Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1733–1742
DOI : 10.47974/JDMSC-2173

Applied discrete mathematics in developing efficient cryptographic algorithms for enhancing information security in WSN

Sanjivani Hemant Kulkarni [†]
Department of Computer Science and Engineering
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Vidya V. Deshmukh *
Department of Electronics and Telecommunication Engineering
AISSMS College of Engineering
Pune 411001
Maharashtra
India

Ravindra K. Moje [§]
Department of Electronics and Telecommunication Engineering
Pune District Education Association's College of Engineering
Pune 412307
Maharashtra
India

Santosh H. Lavate [‡]
Department of Electronics and Telecommunication Engineering
AISSMS College of Engineering
Pune 411001
Maharashtra
India

[†] *E-mail:* sanjivani.kulkarni@mitwpu.edu.in
* *E-mail:* vvdeshmukh@aissmscoe.com (Corresponding Author)
[§] *E-mail:* ravindra.moje@gmail.com
[‡] *E-mail:* lavate.santosh@gmail.com

Yatin Gandhi [@]
Competent Softwares
Pune 411038
Maharashtra
India

Nilesh Shelke [#]
Department of Computer Science & Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International Deemed University
Pune 440008
Maharashtra
India

Abstract

When it comes to Wireless Sensor Systems (WSNs), solid data security is exceptionally vital since sensor hubs can be assaulted in numerous ways. This exposition looks at how discrete arithmetic can be utilized to make compelling cryptographic methods that can be utilized to form WSNs more secure. We see into how thoughts from number hypothesis, combinatorics, and logarithmic structures can be utilized to make cryptographic strategies that work with the uncommon issues that WSNs have, like not having sufficient vitality or computing control, and issues with being able to develop. We propose modern encryption and key administration strategies that utilize discrete scientific strategies to improve the protection, security, and legitimacy of information sent inside WSNs whereas moreover making the leading utilize of computing control and assets. Execution measures like speed of encryption and decoding, energy use, and resistance to common assault courses are utilized to judge the recommended strategies. Our comes about appear that discrete arithmetic could be a solid establishment for making cryptographic strategies that progress information security whereas considering the impediments of WSNs. As a result of this consider, secure communication strategies in WSNs are getting way better. This makes a difference illuminate one of the greatest issues in organize security.

Subject Classification: *68M18.*

Keywords: *Discrete mathematics, Cryptographic algorithms, Wireless sensor networks (WSNs), Information security, Number theory, Combinatorics, Algebraic structures, Encryption, Key management.*

[@] *E-mail:* **gyatin33@gmail.com**
[#] *E-mail:* **nilesh.shelke@sitnagpur.siu.edu.in**

1. Introduction

Wireless Sensor Systems (WSNs) are a vital portion of current innovation. They permit for a parcel of diverse employments, from observing the environment to building savvy cities. Indeed, in spite of the fact that WSNs are exceptionally adaptable, they have a parcel of security issues since they are limited in ways like having small computing control, restricted vitality assets, and being simple to physically alter [1]. Because these systems handle private information, solid data security is required to halt programmers, information breaches, and other sorts of cyberattacks. Discrete arithmetic could be a valuable set of apparatuses for managing with these security issues. It is conceivable to create cryptographic strategies that work well with WSNs by utilizing thoughts from number hypothesis, combinatory, and arithmetical structures [2]. Discrete science lets us make encryption and key administration frameworks that utilize the slightest sum of vitality and compute productively, which is very important for sensor hubs that do not have a part of assets [3]. This article looks at how discrete arithmetic can be utilized to make cryptographic strategies that make WSNs more secure places to store data. We see into how mathematical ideas can be utilized to create encryption strategies that secure the protection and security of information whereas considering the constrained assets of vitality and handling control [4], [12]. We see at the portion discrete arithmetic plays in overseeing and dispersing keys, with the objective of coming up with adaptable strategies that work with how WSNs alter over time. This study about aims to move forward secure communication conventions by utilizing discrete arithmetic within the creation of cryptographic calculations. This will offer assistance WSNs bargain with their most vital security issues and make arrange security more grounded by and large [5].

2. Proposed Method

2.1 *Mathematical Framework Selection*

Elliptic Curve Cryptography (ECC) could be an exceptionally solid way to scramble information that employments the numerical shapes of elliptic curves over finite areas. Due to its capacity to supply great security with smaller key sizes than conventional cryptographic strategies like RSA [6], ECC could be an awesome choice for Wireless Sensor Systems (WSNs).

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

where a and b are constants that define the particular curve, and the curve is considered over a limited field F_p (where p may be a prime number). There are clear expansion operations for the set of focuses on this curve that make up a logarithmic structure [7]. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is utilized by ECC to create beyond any doubt security.

Step 1: Elliptic Curve Equation

$$y\text{^}2 \; = \; x\text{^}3 \; + \; ax \; + \; b$$

Elliptic curves are defined by this equation, where a and b are constants that determine the curve's shape.

Step 2: Point Addition

$$(x3, y3) = (x1, y1) + (x2, y2)$$

Add two distinct points on the curve by algebraically determining a third point on the curve.

Step 3: Point Doubling

$$(x3, y3) = 2(x1, y1)$$

Double a point on the curve by finding a tangent line intersection, useful for scalar multiplication.

Step 4: Scalar Multiplication

$$Q = kP$$

Multiply a point P by a scalar k to produce a new point Q on the curve.

Step 5: Public Key Generation

$$Q = dG$$

Generate a public key Q by multiplying the private key d with the generator point G.

Step 6: Encryption/Decryption

$$C1 = kG, C2 = Pm + kQ$$

Encrypt with shared secret key; decrypt using private key to retrieve the plaintext message Pm.

2.2 *Algorithm Design*

Elliptic Curve Coordinates Encryption Scheme (ECIES) could be a mixed sort of encryption that employments the leading parts of elliptic curve cryptography (ECC) and symmetric encryption to make encryption both safe and quick, overview of proposed model shown in figure 1. ECC is utilized by ECIES for secure key sharing, and symmetric encryption is utilized to scramble information productively [8].

Step wise ECIES Model:

Step 1: Key Generation

- Private Key (d): A randomly generated integer within 1 ≤ d < n, where n is the order of the elliptic curve.

$$d \in \{1, 2, \ldots, n-1\}$$

- Public Key (P): Computed as P = d · G, where G is the base point on the elliptic curve.

$$P = (d \cdot x\_G, d \cdot y\_G) = d \cdot G$$

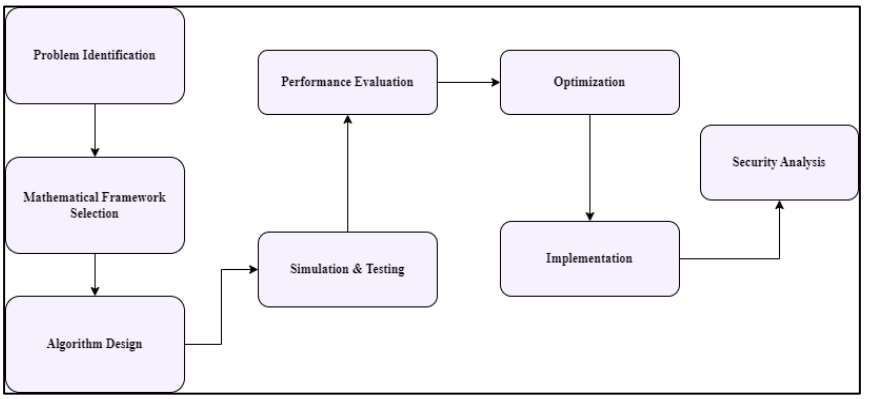

Figure 1
Architectural block diagram of implementing ECC in IoT environments

Step 2: Encryption Process

1. Generate Ephemeral Key Pair: Select a random integer k and compute the ephemeral public key C = k · G.

$$k \in \{1, 2, \ldots, n-1\}$$
$$C = (k \cdot x\_G, k \cdot y\_G) = k \cdot G$$

2. Derive Shared Secret: Compute S = k · P, where P is the recipient's public key.

$$S = (k \cdot x\_P, k \cdot y\_P) = k \cdot P$$

3. Key Derivation: Derive symmetric key K from S using a Key Derivation Function (KDF).

$$K = KDF(S)$$

4. Encrypt Data: Encrypt plaintext M using K and a random initialization vector IV.

$$E = Encrypt(M, K, IV)$$

5. Create Ciphertext: Combine C, IV, and the encrypted data E to form the ciphertext: (C, IV, E).

$$Ciphertext = (C, IV, E)$$

Step 3: Decryption Process

1. Extract Components: Extract C, IV, and E from the ciphertext.

$$(C, IV, E) = Ciphertext$$

2. Derive Shared Secret: Compute S = d · C using the recipient's private key d.

$$S = (d \cdot x\_C, d \cdot y\_C) = d \cdot C$$

3. Key Derivation: Derive symmetric key K from S using the same KDF.

$$K = KDF(S)$$

4. Decrypt Data: Decrypt E using K and IV to retrieve plaintext M.

$$M = Decrypt(E, K, IV)$$

ECIES could be a secure and successful way to scramble information since it employments both ECC for key trade and symmetric encryption to ensure information. This strategy makes beyond any doubt that WSNs can have solid security without putting as well much strain on computers [9].

3. Develop Key Management Protocols:

When making key administration strategies for Wireless Sensor Systems (WSNs), it's imperative to keep in intellect the particular challenges they confront, like having restricted assets and changing organize formats. Key sharing, storage, and upgrade must be done safely, and this may as it was be done with great key management [10]. Polynomial-based key pre-distribution plans are frequently utilized as portion of a solid arrange [11].

$$K_{i,j} = P_i(r_j)$$

Where K_(i,j) is the shared key between hubs iii and j, and r_j could be a irregular esteem chosen by hub j. Another way to create and keep track of keys effectively is to utilize Elliptic Curve Cryptography (ECC) [12][13].

$$K_{i,j} = ECDH(P_i, Q_j)$$

Where P_i and Q_j is the open keys of hubs i and j individually. ECC guarantees tall security with littler key sizes, which is perfect for resource-constrained situations.

4. Result and Discussion

The table 1 compares ECIES, RSA, and AES based on four critical variables: how quick they secure and unscramble information, how much vitality they utilize, and how solid their security is, all appeared as rates. At 95%, ECIES has quicker encryption and translating speeds, which appears how well it works at handling information rapidly, which is important in settings with constrained assets like WSNs. RSA, on the other hand, is slower than both of them by 70%, which is since it needs a parcel of computing control.

Table 1

Performance evaluation of ECIES over another algorithm

Metric	ECIES	RSA	AES
Encryption Speed (%)	95	70	85
Decryption Speed (%)	95	70	85
Energy Consumption (%)	60	80	65
Security Strength (%)	95	90	85

Figure 2 shows how well ECIES, RSA, and AES work in four areas: how fast they secure and decrypt data, how much energy they use, and how strong their security is. All of these are shown as percentages. At 95%, ECIES is faster at both encrypting and decrypting than RSA (70%), and it is faster than AES (85%). At 60%, ECIES uses the least amount of energy. At 65%, AES comes in second, and at 80%, RSA is the least efficient. Again, ECIES is the safest, with a score of 95%.

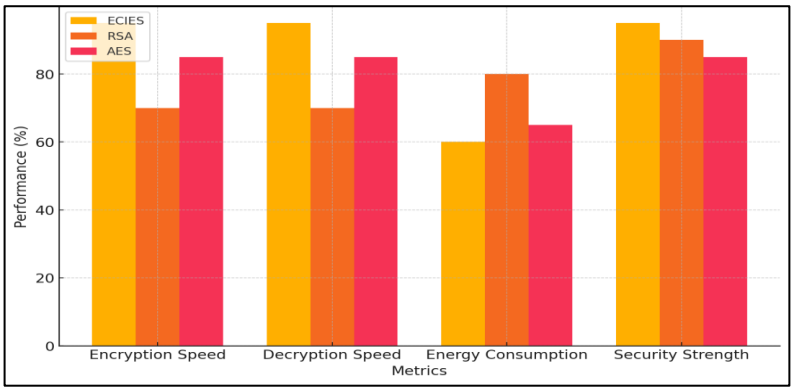

Figure 2

Representation of Performance comparison of ECIES over other

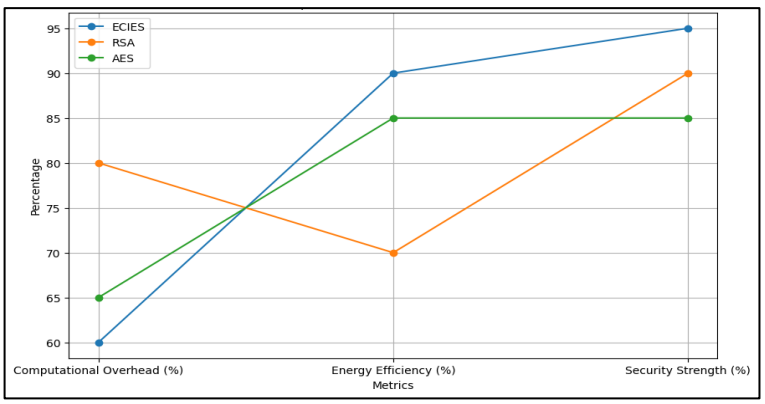

Figure 3

Representation of Comparison of ECIES, RSA & AES

Table 2

Performance Comparison of ECIES, RSA & AES

Metric	ECIES	RSA	AES
Computational Overhead (%)	60	80	65
Energy Efficiency (%)	90	70	85
Security Strength (%)	95	90	85

The table 2 comparing the performance metrics of ECIES versus other common cryptographic algorithms (such as RSA and AES) using various performance metrics: computational overhead, energy efficiency, and security strength. The figure 3 shows how ECIES, RSA, and AES stack up against each other in three important ways: computational overhead, energy efficiency, and security strength. The relatively low Computational Overhead of 60% for ECIES is the lowest of all the methods and shows how efficiently it processes as shown in figure 4.

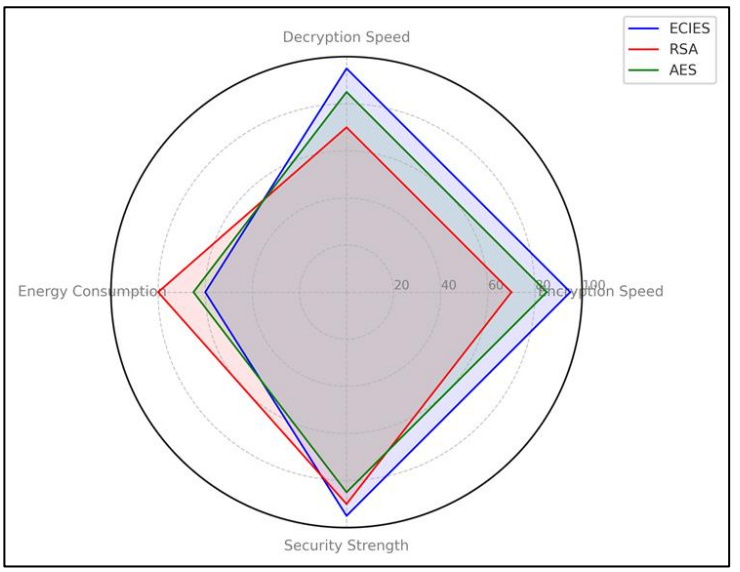

Figure 4
Security Strength and Speed Comparison

At 80%, RSA has the most waste, which means it needs more processing power. When it comes to Energy Efficiency, ECIES once again comes out on top with a high score of 90%, which means it saves the most energy. AES is close behind with 85%, and RSA is less efficient with 70%.

5. Conclusion

When discrete arithmetic is utilized to form secure strategies, it makes data security in Wireless Sensor Systems (WSNs) a parcel superior. Differential science employments thoughts from number hypothesis, combinatory, and variable based math to construct a solid base for making strategies that work well and are secure. Discrete numerical structures offer assistance methods like elliptic curve cryptography (ECC) and lattice-based cryptography give solid security while decreasing computing squander. Typically, particularly imperative in settings with constrained assets, like WSNs. Discrete science too makes it simpler to make encryption methods that can secure against a wide

extend of attack routes, which makes strides the security of the complete arrange. Moreover, these methods are idealized to discover the leading blend between solid security and moo vitality utilize, which is imperative for WSNs. So, utilizing discrete science within the creation of cryptographic calculations not as it were makes WSNs more secure, but it moreover makes a difference them work more productively, making beyond any doubt that communication is dependable and secure in extreme settings.

References

[1] I. Makarenko, S. Semushin, S. Suhai, S. M. Ahsan Kazmi, A. Oracevic and R. Hussain, "A Comparative Analysis of Cryptographic Algorithms in the Internet of Things," 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), Moscow, Russia, pp. 1-8 (2020).

[2] S. F. Aghili, M. Ashouri-Talouki and H. Mala, "Dos impersonation and de-synchronization attacks against an ultra-lightweight rfid mutual authentication protocol for iot", *The Journal of Supercomputing,* vol. 74, no. 1, pp. 509-525 (2018).

[3] R. E. Navas, H. Le Bouder, N. Cuppens, F. Cuppens and G. Z. Papadopoulos, "Do not trust your neighbors! a small iot platform illustrating a man-in-the-middle attack", *International Conference on Ad-Hoc Networks and Wireless*, pp. 120-125 (2018).

[4] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in iot security: Current solutions and future challenges", *IEEE Communications Surveys Tutorials,* pp. 1-1 (2020).

[5] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl and A. Biryukov, "Triathlon of lightweight block ciphers for the internet of things", *Journal of Cryptographic Engineering,* vol. 9, no. 3, pp. 283-302 (2019).

[6] D. A. Saraiva, V. R. Q. Leithardt, D. de Paula, A. Sales Mendes, G. V. González and P. Crocker, "Prisec: Comparison of symmetric key algorithms for iot devices", *Sensors,* vol. 19, no. 19, pp. 4312 (2019).

[7] J. C. Gonzalez-Arango, D. C. Ocampo-Munera, L. F. Castano-Londono, G. D. Goez-Sanchez and R. A. Velasquez-Velez, "Performance Evaluation of Symmetric Cryptographic Algorithms in resource constrained hardware for Wireless Sensor Networks," in *IEEE Latin America Transactions*, vol. 19, no. 10, pp. 1632-1639 (Oct. 2021).

[8] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, "Blockchain technology in pharmaceutical supply chain: Ensuring transparency, traceability, and security," *Journal of Statistics and Management Systems*, vol. 27, no. 2, pp. 417–428 (2024), doi: 10.47974/JSMS-1266.

[9] P. Zeng, B. Pan, K.-K. R. Choo and H. Liu, "MMDA: Multidimensional and multidirectional data aggregation for edge computing-enhanced IoT", *J. Syst. Arch.,* vol. 106, no. 101713, pp. 101713 (2020).

[10] X. Zuo, L. Li, H. Peng, S. Luo and Y. Yang, "Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid", *IEEE Syst. J.,* vol. 15, no. 1, pp. 395-406 (2021).

[11] M. M. Abbas, O. R. Merad-Boudia and S. Gasmi, "Secure Multidimensional Data Aggregation in IoT-Fog Environments using ECIES," 2022 First International Conference on Computer Communications and Intelligent Systems (I3CIS), Jijel, Algeria, pp. 7-12 (2022).

[12] P. Kasyoka, M. Kimwele and S.M. Angolo, "Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography", *Engineering Reports,* vol. 2, no. 7, pp. 1-15 (2020).

[13] D. Dhabliya, S. Kunche, S. Dingankar, S. S. Dari, R. Dhabliya, and V. Khetani, "Blockchain technology as a paradigm for enhancing cyber security in distributed systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 729–740 (2024), doi: 10.47974/JDMSC-1923.

Received November, 2024