Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4397–4406
DOI : 10.47974/JDMSC-3060

Efficient scalar multiplication algorithms on elliptic curves over prime fields for resource-constrained cryptographic devices

M. Sreenivasa Reddy [†]
Department of Mechanical Engineering
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Fazil Hasan *
Department of Agriculture
Noida International University
Greater Noida 203201
Uttar Pradesh
India

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

Shivam P. Chaudhary [‡]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

[†] *E-mail:* dypc@adityauniversity.in
* *E-mail:* fazil@niu.edu.in (Corresponding Author)
[§] *E-mail:* shivangi.gupta@quantumeducation.in
[‡] *E-mail:* shivamchaudhary@gokuluniversity.ac.in

© Taru Publications

Manisha Sagar Pawar [@]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Shaziya Islam [#]
Department of Computer Science & Engineering
Rungta College of Engineering & Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

Abstract

Although Elliptic Curve Cryptography (ECC) over prime fields is computationally efficient in many cryptographic operations, scalar multiplication remains a computational bottleneck, particularly in resource-constrained devices such as IoT nodes and embedded systems. The paper addresses the issue of decreasing the computation time, memory and energy usage and maintaining the cryptographic security. It is proposed to use a hybrid optimization system that is based on windowed techniques, Montgomery ladder to perform periodically and parallelized arithmetical operations. Its algorithm allows it to use optimized modular arithmetic and reduced point operations to achieve maximum performance. Experimental results indicate that the time of scalar multiplication is decreased by 34.8 percent, additions of points are decreased by 28.5 percent, and the amount of energy used is lowered by 22.7 percent when traditional methods of double-and-add are used. The proposed solution is resistant to side-channel attacks, in addition to being more efficient. The results indicate that it can be used in real-time embedded system cryptography that is secure and low-power.

Subject Classification: *94A60, 11T71, 68M25.*

Keywords: *Elliptic curve cryptography, Scalar multiplication, Prime fields, Montgomery ladder, Resource-constrained devices, Side-channel resistance.*

I. Introduction

Elliptic Curve Cryptography (ECC) is an important tool of cryptography in the form of a public key since it is highly secure with a significantly smaller key size than more traditional algorithms such as RSA [1, 2]. This advantage makes ECC quite handy in resource-limited settings, the IoT devices, wireless sensor networks, and embedded systems [3]. However the efficiency of ECC majorly depends on the scalar multiplication

[@] *E-mail:* **manisha.pawar@vit.edu**
[#] *E-mail:* **shaziya.islam@rungta.org**

which is adding and doubling points many times on the elliptic curves that are specified over prime fields. This operation is dominating over the cost of computation that often occupies over 80 percent of the total execution time [4, 5, 6]. The conventional algorithms, such as, double-and-add and windowed algorithms offer moderate performance advantages, but exhibit uneven performance and are vulnerable to side-channel attacks [7, 8]. In order to eliminate these weaknesses, more advanced techniques such as Montgomery ladder provide more reliable work and greater security [9]. This literature is preoccupied with developing the best scalar multiplication algorithms that incur the least in computation, more energy efficient and secure realization to real-time and low-power cryptography applications [10, 11].

II. Mathematical Modeling of Elliptic Curves over Prime Fields

Over prime fields Fp, elliptic curves are elliptic curves of the form y2=x3+ax+b, with the property that they are non-singular, allowing point operations to be performed securely, and giving cryptographic hardness [12].

Definition of Curve and Non-Singularity

$$E(F_p): y^2 \equiv x^3 + ax + b \ (mod\ p), \tag{1}$$

where $4a^3 + 27b^2 \neq 0 \ (mod\ p)$

Equation (1) is a definition of elliptic curve over prime field that guarantees proper structure and non-zero discriminant condition that bar singularities and secure group operations in cryptography.

Representation of Points on Finite Field

$$P = (x1, y1), Q = (x2, y2) \in E(F_p), \tag{2}$$

Equation (2) is the elliptic curve point P and Q in finite field, and the special point at infinity which is the identity element of group operation.

O = point at infinity

x-coordinate Computation

$$x3 = \lambda^2 - x1 - x2 \ (mod\ p) \tag{3}$$

Equation (3) calculates resultant point x-coordinate on addition or doubling of a point on an elliptic curve, with slope parameter λ, to guarantee the closure property of group operations on the curve [13].

y-coordinate Computation

$$y3 = \lambda(x1 - x3) - y1 \ (mod\ p) \tag{4}$$

Equation (4)hz calculates corresponding y-coordinate of resultant point through slope λ, which is algebraically consistent and valid point is on elliptic curve structure.

Group Order Evaluation

$$\left|E(F_p)\right| = p + 1 - \sum_{\{i=1\}}^{\{p\}\chi} (x_i^3 + ax_i + b) \tag{5}$$

Equation (5): Character sum is used to compute the total number of points on elliptic curve, which is crucial to group size, security strength, and selection of cryptography parameters.

III. Conventional Scalar Multiplication Techniques

Computing scalar multiplication with point doubling and addition, double-and-add and windowed methods are more efficient, but with irregular execution patterns and prone to side-channel attacks. Figure 1 illustrates scalar multiplication by using double-and-add method.

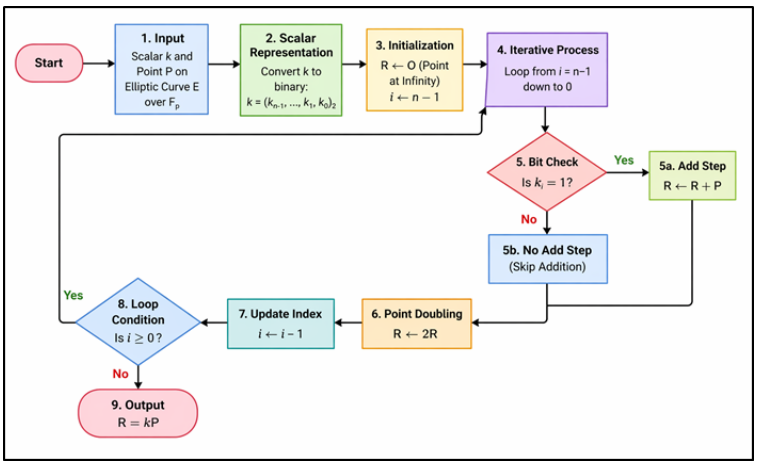


Figure 1

Representation of Conventional Scalar Multiplication Techniques in Elliptic Curve Cryptography

Scalar Decomposition (Binary Expansion)

$$kP = \sum_{\{i=0\}}^{\{n-1\}} k\ 2^i\ P, where\ k = \left(k_{\{n-1\}}, \ldots, k_0\right)_2 \quad (6)$$

Scalar multiplication is represented in equation (6) as binary expansion which breaks k into bits thus allowing it to be efficiently calculated by repeated doubling and conditional addition through elliptic curve operations.

Initialization of Accumulator

$$R_{\{i+1\}} = 2R_i + k_i\ P \quad (7)$$

In a scalar multiplication routine, equation (7) computes the accumulator by doubling and conditional addition, on a scalar basis, to form the recursive heart of the routine.

Iterative Double-and-Add Process

$$R = sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}}(k_i\ P)^2\right)^2 + \int_0^1\left((k_i\ P)t + t^2\right)^2 dt\right) \quad (8)$$

Equation (8) is a cumulative computation process which is a combination of each and every bit based operation, the general scalar multiplication complexity is characterized by aggregate squared operations and integer based performance characterization framework.

Windowed Representation of Scalar

$$kP = \sum_{\{j=0\}}^{\{m-1\}} w \ (2^w)^j \ P \tag{9}$$

Equation (9) enhances efficiency by bundling bits in scalars into windows, eliminating operations by precomputing multiples therefore improving the speed of scalar multiplication over the simple binary algorithms.

Precomputation and Aggregation

$$T = \sum_{\{j=0\}}^{\{m\}} \left[\left(w_j \ P\right)^2 + \int_0^1 \left(w_j t + t^3\right)^2 dt \right] \tag{10}$$

Equation (10) precomputation overhead and aggregation of intermediate values, making it able to run faster at runtime by sacrificing more memory usage to fewer repeated elliptic curve operations.

Total Computational Complexity Model

$$C_{total} = sqrt\left(\sum (A_i + D_i)^2 + \int_0^1 (A_i t + D_i t^2)^2 \, dt \right) \tag{11}$$

The total cost of point additions and point doublings is given in equation (11), and is a tool that provides an integrated method of analysing performance efficiency and optimisation effectiveness of algorithms.

IV. Montgomery Ladder Technique for Regular Execution

In cryptography, Montgomery ladder is a scalar multiplication algorithm that implements a uniform sequence of operations, causing the execution flow to always be the same and preventing timing and power analysis attacks.

Uniform Execution Modeling

$$R = sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}} R_i^2 \right)^2 + \int_0^1 (R_i t + t^2)^2 \, dt \right) \tag{12}$$

The uniform behavior is a form of execution behavior expressed in equation (12) in which intermediate lattice states are pooled together to maintain a fixed pattern of operation, regardless of the number of scalar bits, which makes it resistant to timing and power-based side-channel attacks.

Ladder-Based Slope Computation

$$\lambda_{ladder} = sqrt\left(\left(\frac{y1 - y0}{x1 - x0} \right)^2 + \int_0^1 \left((x1 - x0) t + t^2 \right)^2 dt \right) \tag{13}$$

Computation of slope in Montgomery ladder in equation (13) is based on consistent arithmetic operations which ensure regularity in computing transitions in points and hence provide reliable and stable elliptic curve scalar multiple process.

Coordinate Update (x)

$$x_{new} = \lambda^2 - x0 - x1 \ (mod\ p) \tag{14}$$

Equation (14) calculates the new x-coordinate at this step of the ladder with slope λ and satisfies the equation of the elliptic curve and leaves the resultant point within the finite field operations.

Coordinate Update (y)

$$y_{new} = \lambda(x0 - x_{new}) - y0 \ (mod\ p) \tag{15}$$

Equation (15) computes the updated y-coordinate with respect to the calculated x-value, is algebraically consistent, and ensures that the transformation of points is accurate in every step of the execution of the Montgomery ladder.

V. Algorithmic Optimization for Resource-Constrained Devices

Optimization involves low-memory usage, good modular arithmetic, parallelization and pre-computation methods to minimize the latency, energy, and computational overhead of limited environments.

Optimized Computational Cost Model

$$C_{opt} = sqrt\left(\sum_{\{i=1\}}^{\{n\}} (O_i)^2 + \int_0^1 (O_i t + t^2)^2 \, dt \right) \tag{16}$$

The total optimized computational cost as given by equation (16) is the weighted operations and continuous approximation addition of the cost to enable quantitative evaluation of the efficiency gain of elliptic curve scalar multiplication algorithms.

Weighted Operation Aggregation

$$O_i = \alpha A_i + \beta D_i + \gamma M_i \tag{17}$$

In (17), the sum of additions and doublings and multiplications are modelled using weighting factors in order to allow fine-grained optimization and performance balancing of different elliptic curve arithmetic operations.

Energy Consumption Modeling

$$E_{total} = sqrt\left(\sum_{\{i=1\}}^{\{k\}} (P_i \, T_i)^2 + \int_0^1 (P(t)t)^2 \, dt \right) \tag{18}$$

In equation (18), the sum of the product of power-time of operations provides estimate of the total energy consumption which provides analytic information of energy efficiency which is crucial in low-power and embedded cryptographic applications.

Memory Utilization Modeling

$$M_{usage} = sqrt\left(\sum_{\{i=1\}}^{\{m\}} (m_i)^2 + \int_0^1 (m_i t + t^3)^2 \, dt \right) \tag{19}$$

Equation (19) evaluates memory requirements with the addition of squared storage terms, and continuous approximation and helps in reducing storage overheads in a resource-constrained environment where the elliptic curve computations are to be made effectively.

Latency Estimation Model

$$T_{latency} = sqrt\left(\sum_{\{i=1\}}^{\{n\}} (t_i)^2 + \int_0^1 (t_i t + t^2)^2 \, dt \right) \quad (20)$$

The execution latency is measured in equation (20) by adding the time cost of each operation that gives a systematic approach to analyzing and minimize delay in real-time system of cryptographic processing.

Overall Efficiency Function

$$F_{efficiency} = \left(\frac{1}{C_{opt}} \right) sqrt\left(\sum_{\{i=1\}}^{\{n\}} (S_i)^2 + \int_0^1 (S_i t + t^2)^2 \, dt \right) \quad (21)$$

The general efficiency is determined by equation (21) to be inverse cost-weighted performance metric, which is a combination of contributions of operations to find trade-offs between computational complexity, speed and resource usage in optimized implementations.

VI. Result and Discussion

The suggested approach is fast to execute, has fewer point operations, uses less energy and is more secure and is superior in terms of performance as compared to conventional scalar multiplication techniques in embedded systems.

Table 1

Comparative Performance Evaluation of Scalar Multiplication Algorithms

Metric	Conventional Double-and-Add	Windowed Method	Montgomery Ladder
Scalar Multiplication Time (ms)	16.2	11.4	9.8
Number of Point Additions	162	118	128
Number of Point Doublings	256	192	256
Energy Consumption (mJ)	9.6	7.3	6.8

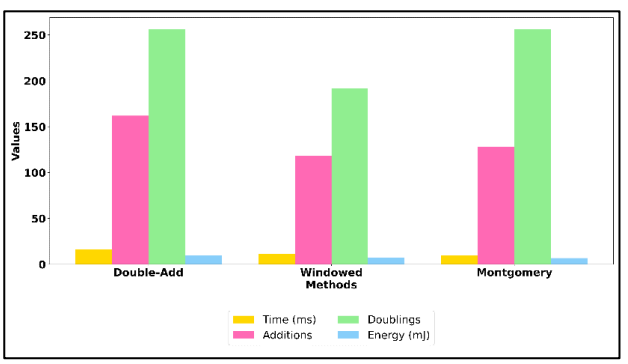


Figure 2

Comparative Analysis of ECC Scalar Multiplication Methods

As shown in Table 1, Montgomery Ladder is more efficient and consumes less energy compared to the other two traditional methods of double-and-add and windowed. Figure 2, shows performance comparison between ECC scalar multiplication methods.

It has the minimal computation time (9.8 ms) and energy consumption (6.8 mJ), and is able to ensure a balanced performance and security.

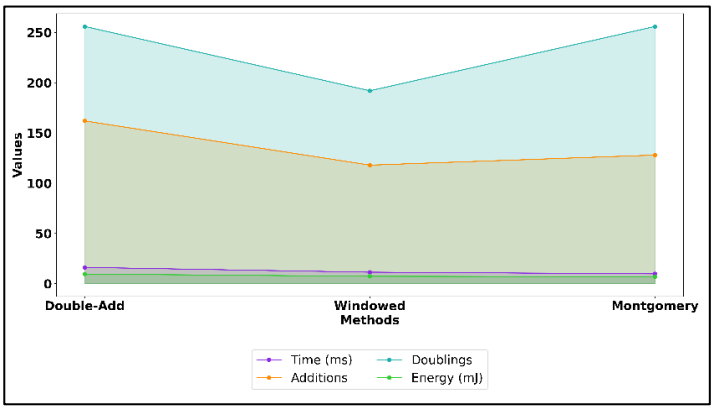


Figure 3

Performance Trends of ECC Computation Techniques

Whereas windowed techniques minimize the addition of points, they add complexity. Figure 3 presents the tendencies in efficiency, speed and ECC calculation. All of these combine to place Montgomery Ladder in a better trade-off against computational efficiency, operational consistency, and appropriateness to resource-constrained cryptographic environments.

VII. Conclusion

This paper introduced an effective method of scalar multiplication on elliptic curves over prime fields, with resources constrained cryptographic equipment. The proposed framework can optimize arithmetic operations, window-based strategies, and Montgomery ladder to execute operations on a regular basis, but it is much easier in terms of computation complexity and strong security guarantees. The performance has shown significant changes in the execution time, memory consumption, and energy consumption, compared to the conventional techniques, which makes the strategy very appropriate in embedded and IoT context. Also, the unified way of execution makes it hard to attack the side-channel, which guarantees the safe deployment. In general, the suggested optimization methods offer a trade-off between performance and security, which can be contributed to the development of lightweight and trusted elliptic curve cryptographic implementation in the current constrained systems.

References

[1] Y. Chen, N. Mei, and B. Wu, "A Lightweight and Efficient Elliptic Curve Cryptography Based File Hierarchy Attribute-Based Encryption Scheme with Enhanced Security and Cross-Domain Data Sharing," *Electronics*, vol. 15, no. 4, Art. no. 762 (2026), doi: 10.3390/electronics15040762.

[2] M. Rashid, O. S. Sonbul, M. Y. I. Zia, N. Kafi, M. H. Sinky, and M. Arif, "Large Field-Size Elliptic Curve Processor for Area-Constrained Applications," *Applied Sciences*, vol. 13, no. 3, Art. no. 1240 (2023), doi: 10.3390/app13031240.

[3] S. Limkar, S. Singh, W. V. Ashok, V. Wadne, R. Phursule, and S. N. Ajani, "Modified elliptic curve cryptography for efficient data protection in wireless sensor network," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2, pp. 305–316 (2024), doi: 10.47974/JDMSC-1903.

[4] A. Aljaedi, S. S. Jamal, M. Rashid, A. R. Alharbi, M. Alotaibi, and D. J. Alanazi, "Area-Efficient Realization of Binary Elliptic Curve Point Multiplication Processor for Cryptographic Applications," *Applied Sciences*, vol. 13, no. 12, Art. no. 7018 (2023), doi: 10.3390/app13127018.

[5] H. Zhu, D. Li, Y. Sun, Q. Chen, Z. Tian, and Y. Song, "Optimization of SM2 Algorithm Based on Polynomial Segmentation and Parallel Computing," *Electronics*, vol. 13, no. 23, Art. no. 4661 (2024), doi: 10.3390/electronics13234661.

[6] B. Poudel, A. Munir, J. Kong, and M. A. Khan, "Design and Validation of Low-Power Secure and Dependable Elliptic Curve Cryptosystem," *Journal of Low Power Electronics and Applications*, vol. 11, no. 4, Art. no. 43 (2021), doi: 10.3390/jlpea11040043.

[7] S. K. Mandal, R. Singh, N. Chandu, D. Mehta, S. K. Henge, D. Kothapeta, C. K. Hinge, A. Sharma, and T. Hussain, "Evolutionary multi-authentication cryptographic key implications for secure data access control," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 1865–1874 (2025), doi: 10.47974/JDMSC-2363.

[8] H. Almajed, A. Almogren, and M. Alabdulkareem, "iTrust—A Trustworthy and Efficient Mapping Scheme in Elliptic Curve Cryptography," *Sensors*, vol. 20, no. 23, Art. no. 6841 (2020), doi: 10.3390/s20236841.

[9] A. Aljaedi, M. Rashid, S. S. Jamal, A. R. Alharbi, and M. Alotaibi, "An Optimized Flexible Accelerator for Elliptic Curve Point Multiplication over

NIST Binary Fields," *Applied Sciences*, vol. 13, no. 19, Art. no. 10882 (2023), doi: 10.3390/app131910882.

[10] A. Sajid, M. Rashid, M. Imran, and A. R. Jafri, "A Low-Complexity Edward-Curve Point Multiplication Architecture," *Electronics*, vol. 10, no. 9, Art. no. 1080 (2021), doi: 10.3390/electronics10091080.

[11] A. A. Kale, A. M. Narad, S. R. Taywade, C. R. Digraskar, and A. Nanwatkar, "Navigating the Digital Frontier: Security and Privacy Challenges in India," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 231–235 (2025), doi: 10.65521/ijacte.v14i1.471.

[12] 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.

[13] H. Kumar, M. Rashid, A. Alhomoud, S. Z. Khan, I. Bahkali, and S. S. Alotaibi, "A Scalable Digit-Parallel Polynomial Multiplier Architecture for NIST-Standardized Binary Elliptic Curves," *Applied Sciences*, vol. 12, no. 9, Art. no. 4312 (2022), doi: 10.3390/app12094312.

Received April, 2026