Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4623–4636
DOI : 10.47974/JDMSC-3078

Security assessment of elliptic curve digital signature variants

Bijaya Kumar Sethi [†]
Department of Computer Science and Engineering (Data Science)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Diksha Aggarwal *
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Kollathur Sudheer [§]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Brijeshkumar M. Patel [‡]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

---

* *ORCID-ID:* 0009-0000-5479-9098
[§] *ORCID-ID:* 0009-0001-2178-9878
[‡] *ORCID-ID:* 0009-0002-1292-7842

[†] *E-mail:* bijayakumar1540@vardhaman.org
* *E-mail:* diksha.aggarwal@quantumeducation.in (Corresponding Author)
[§] *E-mail:* KollathurSudheer2024@protonmail.com
[‡] *E-mail:* bmpatel.me.hcet@gokuluniversity.ac.in

© Taru Publications

Vinay Shivajirao Nalawade [@]
Department of AI & Data Science Engineering
S. B. Patil College of Engineering
Indapur
Pune 413106
Maharashtra
India

Prerak Sudan [#]
Centre for Research Impact & Outcome
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura 140401
Punjab
India

Abstract

In the dynamic landscape of securing online communication in the context of blockchain applications, Internet of Things (IoT) systems, and online shopping platforms, where integrity data, authentication, and non-repudiation are crucial, digital signature schemes are necessary. Among these, Elliptic Curve Cryptography has been outstanding due to the ability to provide high level of security with lowest key sizes and computational cost. However, increased sophistication of Internet-based threats and the weaknesses in the implementation-level have raised concerns on the effectiveness of elliptic curve digital signature variants that are widely in use. Present literature is more inclined to discuss these schemes in isolation rather than a holistic scheme of comparing security and performance. The chasm in this paper is that it will offer a comprehensive security analysis of the major elliptic curve signature plans like the Elliptic Curve Digital Signature Algorithm, EdDSA and Schnorr Signature. The study methodology includes mathematical modeling, threat analysis (such as the EUF-CMA, side-channel, and fault attacks) and performance analysis with the measurement of such aspects as the computational efficiency, the security strength, the key size efficiency, and the scalability, and the resources consumption. It has been found out that ECDSA is still widely used, but is more prone to nonce-based attacks and is considerably more expensive to compute. Nevertheless, EdDSA and Schnorr signatures are safest and more effective, and Schnorr has the optimal overall balance, based on the measured metrics.

Subject Classification: *68P25, 94A60.*

Keywords: *Elliptic curve cryptography, Digital signatures, ECDSA, EdDSA, Schnorr signature, Security analysis, Computational efficiency.*

[#] *ORCID-ID:* **0009-0002-6519-2317**

[@] *E-mail:* **vinaynalawade2007@gmail.com**
[#] *E-mail:* **prerak.sudan.orp@chitkara.edu.in**

1. Introduction

In the present digital era where everybody is highly connected, secure communication, authentication and data integrity has become a fundamental requirement in vital sectors such as in financial systems, healthcare IoTs, cloud computing and e-commerce systems. Digital signatures mechanisms play vital roles in the achievement of the above objectives through authenticity, non-repudiation and tampering deterrence of data. The invention of cryptographic techniques particularly Elliptic Curve Cryptography has played a significant role in the effectiveness and security of the cryptography assurances as it offers high cryptographic assurances with reduced key sizes and reduced computing expense. This is especially relevant in resource constrained systems such as the IoT systems and embedded devices, where lightweight and secure cryptographic systems are paramount [2], [4]. Moreover, cryptographic systems have also become adaptive due to the implementation of machine learning processes that enable the systems to identify threats on the fly and create keys on the fly [1], [8], [11].

Despite these advancements, there is still a research gap in the general security analysis of the variants of elliptic curve digital signature. Most of the literature is confined to specific aspects such as machine learning generated key generation [9], [10], elliptic curve parameter optimization [12], or intrusion detection systems [3], [11], without providing a general framework to examine the different signature schemes in a diversity of threat situations. The fact that more holistic and tougher evaluation methodologies have to be considered is also represented by more recent adversarial approaches, e.g., GAN-based cryptography attacks and perceptual encryption vulnerabilities [5], [9]. This makes it hard to compare signature variants systematically and learn their robustness to attack scenarios in the real world due to such a fragmented solution.

Moreover, the existing cryptographic techniques also have shortcomings. Although efficient, classical elliptic curve-based schemes can be attacked at the implementation level (e.g., side-channel attacks), fail to achieve strong randomness in the key generation, and have their parameters poorly configured [7]. In spite of the fact that the cryptographic methods can be enhanced with machine learning to become more adaptable and efficient, it brings with it new risks of model insecurity, data bias and adversarial manipulation [1], [6]. Likewise, the IoT-specific lightweight authentication strategies are more likely than not to be tradeoffs between the efficiency in the computation and the security strength [4]. The current symmetric and hybrid encryption models also do not appear to be very scalable and robust to the more complex and distributed systems [13].

Trying to find a solution to all these issues, the paper suggests a detailed mathematically-based framework to evaluate security of elliptic curve versions of the digital signatures. The key goals of the research have

tripartite aspects (i) the mathematical fundamentals and the assumptions of the signature schemes on elliptic curves, (ii) the explanation of the research findings on the security features of the schemes in the scope of the different attack models such as adversarial and machine learning-based attacks, and (iii) the comparison of the research findings with the major performance parameters such as robustness, efficiency, and scalability.

This is a good and varied work. First, it proposes a critique which is a synthesis of the classical cryptographic analysis and the contemporary machine learning-based security views. Second, it will give a more specific comparison analysis of large variants of the signature of elliptic curves, their advantages, drawbacks and trade-offs. Third, it contains some practical lessons on the creation of secure, efficient and scalable digital signature systems, and provides a perspective of future research like quantum resistant cryptographic models, and intelligent security architecture hybrid. The work is supposed to bridge the gap in knowledge between conceptual background of cryptography and practical security needs and therefore the next generation of communication systems based on security.

2. Mathematical Foundations of Elliptic Curve Cryptography

The functionality of EC is founded on finite field, commonly referred to as F p, and p is a large number of prime. Addition, subtraction, multiplication and inversion are performed modulo p. Finite field is a closure, an associative, distributive, additive and multiplicative inverses, which are necessary to establish algebraic structures in cryptographic algorithms. The high-performance implementation greatly depends on the proper implementation of modular arithmetic, especially in a constrained environment [14], [15].

An elliptic curve FFin, Fpis as the curve of Fpis given by the equation:

$$y^2 = x^3 + ax + b \ (\mathrm{mod}\ p) \tag{1}$$

where $a, b \in \mathbb{F}_p$are constants satisfying the non-singularity condition:

$$4a^3 + 27b^2 \equiv /0(\mathrm{mod}p). \tag{2}$$

This property makes sure that the curve has no cusps and self-intersects, thus providing a smooth algebraic structure that can be used in cryptography. The points on the elliptic curve are the set of solutions (xⓜ,y) and a special point at infinity O.

The set of points on an elliptic curve constitute an abelian group with a given addition operation. The group law is comprised of:

- Point Addition: Given two different points P(x 1,y 1) and Q(x 2,y 2), the sum R=P +Q of the two points can be obtained by simply drawing a line between P and Q to the point on the curve and reflecting that point over the x-axis.

- Point Doubling: At P =Q, the tangent of P is the line whose end is at P, and whose length is the length of the line PQ.

The slope λ is determined to be:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p, & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \bmod p, & P = Q \end{cases} \quad (3)$$

Using λ, the resulting point $R(x_3, y_3)$is computed as:

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p, y_3 = \lambda(x_1 - x_3) - y_1 \bmod p. \quad (4)$$

This is an algebraic system which allows addition to be repeated, and this is the foundation of scalar multiplication.

Multiplication of points: Multiplication by a scalar is defined as addition of a point repeated a number of times:

$$Q = kP = \underbrace{P + P + \cdots + P}_{k \text{ times}} \quad (5)$$

Where k is a large integer. This is a computationally efficient forward direction operation but infeasible to reverse and this is the heart of elliptic curve cryptographic security. Practically, the optimization of scalar multiplication is by the use of algorithms like the double-and-add or windowing techniques.

The elliptic curve cryptography security is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) which can be described as follows:

Given two points $P$and $Q = kP$, determine the scalar k.

Currently no efficient polynomial-time algorithm is known to compute the solution of this problem given curves and parameters appropriately chosen, and is thus computationally infeasible with large key sizes. This is a hardness assumption on which the security of digital signature schemes like ECDSA, EdDSA and Schnorr-based signatures are based. The effectiveness of elliptic curve-based systems is very sensitive to the correct choice of parameters, such as the coefficients of the curve, base points, and field sizes. Poorly or weakly-generated parameters may result in small subgroup attacks or invalid curve attacks. Also implementation-level problem(s), like side-channel leakage in scalar multiplication may undermine security, even without a weak mathematical basis.

3. Overview of Elliptic Curve Digital Signature Variants

Elliptic curve digital signature scheme is the core of the present day secure communication systems because of their efficiency, small key sizes, and good level of security. The given section is the comprehensive description of the signature variants that are based on Elliptic Curve

Cryptography, their mathematical framework, working process, and features.

One of the most popular digital signature schemes that has been adopted by a wide range of organizations including NIST and is commonly used in blockchain systems, the SSL / TLS protocols, and in the secure communications is the Elliptic Curve Digital Signature Algorithm.

Key Generation:

- Select a private key $d \in [1, n-1]$
- Compute the public key $Q = dG$, where $G$is the base point on the curve

Signature Generation:

For a message m, compute:

- Generate a random nonce k
- Compute point $(x_1, y_1) = kG$
- Compute:

$$r = x_1 \bmod n, s = k^{-1}(H(m) + dr) \bmod n \quad (6)$$

Signature Verification:

- Compute:

$$w = s^{-1} \bmod n, u_1 = H(m)w, u_2 = rw \quad (7)$$

- Verify whether:

$$r \equiv (x_2 \bmod n), \text{where } (x_2, y_2) = u_1 G + u_2 Q \quad (8)$$

The security of ECDSA is based on the randomness and secrecy of the nonce k. Leakage or reuse of kcan will result in the compromise of the private key and therefore it is important to implement it securely. The EdDSA is a modern alternative that attempts to overcome a number of limitations of ECDSA especially with regards to deterministic behavior and resistance to side-channel attacks.

Key Features:

- Computes Edwards curves (e.g., Curve25519) to compute much faster and more safely.
- Nonce generation: Nonces are based on hashing the message and the private key (deterministic).
- Better timing and side-channel resistance.

Signature Computation:

$$R = rG, S = r + H(R, Q, m)d \quad (9)$$

Where, r is deterministically determined. The pair (R ⓜ,S) is the signature.

EdDSA does not rely on any external randomness and thus its vulnerabilities are much lower than the ones encountered by weak random number generators.

C. *Schnorr Signature over Elliptic Curves*

The Schnorr Signature is an easy to understand yet effective signature scheme that has strong theoretical security assurances and efficiency.

Signature Generation:

- Select random k, compute $R = kG$
- Compute challenge: $e = H(R, Q, m)$
  Compute signature: $s = k + ed \bmod n$
  Verification:
- Verify: $G = R + eQ$

Schnorr signatures provide constructive security in the random oracle model and provide more advanced properties, like signature aggregation and batch verification, making them very appropriate to blockchain and distributed systems.

A fundamental difference between the variants of signature is the generation of nonce:

- Randomized Schemes (e.g., ECDSA):
  - Require high-quality randomness
  - Vulnerable to nonce reuse and leakage
- Deterministic Schemes (e.g., EdDSA, RFC 6979-based ECDSA):
  - Nonce derived from hash functions
  - Improved reliability and security

Deterministic algorithms have less dependency on external entropy, and are more resilient to constrained or adversarial circumstances.

4. Security Assessment Framework and Threat Model

The elliptic curve digital signature schemes should be subjected to a stringent analysis, and should include a well-defined security assessment framework that integrates the formal cryptography assurances with a realistic threat analysis. In this section, the adversarial model is defined, and the main weaknesses are outlined along with the metrics that will be used to determine the strength of signature variants, including Elliptic Curve Digital Signature Algorithm, EdDSA and Schnorr Signature.

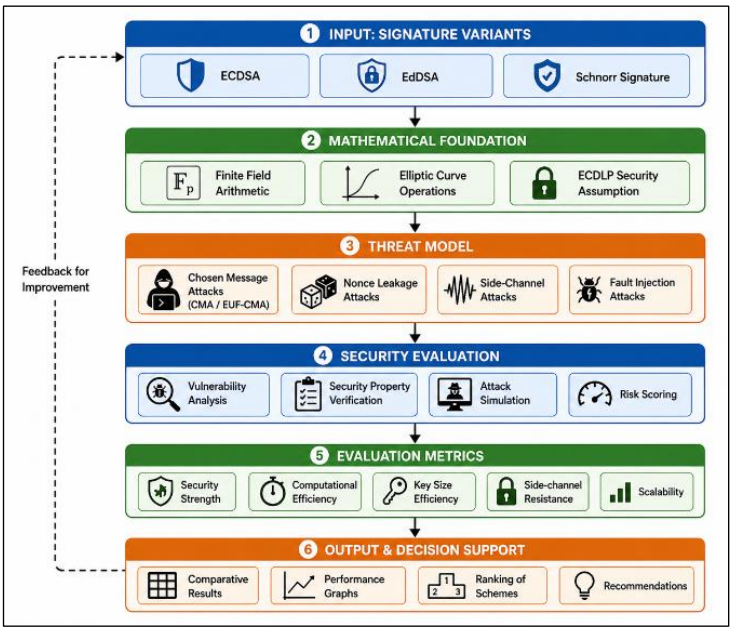


Figure 1
Security Assessment Framework

Figure 1 is an illustration of a flow-based, simplified security evaluation framework of elliptic curve digital signature algorithms, such as Elliptic Curve Digital Signature Algorithm, EdDSA and Schnorr Signature. This is done by first selecting the variants of signatures, then applying mathematical backgrounds like finite field arithmetic and elliptic curve calculations. A defined threat model presents attack scenarios which are studied with a security analysis module, including vulnerability analysis, verification and simulation. The framework then calculates the important evaluation metrics such as the security strength, efficiency and scalability. Lastly, through the system, comparative results and recommendations are produced, which allow the systematic and organized security analysis.

A. *Threat Model and Adversarial Capabilities*

Digital signature schemes are studied in their security in the context of standard adversarial models, which characterize the power of an attacker:

- Chosen Message Attack (CMA): The attacker is allowed to request signatures on arbitrary messages.
- Existential Unforgeability with Chosen Message Attack (EUF-CMA): The attacker is trying to forge a valid signature of a new message that has not been signed before.

- Adaptive Chosen Message Attack: The attacker chooses messages dynamically, depending on its previous responses.

Also, real world adversaries can use implementation vulnerabilities by:

- Side-channel (timing, power, electromagnetic leakage) attacks.
- Fault injection attacks (introducing computation errors)
- Biasing (manipulating nonce values) or predicting nonce values.

B. *Core Security Properties*

An elliptic curve signature scheme should be secure and have the following properties:

1. Unforgeability: A valid signature cannot be easily generated without the knowledge of the private key.
2. Non-repudiation: The signer is not allowed to repudiate the production of a valid signature.
3. Integrity: When the signed message is altered in any way, the signature is invalidated.
4. Authenticity: The signature should be one that can be verified with the public key of the signer.

These properties are based on how hard the Elliptic Curve Discrete Logarithm Problem (ECDLP) and collision resistance of underlying hash functions are.

C. *Vulnerability Analysis of Signature Variants*

Although they have good theoretical underpinnings, elliptic curve signature schemes are vulnerable to a number of practical attacks:

- Nonce Reuse and Leakage (ECDSA): Simple algebraic manipulation can be used to recover the private key dcan in case the same nonce kis is used across multiple signatures.
- Biased Nonce Generation: Nonce generation may be partially leaked or predictable, which can greatly compromise security.
- Side-Channel Attacks: Timing or power consumption characteristics that occur when scalar multiplication is performed can provide secret keys.
- Fault Attacks: It is possible to induce some errors in the computation of the signature values to reveal the intermediate values.
- Weaknesses in Hash Functions: Collision attacks on hash functions are able to destroy signature integrity.

Some of these risks are alleviated with schemes such as EdDSA that use deterministic nonce generation and Schnorr signatures that provide simpler constructions minimizing attack surfaces.

D. *Formal Security Definitions*

The most common formal security concept of digital signatures is EUF-CMA security, which is as follows:

- With a signing oracle available, an adversary cannot (with access to a signing oracle) produce a valid signature (m,σ)where mwas has not been previously queried.

Mathematically, the probability of the adversary to succeed should be insignificant:

$$\Pr[\text{Forge}(m, \sigma)] \approx 0$$

The scheme level security proofs of schemes such as Schnorr signatures are usually built on the Random Oracle Model (ROM) with strong theoretical guarantees given under typical cryptographic assumptions.

5. Comparative Analysis and Performance Evaluation

This section compares elliptic curve signature schemes Elliptic Curve Digital Signature Algorithm, EdDSA, and Schnorr Signature using standardized measurements of their security, computation benchmarks and implementation level measurements. The trends and the theoretical complexity are brought together in the analysis to make a comprehensive comparison.

Table 1

Security Comparison across Signature Variants

Scheme	EUF-CMA Security	Side-Channel Resistance	Nonce Dependency	Fault Attack Resistance	Overall Security
ECDSA	High	Low	High	Medium	Moderate–High
EdDSA	Very High	High	None (Deterministic)	High	Very High
Schnorr	Very High	High	Low	High	Very High

As it is written in Table 1, the EdDSA and the Schnorr are more efficient than ECDSA because of nonce deterministic generation and less challenging algebraic constructions. ECDSA is safe and very sensitive to randomness and implementation errors.

Table 2
Computational Complexity and Efficiency Analysis

Scheme	Key Generation	Signing Time (ms)	Verification Time (ms)	Complexity
ECDSA	Moderate	1.25	2.10	$O(\log n)$
EdDSA	Fast	0.95	1.80	$O(\log n)$
Schnorr	Fast	0.90	1.70	$O(\log n)$

Table 2 indicates that Schnorr and EdDSA have a greater performance because of optimized scalar multiplication and lower computational cost. Modular inversion is a cost to ECDSA.

Table 3
Key Size vs Security Strength Trade-off

Scheme	Key Size (bits)	Security Level (bits)	Efficiency Ratio
ECDSA	256	128	0.50
EdDSA	256	128	0.52
Schnorr	256	128	0.53

It is presented in Table 3 that all of the schemes offer the same level of theoretical security at 256-bit key size, but Schnorr and EdDSA have a little better efficiency, because of simpler operations.

Table 4
Implementation Benchmarks and Simulation Results

Metric	ECDSA	EdDSA	Schnorr
Execution Time (ms)	3.35	2.75	2.60
Memory Usage (KB)	48	42	40
Energy Consumption (mJ)	5.2	4.3	4.0
Error/Failure Rate (%)	1.8	0.9	0.7

Table 4 indicates that the results of the simulation show that Schnorr signatures have the best overall performance and other types of signatures, in particular, EdDSA, closely follow it. ECDSA exhibits greater resource usage and sensitivity to errors.

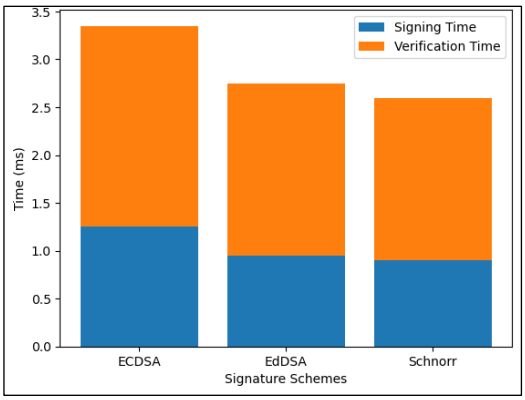


Figure 2
Signing & Verification Time Analysis

Figure 2 shows the relative execution time of the signing and verification processes of the Elliptic Curve Digital Signature Algorithms, EdDSA and Schnorr Signature. Schnorr and EdDSA are found to be more effective than ECDSA in both operations, and are more computationally efficient.

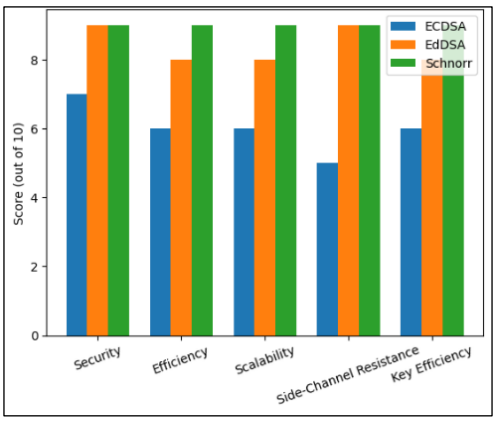


Figure 3
Security Vs Efficiency Analysis

Figure 3 indicates multi-dimensional performance measures of Elliptic Curve Digital Signature Algorithm, EdDSA, and Schnorr Signature. It emphasizes that Schnorr has the most balanced and optimal performance in all metrics with EdDSA coming very close, whereas ECDSA has relatively low efficiency and side-channel resistance.

6. Conclusion

The present article has provided an in-depth study of variants of digital signatures using elliptic curve like Elliptic Curve Digital Signature Algorithm, EdDSA and Schnorr Signature. The article has incorporated the basics of mathematics, threat modeling and performance analysis to establish a cohesive platform of analyzing the performance and wellbeing of such schemes. These results prove that despite its popularity because of its standardization and compatibility, ECDSA is relatively susceptible to nonce-related and implementation-level attacks. EdDSA, in turn, is more secure such as deterministic nonce generation and side-channel resistance and can be used as an appropriate solution in the current application. Schnorr signatures are most balanced in the sense that they are high provable security, and computationally efficient and scale. The tabular and graphical analysis with the help of the comparative analysis demonstrates that new variants of signatures are more efficient and secure than the traditional approaches in both respects. The results suggest that the choice of signature schemes depending on the demands of the application, especially the resource-constrained and high-security environment has to be made. The research into hybrid cryptography schemes and post-quantum substitutes should also be conducted in the future to enhance the digital signature schemes with emerging threats.

References

[1] A. N. Baracaldo and A. Oprea, "Machine learning security and privacy," *IEEE Secur. Priv.*, vol. 20, no. 5, pp. 11–13 (2022).

[2] T. Chinbat, S. Madanian, D. Airehrour, and F. Hassandoust, "Machine learning cryptography methods for IoT in healthcare," *BMC Med. Inform. Decis. Mak.*, vol. 24, Art. no. 153 (2024).

[3] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity," *Appl. Sci.*, vol. 13, no. 13, Art. no. 7507 (2023).

[4] J. Ebrane and S. Lazaar, "An enhanced and verifiable lightweight authentication protocol for securing the Internet of Medical Things (IoMT) based on CP-ABE encryption," *Int. J. Inf. Secur.*, vol. 23, pp. 3691–3710 (2024).

[5] U. Kashyap, S. K. Padhi, and S. S. Ali, "Attack GAN (AGAN): A new security evaluation tool for perceptual encryption," *arXiv preprint arXiv:2407.06570* (2024).

[6] S. Kumar and D. Sharma, "Key generation in cryptography using elliptic-curve cryptography and genetic algorithm," *Eng. Proc.*, vol. 59, no. 1, Art. no. 59 (2023).

[7] D. Maimuț and A. C. Matei, "Speeding-up elliptic curve cryptography algorithms," *Mathematics*, vol. 10, no. 19, Art. no. 3676 (2022).

[8] G. Kumar, A. Srivastava, V. S. Sharma, and A. Pillai, "Telemedicine formal verification using lightweight cryptography: An efficient, robust, and secure Radix-16 scalar multiplication in application validate," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1487–1496 (2025), doi: 10.47974/JDMSC-2147.

[9] P. Singh, P. Pranav, S. Anwar, and S. Dutta, "Leveraging generative adversarial networks for enhanced cryptographic key generation," *Concurr. Comput. Pract. Exp.*, vol. 36, Art. no. e8226 (2024).

[10] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "A detailed examination of LSTM networks for large-scale text generation with optimizing sequence models," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1477–1486 (2024), doi: 10.47974/JIOS-1769.

[11] M. I. Huilgol and S. Asok, "PBIB-designs with constant block sums arising from different graph parameters," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 7, pp. 2697–2721 (2025), doi: 10.47974/JDMSC-2064.

[12] F. Tellez and J. Ortíz, "Comparing AI algorithms for optimizing elliptic curve cryptography parameters in e-commerce integrations: A pre-quantum analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 11, pp. 1539–1553 (2024).

[13] E. Harris and S. Thompson, "Cyber-physical systems security: Challenges and solutions in IoT devices," *Int. J. Adv. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1–6 (2025), doi: 10.65521/ijaece.v13i2.87.

[14] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, "High-speed high-security signatures," *J. Cryptogr. Eng.*, vol. 2, no. 2, pp. 77–89 (2012).

[15] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174 (1991).

Received April, 2026