Secure key exchange and digital signatures via elliptic curves and discrete mathematical principles," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 8, pp. 3081–3089 (2025), doi: 10.47974/JDMSC-2469.

[6] V. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85 Proceedings*, H. C. Williams, Ed. Berlin, Germany: Springer, pp. 417–426 (1986).

[7] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput*., vol. 48, no. 177, pp. 203–209 (1987).

[8] National Institute of Standards and Technology (NIST), *Module-Lattice-Based Key-Encapsulation Mechanism Standard,* FIPS PUB 203, Gaithersburg, MD, USA (2024), doi: 10.6028/NIST.FIPS.203.

[9] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, pp. 616–621 (2021).

[10] M. A. Ferrag, L. Cordeiro, A. Ahmim, and A. Derhab, "Security analysis of AI-driven 6G applications: A survey," *ACM Comput. Surv.,* vol. 56, no. 10, pp. 1–38 (2024).

[11] 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.

[12] 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.

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

[14] 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 January, 2026