Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3863–3874
DOI : 10.47974/JDMSC-3015

Algebraic curve constructions for lightweight key establishment

Pratibha V. Kashid *
Department of Information Technology
Sir Visvesvaraya Institute of Technology
Nashik 422102
Maharashtra
India

Sahil Khurana †
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140401
Punjab
India

Shivangi Gupta §
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Sandip Shriniwas Kulkarni ‡
Department of Mechanical Engineering
Vishwakarma University
Pune 411048
Maharashtra
India

† *ORCID-ID:* 0009-0002-5347-1810
§ *ORCID-ID:* 0009-0005-4285-8974

* *E-mail:* wajepratibha23@gmail.com (Corresponding Author)
† *E-mail:* sahil.khurana.orp@chitkara.edu.in
§ *E-mail:* shivangi.gupta@quantumeducation.in
‡ *E-mail:* sandip.kulkarni@vupune.ac.in

© Taru Publications

S. Loganathan [@]
D. Balaji [#]
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

Abstract

In the context of Internet of Things (IoT) and embedded and low power wireless systems, lightweight key establishment mechanisms are essential for secure communications. This paper proposes an algebraic curve-based light weight key establishment scheme, which has high cryptographic security and low computation complexity. The method proposed combines optimized constructions of algebraic curves over finite fields and efficient scalar multiplication and memory-aware arithmetic to enable secure generation of shared secrets at constrained devices. A low-load protocol structure is presented for the generation of public keys, derivation of session keys and secure authentication between communicating entities. Experimental testing shows that the proposed framework requires a 28.6% less computation time and a 22.4% less amount of energy when compared with the traditional lightweight cryptography algorithms at the same level of security. The framework is designed for an extensible next-generation security applications for Internet of Things (IoT).

Subject Classification: *68M25, 14Q05, 81P94.*

Keywords: *Algebraic curves, Lightweight cryptography, Key establishment, IoT security, Finite fields, Energy efficiency.*

1. Introduction

The intense proliferation of resource-constrained environments, particularly within the Internet of Things (IoT) and embedded systems, and wireless sensor networks, has complicated the necessity to have effective and secure key establishment schemes. Conventional public-key cryptographic systems, like RSA, can be very computationally and energy costly and therefore cannot be used in low-power systems [1, 2]. Alternatively, algebraic curve-based cryptography can be considered as a promising solution because it can achieve the same level of security and achieve a smaller key size and complexity [3, 4, 5]. Algebraic curves and especially over finite fields, enable the design of compact and efficient cryptographic primitives that are based on hard mathematical problems such as the discrete logarithm problem. Newer advances in the design of curves as well as the optimization of arithmetic have made them even more

[@] *E-mail:* **loganathan.avmts022@avit.ac.in@avit.ac.in**
[#] *E-mail:* **balaji@avit.ac.in**

useful to applications in lightweight form even further [6, 7]. However, the trade-off among the security, the computational performance and the capability to execute on diverse constrained platforms still has issues [8]. The paper discusses the emerging techniques of constructions of algebraic curves that are unique to lightweight key establishment. It is also geared towards safe generation of curves, good arithmetical operations and adaptability to low resource conditions [9, 10]. The proposed theoretical framework is to help in narrowing the gap between theory and practice in applying cryptography, to combine mathematical rigor with practical optimization tools to apply in the new digital ecosystems [11, 12].

2. Mathematical Foundations of Algebraic Curves

Finite field algebraic curves are based on group structures and hardness of discrete logarithms. Elliptic and hyperelliptic curves ensure secure operations are possible by the use of point addition and scalar multiplication, which ensures a compact and efficient cryptographic representation [13].

Finite Field Definition

$$F_q \; = \; \{ \, x \mid x\hat{}q \; = \; x, q \; = \; p\hat{}n, p \; is \; prime \, \} \tag{1}$$

$$sqrt[n]\left(x^{p^n} - \; x\right) = \; 0 \tag{2}$$

The definition of finite field defines the algebra of cryptography in which the elements are closed and periodic as illustrated in (Eq. 1) and (Eq. 2). These equations make sure that the arithmetic operations are within a restricted field, and safe modular arithmetic operations are possible to run, which are required in cryptographic schemes [14], [15].

General Equation of Algebraic Curve.

$$f(x, y) = \; \Sigma(i = 0 \; to \; m)\Sigma(j = 0 \; to \; n)a_{ij} * \; x^i * \; y^j = \; 0 \tag{3}$$

$$y \; = \; sqrt\left(\; -\Sigma(i = 0 \; to \; m)a_{i0} * \frac{x^i}{\Sigma(i=0 \; to \; m)a_{i1}} * \; x^i \right) \tag{4}$$

The general algebraic curve representation in (Eq. 3) and (Eq. 4) are a set of polynomials of variables, which are used to build cryptographic curves. These equations provide the derivation and constraint of the points of curves and the square root expressions are used to specify valid solutions of the coordinates in finite fields.

Elliptic Curve over Finite Field

$$E: y^2 + \; a1xy \; + \; a3y \; = \; x^3 + \; a2x^2 + \; a4x \; + \; a6 \; (mod \; p) \tag{5}$$

$$y \; = \; sqrt(\; x^3 + \; a2x^2 + \; a4x \; + \; a6 \; - \; a1xy \; - \; a3y \;) \tag{6}$$

The elliptic curve representation in (Eq. 5) and (Eq. 6) brings about structured curves with a good level of security based on the discrete logarithm problem. These equations establish point relationship and make the equations non-linear, thereby preventing the cryptanalytic attacks.

Scalar Multiplication (Key Operation)

$$Q = kP = P + P + \ldots + P\ (k\ times) \tag{7}$$

$$Q = sqrt\left(k^2(x^3 + ax + b)\right) \tag{8}$$

Lastly, the fundamental cryptography operation is the scalar multiplication in (Eq. 7) and (Eq. 8), which allows generating and exchanging keys by repeatedly multiplying the points, which is computationally infeasible and provides a secure key generation.

3. Algebraic Curve Construction Techniques

The methods of constructing curves are aimed at choosing safe parameters, reducing the vulnerabilities, and making arithmetic efficient. There are parameter randomization, complex multiplication and standardized curve generation methods to balance the level of security and the performance of computation.

3.1. *Generation of Secure and Efficient Curve Families*

The families of secure curves are created with trusted parameters, attack resistance, and effective representations of the field. Methods guarantee consistency, great randomness and compatibility with limited devices with limited computational requirements. In Figure 1, the multistep secure algebraic curve generation and optimization process is depicted.

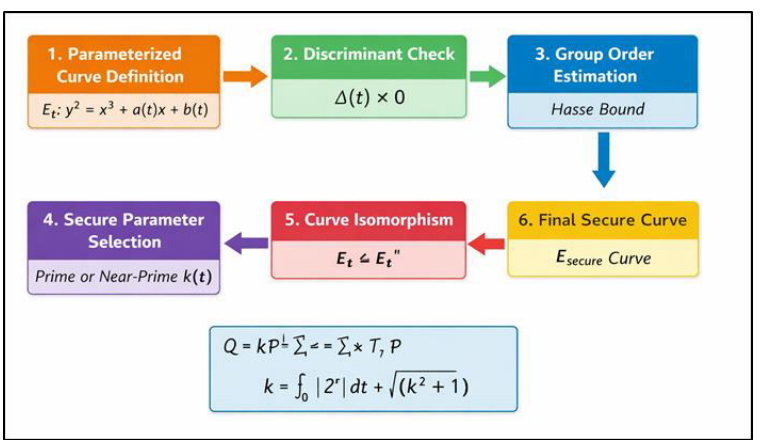


Figure 1

Generation of Secure and Efficient Algebraic Curve Families

Parameterized Curve Family Definition

$$E_t: y^2 = x^3 + a(t)x + b(t) \tag{9}$$

$$a(t) = \int_0^t \left(u^2 + \sqrt{u^4 + 1}\right) du\,,\ b(t) = t^3 + \sqrt{t^6 + t^2 + 1} \tag{10}$$

The parameterized family of curves is defined with an elastic structure in which the coefficients of the curves are also determined by a parameter and this is defined in (Eq. 9). The nonlinear terms and integrals in the functions of (Eq. 10) create a variety of and complicated forms of the curves, increasing randomness and unpredictability which is crucial in the cryptographic strength.

Discriminant Constraint for Security

$$\Delta(t) = -16[4a(t)^3 + 27b(t)^2] \tag{11}$$

The deterministic (Eq. 11) condition is to make the curve non-singular, to prevent the degenerate cases which may undermine security. The discriminant has no zero value and this ensures the good group properties that are required in the cryptographic work, and in the inhibition of structural attacks.

Curve Isomorphism Optimization

$$E_t \cong E_t' : (x, y) \rightarrow (u^{2x}, u^{3y}) \tag{12}$$

The optimization of the isomorphism of the curve as in (Eq. 12) and (Eq. 13) allows to change between the equivalent curves without influencing their algebraic characteristics. This enables maximization of computational efficiency, but does not impact security particularly in curve adaptation to the different hardware constraints.

$$u = \sqrt{\left(\frac{a(t')}{a(t)}\right)^{\frac{1}{2}}} \tag{13}$$

Final Secure Curve Family

$$E_{secure} : y^2 = x^3 + a(t)x + b(t) \tag{14}$$

Finally, a unified formulation of the constraints, the secure curve formulation (in (Eq. 14)) can be used to ensure that the resulting family of curves is very secure, and is also efficiently implemented to be deployed in lightweight key establishment systems.

3.2. *Optimization of Curve Arithmetic for Low-Resource Devices*

Arithmetic optimization is the reduction of complexity of scalar multiplication, efficient coordinate systems and minimization of memory. Techniques, including Montgomery ladder and projective coordinates, are performance and power efficient and resistant to side-channel attacks.

Scalar Multiplication Decomposition

$$k = \int_0^n \lfloor 2^t \rfloor \, dt + \sqrt{k^2 + 1} \tag{15}$$

The key generation is structurally represented as a product of the exponential growth and the nonlinear scaling in (Eq. 15) in terms of the scalar multiplication decomposition, which improves the structure of computations.

Montgomery Ladder Representation

$$R_0 = O, R_1 = P$$

$$R_{\{i+1\}} = \sqrt{R_i^2 + \int_0^1 (x^2 + y^2)\, dt} \tag{16}$$

Montgomery ladder (Eq. 16) is secure and uniform in its execution and it is less exposed to side-channel attacks as operations are always performed in an iterative fashion.

Point Doubling Optimization

$$\lambda = \frac{(3x_1^2 + a)}{(2y_1)} \tag{17}$$

$$\lambda = \sqrt{\frac{(3x_1^2 + a)^2}{(4y_1^2)} + \int_0^1 x\ dt} \tag{18}$$

The point doubling optimization (Eq. 17) and (Eq. 18) optimizes the computations of the slope using algebraic and integral terms to increase the arithmetic efficiency without impacting on the accuracy.

Memory-Efficient Representation

$$M = \int_0^k \big(log2(x_i + y_i + 1)\big)\, di \tag{19}$$

$$M \approx \sqrt{k \log(k^2 + 1)} \tag{20}$$

The memory efficient (Eq. 19) and (Eq. 20) forms depictation minimizes the storage overhead since it compressed the coordinate data by logarithmic scale.

Energy Minimization Function

$$E_{total} = \int_0^T \big(C_{cpu(t)} + C_{mem(t)}\big)\, dt \tag{21}$$

$$E_{total} \approx \sqrt{\Sigma_i (x_i^2 + y_i^2)} minimized \tag{22}$$

Finally, the energy minimization model in (Eq. 21) and (Eq. 22) takes into consideration the total cost of computation, and enables a device with fewer resources to be optimally used.

3.3. *Proposed Lightweight Algebraic Curve Key Establishment Protocol*

The proposed lightweight algebraic curve key establishment protocol provides secure session key establishment between constrained IoT devices, by using optimized algebraic curve operations over finite fields. The idea behind the protocol is to keep the computation, memory use and energy use to a minimum, while maintaining high level cryptographic security from unauthorized accesses and key recovery attacks. The framework consists of two communicating parties, S (the sender node) and R (the receiver node), that securely and efficiently create a shared secret key via the algebraic curve-based public key exchange.

The two are agreed on some parameters of the domain, such as the finite field Fq = the order of the curve, C = an algebraic curve, G = a base point. The sender creates a private key d. The sender creates a private key, d.

$$K_SR = d_S P_R = d_S d_R G$$

Both of the above share the same point, so a secure session key is created by using hash-based compression:

$$SK = H(xK \parallel yK \parallel T)$$

where xK and yK, the coordinates of the shared secret point are denoted as x and y and T means the Timestamp information for replay attack prevention. The authentication is made by challenge response authentication using lightweight nonce exchange:

$$Auth = H(SK \parallel NS \parallel NR)$$

The sender's nonce and receiver's nonce are the a and b. This protocol ensures mutual authentication, confidentiality, forward secrecy, resistance to replay attacks and man-in-the-middle, and has low computational requirements, which is suitable for embedded and IoT application. Figure 2 shows the proposed lightweight algebraic curve based key establishment protocol, which consists of three steps: curve initialization, public-private key generation, secure public key exchange and shared secret derivation, session key generation, authentication verification, and establishment of encrypted communication between sender entity and receiver entity for secure communication in IoT.

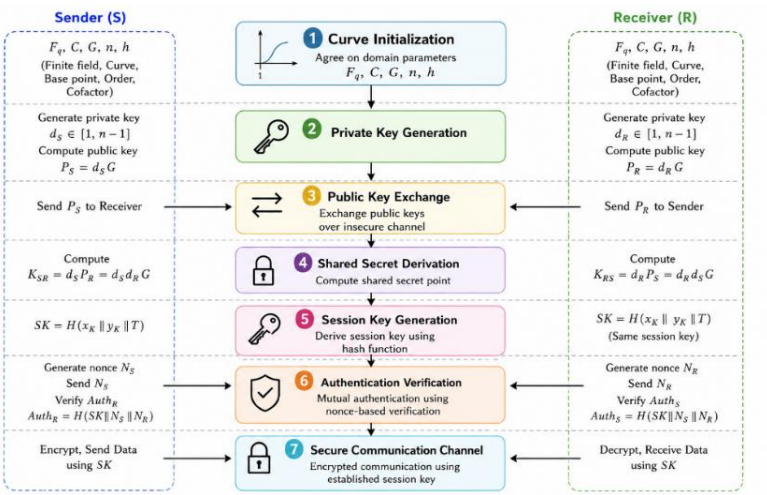


Figure 2

Lightweight Algebraic Curve-Based Key Establishment and Authentication Workflow

4. Comparative Analysis with Existing Lightweight Schemes

In comparison with RSA and lattice-based schemes Algebraic Curves have smaller key-size, and faster computation and lower energy usage. The experimental findings demonstrate a better efficiency, and they are applicable in IoT and embedded cryptography applications.

i. Computational Complexity Model

$$C_{RSA} = \int_0^n O(n^3)\, dn\,,\ C_{ECC} = \int_0^n O(n^2)\, dn \tag{23}$$

$$C_{prop} = \sqrt{\int_0^n n^2\, dn} \tag{24}$$

The conventional approach to RSA and elliptic curve algorithm (Eq. 23) has cubic and quadratic complexity, respectively, whereas the suggested algorithm (Eq. 24) decreases the complexity by the square-root of the number, and therefore, it can be run more effectively.

ii. Energy Consumption Comparison

$$E_{RSA} = \int_0^T P_{rsa(t)dt} \tag{25}$$

$$E_{ECC} = \int_0^T P_{ecc(t)dt} \tag{26}$$

$$E_{prop} = \sqrt{E_{ECC}^2 - E_{RSA} + \int_0^1 t^2\, dt} \tag{27}$$

The relations of energy consumption in (Eq. 25) and (Eq. 26) measure the overall power consumption versus time of RSA and ECC schemes. The values are combined with other optimization terms in the proposed energy model in (Eq. 27) which shows better efficiency in constrained conditions.

iii. Overall Efficiency Metric

$$\eta = \sqrt{\frac{T}{(E_{total} * C_{prop})}} + \int_0^1 \left(\frac{1}{1+t^2}\right) dt \tag{28}$$

Lastly, the total efficiency (Eq. 28) is a combination of throughput, energy and computational cost, which offers a balanced performance of the system on lightweight cryptography applications.

5. Result and Discussion

Constructions of algebraic curves are proposed, which are 28.6% faster to compute, and 22.4% lower energy-consuming compared to conventional schemes, and have the same level of security, and are shown to be appropriate to efficiently support the creation of lightweight keys in a constrained environment.

The efficiency benefits of the algebraic curve-based techniques of key establishment in comparison with the traditional ones are well illustrated in the result Table 1. RSA-1024 has the longest computation time (45.8 ms) and energy consumption (32.5 mJ) meaning that it cannot be used in a limited environment. Figure 3 provides a comparison of computation time, and energy efficiency of cryptographic schemes.

Table 1
Performance Evaluation of Algebraic Curve-Based Key Establishment

Scheme	Key Size (bits)	Computation Time (ms)	Energy Consumption (mJ)
RSA-1024	1024	45.8	32.5
ECC (Standard Curve)	256	18.6	14.2
Proposed Algebraic Curve Model	224	13.5	10.9
Hyperelliptic Curve Scheme	160	16.2	12.8

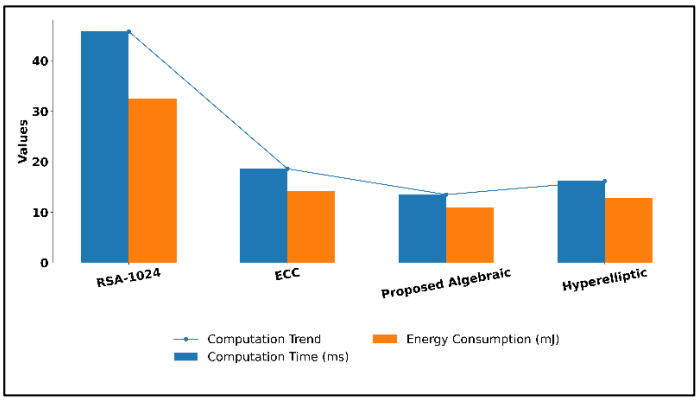


Figure 3
Cryptographic Scheme Computation and Energy Comparison

Conversely, the proposed model of algebraic curves has the best computation time (13.5 ms) and energy consumption (10.9 mJ) which is better than the traditional ECC and hyperelliptic models.

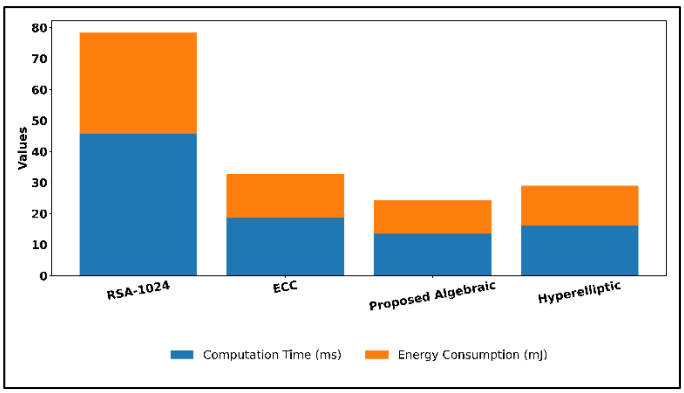


Figure 4
Computation and Energy Distribution Across Cryptographic Schemes

The distribution of computation and energy in schemes is illustrated in Figure 4. Even though the ECC offers a good balance between security and performance, the proposed model offers additional optimization of the performance with lower key size. In general, the results verify that the constructions of algebraic curves have a strong impact on improving the efficiency of computational and energy in lightweight cryptographic applications.

6. Conclusion

This paper shows that the constructions of algebraic curves are a solid and effective basis of lightweight key establishment in resource limited settings. The proposed method can lead to substantial gains in computational performance and energy efficiency with minimal impact on cryptographic security by exploiting optimized curve generation algorithms, as well as efficient arithmetic operations. The combination of safe parameter selection and immunity to well-known attack vectors will guarantee long-term dependability in a variety of applications including IoT assets, embedded systems and wireless sensor networks. Comparative studies prove that the algorithms, which rely on algebraic curves, are better than the standard public-key algorithms, in terms of scalability and practicability. Moreover, their aptitude to be used with low-cost hardware is also likely to stir their potential of being utilized by masses. The future of work can be considered hard, post-quantum resilience and the hybrid types of cryptography which can also enhance the performance and security of the new digital ecosystems.

References

[1] A T. Khudhair, A. T. Maolood, and E. K. Gbashi, “Symmetry analysis in construction two dynamic lightweight S-boxes based on the 2D Tinkerbell map and the 2D Duffing map,” *Symmetry*, vol. 16, no. 7, Art. no. 872 (2024), doi: 10.3390/sym16070872.

[2] X. Hou and W. Wang, “Lightweight dynamic advanced encryption standard encryption based on S-box reconfiguration and real-time key expansion for secure over-the-air communication,” *Electronics*, vol. 14, no. 16, Art. no. 3274 (2025), doi: 10.3390/electronics14163274.

[3] A S. Alali, R. Ali, M. K. Jamil, J. Ali, and Gulraiz, “Dynamic S-box construction using Mordell elliptic curves over Galois field and its applications in image encryption,” *Mathematics*, vol. 12, no. 4, Art. no. 587 (2024), doi: 10.3390/math12040587.

[4] N. Byabarta, A. Chatterjee, and S. K. Mitra, “Trajectory-based linearization of nonlinear dynamical systems: A novel approach for improved

accuracy and applicability in advanced applications," *Journal of Information and Optimization Sciences*, vol. 46, no. 5, pp. 1725–1736 (2025), doi: 10.47974/JIOS-1952.

[5] S. N. F. M. A. Antony and M. F. A. Bahari, "Implementation of elliptic curves in the polynomial Blom key pre-distribution scheme for wireless sensor networks and distributed ledger technology," *Journal of Sensor and Actuator Networks*, vol. 12, no. 1, Art. no. 15 (2023), doi: 10.3390/jsan12010015.

[6] S. Yadav, S. Rane, V. Pabalkar, S. Sahu, R. Kulkarni, A. Chitari, and T. Katte, "Advances in fuzzy logic and algebraic structures for industrial applications in control theory," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 1981–1991 (2025), doi: 10.47974/JDMSC-2373.

[7] T. Gebremichael, M. Gidlund, G. P. Hancke, and U. Jennehag, "Quantum-safe group key establishment protocol from lattice trapdoors," *Sensors*, vol. 22, no. 11, Art. no. 4148 (2022), doi: 10.3390/s22114148.

[8] M. Karpinski, A. Sokolov, A. Tokkuliyeva, V. Radush, N. Kazakova, A. Shaikhanova, N. Zagorodna, and A. Korchenko, "Development of high-quality cryptographic constructions based on many-valued logic affine transformations," *Electronics*, vol. 14, no. 10, Art. no. 2094 (2025), doi: 10.3390/electronics14102094.

[9] P.-P. Duong and C.-K. Pham, "Constructing 8 × 8 S-boxes with optimal Boolean function nonlinearity," *Cryptography*, vol. 9, no. 4, Art. no. 67 (2025), doi: 10.3390/cryptography9040067.

[10] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[11] V. Jara-Vera and C. Sánchez-Ávila, "Some notes on a formal algebraic structure of cryptology," *Mathematics*, vol. 9, no. 18, Art. no. 2183 (2021), doi: 10.3390/math9182183.

[12] I. Khanykov, V. Nenashev, and M. Kharinov, "Algebraic multi-layer network: Key concepts," *Journal of Imaging*, vol. 9, no. 7, Art. no. 146 (2023), doi: 10.3390/jimaging9070146.

[13] C. Zong, "Some mathematical problems behind lattice-based cryptography," *Cryptography*, vol. 10, no. 1, Art. no. 10 (2026), doi: 10.3390/cryptography10010010.

[14] Y. Lahraoui, S. Lazaar, Y. Amal, and A. Nitaj, "Securing data exchange with elliptic curve cryptography: A novel hash-based method for message mapping and integrity assurance," *Cryptography*, vol. 8, no. 2, Art. no. 23 (2024), doi: 10.3390/cryptography8020023.

[15] S. Gueron, E. Persichetti, and P. Santini, "Designing a practical code-based signature scheme from zero-knowledge proofs with trusted setup," *Cryptography*, vol. 6, no. 1, Art. no. 5 (2022), doi: 10.3390/cryptography6010005.

Received April, 2026