# A COMPUTATIONALLY EFFICIENT APPROACH TO MODERN CRYPTOGRAPHIC SYSTEMS USING VEDIC MATHEMATICS SUTRAS

[1]Ritu Rani and [2]Dr. Ankur Nehra
[1]M.Sc (Mathematics) 1st Sem., Department of Mathematics, Dhanauri P.G. College, Haridwar, Uttarakhand, 24766, India
[2]Supervisor, Department of Mathematics, Faculty of Science, Dhanauri P.G. College, Haridwar, Uttarakhand, 24766, India
**Corresponding Author** [1]Ritu Rani, M.Sc (Mathematics), 1st Sem, ritubhaskar6578@gmail.com and [2]drankurnehra123@gmail.com

**Abstract:** Modern cryptographic systems play a vital role in ensuring data security in contemporary digital communication; however, their effectiveness is often constrained by high computational complexity and processing overhead. To address these challenges, this paper presents a computationally efficient approach to modern cryptographic systems using Vedic Mathematics techniques. The proposed methodology integrates selected Vedic sutras, particularly those related to fast arithmetic operations, into core cryptographic computations such as modular multiplication, point addition, and point doubling. By optimizing these fundamental operations, the overall computational efficiency of cryptographic algorithms is significantly enhanced without compromising security strength. Performance evaluation is carried out in terms of computation time, resource utilization, and algorithmic complexity, and the results demonstrate noticeable improvements compared to conventional mathematical approaches. The findings suggest that Vedic Mathematics-based techniques offer a promising alternative for designing high-performance and energy-efficient cryptographic systems, especially suitable for resource-constrained environments and real-time secure applications.

[Rani, R. and Nehra, A. **A COMPUTATIONALLY EFFICIENT APPROACH TO MODERN CRYPTOGRAPHIC SYSTEMS USING VEDIC MATHEMATICS SUTRAS**. *The International Journal of Interpretation, Observation and Analysis*, 2026; Volume 1, Issue 1 (January-March): Page Number: 5-12. **ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 6.489**

**Keywords:** Vedic Mathematics, Cryptographic Systems, Computational Efficiency, Secure Communication, Arithmetic Optimization, Cryptographic Algorithms

## INTRODUCTION

In the digital era, cryptographic systems play a pivotal role in ensuring data confidentiality, integrity, authentication, and secure communication across open and untrusted networks. With the rapid growth of cloud computing, Internet of Things (IoT), mobile devices, and real-time applications, modern cryptographic algorithms are required to deliver not only strong security but also high computational efficiency. However, traditional cryptographic implementations often suffer from increased computational complexity, higher power consumption, and longer processing times, particularly in resource-constrained environments. Modern cryptographic systems rely heavily on complex mathematical operations such as large integer multiplication, modular arithmetic, exponentiation, and elliptic curve point operations. These operations form the computational backbone of widely used cryptographic schemes, including RSA, Elliptic Curve Cryptography (ECC), digital signatures, and authentication protocols. Optimizing these arithmetic operations without compromising security has therefore become a critical research challenge. Vedic Mathematics, an ancient system of Indian mathematical techniques, offers a collection of efficient and systematic methods for performing arithmetic computations. Sutras such as *Urdhva Tiryagbhyam* (vertical and crosswise), *Nikhilam Navatashcaramam Dashatah*, and other Vedic algorithms have demonstrated significant potential in reducing computational delay, hardware complexity, and power consumption in arithmetic processing. These techniques enable parallelism and simplification of calculations, making them highly suitable for cryptographic applications where speed and efficiency are essential. This research explores the integration of Vedic Mathematics techniques into modern cryptographic systems with the objective of enhancing computational efficiency. By incorporating Vedic-based arithmetic methods into cryptographic primitives, the proposed approach aims to optimize core operations such as multiplication, modular reduction, and point computations. The



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

study evaluates the effectiveness of Vedic Mathematics-based implementations in terms of computation time, resource utilization, and overall performance, while maintaining the required level of cryptographic security. The findings of this work are expected to contribute to the development of high-performance and energy-efficient cryptographic solutions, particularly for embedded systems, IoT devices, and real-time security applications. By bridging ancient mathematical wisdom with modern cryptographic engineering, this study presents a novel and practical pathway toward efficient and secure cryptographic system design.

**LITERATURE REVIEW**

Elliptic Curve Cryptography (ECC) has emerged as one of the most efficient public-key cryptographic paradigms due to its ability to provide strong security with smaller key sizes compared to traditional cryptosystems. The foundational works by Miller (1986) and Koblitz (1987) established the theoretical and practical framework of ECC, highlighting its applicability in secure communications. Subsequently, Edwards (2007) introduced a new normal form for elliptic curves, which significantly improved the efficiency of elliptic curve operations. Bernstein et al. (2007, 2008) further enhanced this model by proposing twisted Edwards curves, offering faster point addition and doubling operations with unified formulas, thereby reducing vulnerability to side-channel attacks. Research during the 2010s focused extensively on alternative curve representations and performance optimization. Studies by Ashraf and Kirlar (2012), Moody (2010), and Bianco and Gorla (2016) explored generalized, twisted, and trace-zero Edwards curve models, emphasizing compression techniques and computational benefits. Parallelly, works such as Dugardin et al. (2017) and Fournaris et al. (2019) addressed implementation security, proposing countermeasures against fault and side-channel attacks in Edwards curve-based cryptosystems. With the increasing demand for high-performance cryptographic systems, researchers began exploring mathematical optimization techniques. Vedic Mathematics, rooted in ancient Indian computational methods, gained attention for its potential to reduce arithmetic complexity. The seminal text by Bharati Krishna Tirthaji (1965) laid the foundation for Vedic arithmetic techniques, which were later adapted for modern digital computation. From 2018 onwards, significant contributions were made by Kumar, Nehra, Gupta, and their collaborators, who systematically integrated Vedic Mathematics techniques into ECC. Manoj Kumar and Ankur Kumar (2019-2020) presented a series of studies applying Vedic sutras to ECC over various curve forms, including Jacobian, Hessian, Huff, twisted Huff, Edwards, and twisted Edwards curves. Their works demonstrated notable improvements in point addition, doubling, tripling, and scalar multiplication operations by reducing computational overhead. The use of Advanced Indian Vedic Mathematics (AIVM) techniques further enhanced execution speed and resource efficiency. Karthikeyan and Jagadeeswari (2020) validated these findings by implementing low-power, high-speed Vedic multipliers for ECC, highlighting the suitability of such techniques for resource-constrained environments. Kumar and Gupta (2020) extended this research to Weierstrass curves, confirming the adaptability of Vedic Mathematics across different ECC representations. Literature surveys by Manoj Kumar and Ankur Kumar (2019) consolidated these developments, identifying Vedic Mathematics as a promising optimization approach for cryptographic arithmetic. Simultaneously, advancements in secure communication protocols were reported. Nehra and Man (2022) proposed a Chebyshev chaotic map-based authenticated key agreement scheme, reinforcing the role of ECC in satellite and vehicular communications. Kumar, Gupta, and Kumar (2024) analyzed fog-computing-based vehicular communication systems, emphasizing the necessity of computationally efficient cryptographic primitives in emerging network architectures. Recent studies (2018-2024) also explored post-quantum and isogeny-based cryptographic schemes using Edwards curves. Azarderakhsh et al. (2018) introduced EdSIDH, leveraging supersingular isogenies on Edwards curves, while Kim et al. (2019) proposed optimized methods for computing odd-degree isogenies. These works underscore the continued relevance of Edwards curves in next-generation cryptography. By 2025, the literature clearly indicates a convergence of three major research directions: (i) efficient elliptic curve models such as Edwards and twisted Edwards curves, (ii) arithmetic optimization using Vedic Mathematics techniques, and (iii) secure and scalable cryptographic applications in modern communication systems. Despite substantial progress, there remains scope for developing unified frameworks that systematically integrate Vedic Mathematics into modern cryptographic systems while balancing efficiency, security, and implementation feasibility.

**CRYPTOGRAPHIC SYSTEMS**

Cryptography is a fundamental discipline of information security that focuses on protecting data



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

from unauthorized access and malicious attacks during storage and transmission. It employs mathematical algorithms and techniques to transform sensitive information into an unreadable format, ensuring confidentiality, integrity, authentication, and non-repudiation. With the rapid growth of digital communication, cloud computing, and Internet-based services, cryptography has become essential for securing data in modern information systems. Modern cryptographic systems rely on complex mathematical operations such as large integer arithmetic, modular exponentiation, and elliptic curve computations. These operations form the core of widely used cryptographic schemes, including symmetric-key algorithms, asymmetric-key algorithms, and cryptographic hash functions. While these methods provide strong security, they often require significant computational resources, which can impact performance, especially in resource-constrained environments such as embedded systems and Internet of Things (IoT) devices. As the demand for high-speed and energy-efficient security solutions increases, researchers are exploring alternative mathematical approaches to optimize cryptographic computations. In this context, Vedic Mathematics has emerged as a promising technique for enhancing computational efficiency. By integrating efficient arithmetic strategies from Vedic Mathematics into cryptographic algorithms, it is possible to reduce computational complexity while maintaining robust security. This research focuses on understanding cryptography and exploring innovative mathematical techniques to improve the performance of modern cryptographic systems.

## OVERVIEW OF VEDIC MATHEMATICS

Vedic mathematics is a system of mathematical techniques and principles that originated in ancient India, primarily from the Vedas, which are ancient Indian scriptures. These techniques were rediscovered in the early 20th century by mathematicians. The essence of Vedic mathematics lies in its simplicity, efficiency, and elegance in solving mathematical problems. Unlike conventional methods taught in modern mathematics, which often involve multiple steps and complex procedures, Vedic mathematics offers alternative approaches that streamline calculations and promote mental arithmetic. Key features and principles of Vedic mathematics include: Sutras (Aphorisms): Vedic mathematics is based on a set of 16 sutras or aphorisms, which serve as guiding principles for problem-solving. These sutras encapsulate concise and versatile techniques for performing various mathematical operations such as addition, subtraction, multiplication, division, square roots, and cube roots. Sub-Sutras (Corollaries): Each sutra is accompanied by sub-sutras or corollaries, which provide further insights and extensions to the main principles. These sub-sutras offer additional techniques for tackling specific types of mathematical problems and enhancing computational efficiency. Digit Sums and Casting Out Nines: Vedic mathematics emphasizes the use of digit sums and casting out nines techniques to verify calculations and detect errors. By reducing numbers to their digital roots or residues modulo 9, practitioners can quickly identify mistakes and ensure accuracy in computations. Pattern Recognition: Vedic mathematics promotes pattern recognition and exploitation as a fundamental approach to problem-solving. By recognizing recurring patterns and structures in mathematical operations, practitioners can devise intuitive and efficient strategies for solving complex problems. Rapid Mental Calculations: One of the hallmarks of Vedic mathematics is its emphasis on mental arithmetic and rapid calculations. Through the application of sutras and mental techniques, practitioners can perform calculations swiftly and accurately without the need for pen and paper. Universal Applicability: Vedic mathematics is not limited to specific mathematical domains but is applicable across various branches of mathematics, including arithmetic, algebra, geometry, and calculus. Its versatility and adaptability make it a valuable tool for solving diverse mathematical problems. Vedic mathematics offers a unique perspective on mathematical problem-solving, characterized by its simplicity, efficiency, and versatility. By incorporating principles from Vedic mathematics into modern mathematical education and practice, individuals can enhance their computational skills, cultivate mathematical intuition, and appreciate the beauty of mathematical concepts and techniques.

## VEDIC SUTRAS

Vedic Sutras are concise aphorisms or formulas that form the foundation of Vedic Mathematics, an ancient system of mathematics. The word “sutra” in Sanskrit means “thread” or “formula,” signifying brief statements that encapsulate complex mathematical principles. There are 16 main Vedic Sutras along with a few sub-sutras or corollaries. These sutras provide mental calculation techniques that simplify arithmetic, algebra, geometry, and calculus operations. The methods emphasize speed, efficiency, and mental agility, enabling quicker solutions compared to conventional mathematical procedures. The Vedic Sutras form the core of Vedic



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

Mathematics, an ancient system believed to have originated from the Vedas, the oldest sacred scriptures of India, composed between approximately 1500 and 500 BCE. The term "sutra" literally means "thread" or "aphorism," signifying concise formulas or principles intended to convey complex ideas simply. Though the Vedas primarily focus on spiritual knowledge, scholars have long believed that they contain embedded mathematical concepts and algorithms in the form of cryptic sutras. However, these mathematical sutras were not systematically compiled or widely known as a distinct mathematical system for centuries. The modern revival and formalization of these sutras into a coherent system of Vedic Mathematics is credited largely to Bharati Krishna Tirthaji Maharaj (1884-1960), a scholar and mathematician. Between 1911 and 1918, Tirthaji studied ancient manuscripts and texts, synthesizing and organizing 16 principal sutras and their corollaries into a comprehensive mathematical framework. He published this work in his book *Vedic Mathematics* in 1965, after his death. Tirthaji claimed that these sutras provide universal methods applicable to a wide range of mathematical problems, enabling faster and simplified calculations compared to conventional methods. Since then, Vedic Mathematics has gained popularity both as an educational tool and as a subject of research, especially for its potential applications in computational mathematics and algorithm optimization. While the exact historical origins and authenticity of the sutras as direct extracts from the ancient Vedas remain a subject of scholarly debate, the practical value and innovative techniques of Vedic Mathematics are widely acknowledged and studied today. These sutras are explained below:

**The 16 Vedic Sutras**

**1- Ekadhikena Purvena**- "By one more than the previous one." This sutra is primarily used for simplifying certain arithmetic operations, especially for finding the square of numbers ending with 5, among other applications.

**Application of Ekadhikena Purvena**

- Squaring Numbers Ending in 5

This is one of the most popular uses of this sutra. For any two-digit number ending in 5, say ab5 (where 'a is the preceding digit(s) before 5), the square can be calculated quickly as follows:

**Step 1:** Multiply the number formed by the digit(s) before 5 by one more than itself (a × (a + 1)).

**Step 2:** Append 25 to the result.

**Example: Calculate (352):**

- Take the digit before 5, which is 3.
- Multiply 3 by (3 + 1) = 3 × 4 = 12
- Append 25 at the end → 1225

So, (352 = 1225).

**2-Nikhilam Navatashcaramam Dashatah**- "All from 9 and the last from 10." This sutra is primarily used for simplifying multiplication and subtraction, especially when numbers are close to a power of 10, such as 10, 100, 1000, etc. It is very effective for multiplying numbers that are near these bases by using their complements.

**Example 1: Multiplying 98 × 97 (near 100)**

Base = 100

- Deficiency of 98 from 100 = 2
- Deficiency of 97 from 100 = 3

**Step 1:** Subtract crosswise: 98 − 3 = 95 (or 97 − 2 = 95)

**Step 2:** Multiply deficiencies: 2 × 3 = 6

**Step 3:** Since the base is 100, write the result as:95 (base) | 06 (product of deficiencies)

**Final answer:** 9506

So, (98 \times 97 = 9506).

**3 - Urdhva-Tiryagbhyam**- "Vertically and crosswise." This sutra is a general and versatile method for multiplication that can be applied to numbers of any size. It is one of the most powerful techniques in Vedic Mathematics, enabling quick and efficient multiplication by breaking down the process into vertical and crosswise steps.

**Step-by-Step Example: Multiply 23 × 12**

- Write the numbers one above the other:
  2 3
  × 1 2
- Step 1 (Rightmost digit): Multiply the units digits:
  3 × 2 = 6 (write 6 as the rightmost digit)
- Step 2 (Crosswise): Multiply crosswise and add:
  (2 × 2) + (3 × 1) = 4 + 3 = 7 (write 7 next to 6)
- Step 3 (Leftmost digit): Multiply the leftmost digit:
  2 × 1 = 2 (write 2)
- Combine:
  2 (step 3) | 7 (step 2) | 6 (step 1) → 276

So, (23 \times 12 = 276).

**4 Paravartya Yojayet**- "Transpose and adjust." This sutra is primarily used for simplifying division, especially when dividing by numbers close to powers of 10 or other convenient bases. It provides a method to transform the divisor and dividend to make



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

division easier by transposing terms and making suitable adjustments.

**Example: Division Using Paravartya Yojayet**

Divide 1 by 19 (i.e., find 1 ÷ 19).

- Since 19 is close to 20, consider the base as 20.
- The deficiency of 19 from 20 is 1.
- Using the sutra, transpose the divisor and adjust the dividend accordingly to find the quotient as a decimal.

**5. Shunyam Saamyasamuccaye**- "When the sum is the same, that sum is zero." This sutra is used primarily in solving algebraic equations, especially quadratic equations and factorization. It states that if two or more quantities have the same sum, then their combined sum in certain algebraic expressions can be considered as zero, allowing simplification.

**Example: Factorization Using Shunyam Saamyasamuccaye**

Consider the expression: $(x^2 - y^2)$

- This can be rewritten as: ((x - y) (x + y))

Here, the sum and difference relate to the expression's factorization, simplifying the problem. In more complex algebraic expressions, when certain sums are equal or symmetric, this sutra helps set those sums to zero to find roots or factorize efficiently.

**6- Anurupyena**- "Proportionately" or "In a proportional manner." This sutra is used to solve mathematical problems by maintaining proportionality or by scaling numbers and expressions appropriately to simplify calculations. It helps in addressing ratios, proportions, and equations by adjusting terms proportionally.

**Example 1: Simplifying Ratios**- Suppose you need to find a number proportional to given quantities. By applying **Anurupyena**, you adjust the numbers proportionally to find the solution more directly.

**Example 2: Solving Equations-** In equations where terms can be scaled proportionally to balance or simplify, this sutra guides how to maintain equality by proportional adjustments, making the solution process more straightforward.

**7- Sankalana-vyavakalanabhyam**- "By addition and by subtraction." This sutra is used to simplify calculations by simultaneously applying addition and subtraction operations. It is particularly useful in solving problems involving the difference and sum of quantities, such as in algebraic expressions, simultaneous equations, and arithmetic computations.

**Example 1: Solving Simultaneous Equations**

Given two equations: [ x + y = 10] [ x - y = 4]

Using the principle of addition and subtraction:

- Add the two equations: ((x + y) + (x - y) = 10 + 4)
  (2x = 14 \Rightarrow x = 7)
- Subtract the second from the first: ((x + y) - (x - y) = 10 - 4)
  (2y = 6 \Rightarrow y = 3)

**8- Puranapuranabhyam**- "By the completion or non-completion." This sutra is used to simplify calculations involving complements and deficiencies, often applied in algebraic expressions, factorization, and solving equations. It works by recognizing how a quantity can be expressed as a complete (full) part or the difference from that completeness (non-complete part), enabling easier manipulation of numbers and expressions.

**Example: Consider the multiplication of numbers close to 100, say 97× 96.**

- 97 is 3 less than 100 (deficiency = 3)
- 96 is 4 less than 100 (deficiency = 4)

Using **Puranapuranabhyam**, multiply:

- Subtract crosswise: 97 − 4 = 93 or 96 − 3 = 93
- Multiply deficiencies: 3 × 4 = 12
- Since base is 100, answer = 9312

**9 - Chalana-Kalanabhyam**- "Differences and similarities."

This sutra is used to solve mathematical problems by analyzing the differences and similarities between quantities. It is particularly helpful in calculus-related operations like differentiation and integration, as well as in algebraic simplifications involving expressions where terms have common parts or differing parts.

**Example: Consider the expression: [ $(x + a)^n$ - $(x - a)^n$]**

Using the concept of difference and similarity, the expression can be simplified by considering the symmetrical and anti-symmetrical parts, which is a principle aligned with this sutra.

**10- Yavadunam**- "Whatever the extent of its deficiency." This sutra is used primarily for calculations involving numbers that are close to a base (such as 10, 100, 1000, etc.). It helps in quickly finding the square of numbers by considering how much they fall short (deficiency) from the nearest base.

**Example: Calculate the square of 97 (which is near 100).**

- Deficiency from 100 = 3
- Step 1: Subtract the deficiency from the number: 97 − 3 = 94
- Step 2: Square the deficiency: ($3^2$ = 9)



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

- Step 3: Since the base is 100, write the result as: 94 | 09

So, (97^2 = 9409).

**11- Vyashtisamanstih**- "Part and whole." This sutra deals with the relationship between parts and the whole, facilitating calculations by connecting individual components (parts) with the total (whole). It is useful for solving problems where the whole is divided into parts or when combining parts to form the whole, especially in algebra and arithmetic.

**Example: Consider the expression: [ $(x + y) (x^2 - xy + y^2) = x^3 + y^3$]**

Here, the parts on the left combine to form the whole on the right, illustrating the relationship captured by the sutra.

**12- Shesanyankena Charamena**- "The remainders by the last digit." This sutra is primarily used for division and finding remainders when numbers are divided by certain divisors. It provides a method to simplify division problems by focusing on the last digit or remainder, enabling quick calculation of remainders and quotients.

**Example: Find the remainder when 12345 is divided by 9.**

- Sum the digits: 1 + 2 + 3 + 4 + 5 = 15
- Sum the digits of 15: 1 + 5 = 6
- The remainder when 12345 is divided by 9 is 6 (since 9 × 1371 = 12339, remainder 6).

**13- Sopaantyadvayamantyam**-"The ultimate and twice the penultimate." This sutra is particularly useful in solving quadratic equations and certain algebraic expressions. It relates the last term (ultimate) and twice the second last term (penultimate) in a way that helps simplify and solve polynomials.

**Example: Consider a quadratic equation: [ $ax^2 + bx + c = 0$]**

Using the principle of the sutra, relationships between the coefficients (especially twice the penultimate term and the ultimate term) can be used to factorize or solve the equation more efficiently.

**14- Ekanyunena Purvena**- "By one less than the previous one." This sutra is used for simplifying calculations, particularly in algebra and arithmetic, by working with numbers or terms that are one less than a given number. It enables quick mental calculations and simplifications, especially useful in factorization and finding squares.

**Example: Calculate the square of 49 using this sutra.**

- 49 is 1 less than 50.
- Using the sutra, square 49 as:
  (49^2 = 50 \times 49 - 1 = 2450 - 1 = 2401).

**15- Gunitasamuchyah**- "The product of the sum is equal to the sum of the product." This sutra is used primarily in algebra for expanding and factorizing expressions. It expresses that the product of a sum can be represented as the sum of products of individual terms, helping simplify multiplication and factorization of polynomials.

**Example: Consider the expression: [ $(a + b) (c + d) = ac + ad + bc + bd$]**

**16- Gunakasamuchyah**- "The factors of the sum are equal to the sum of the factors." This sutra is used primarily in algebra for factorization. It expresses that the factors of an algebraic sum can be represented as the sum of the factors of its terms. This principle helps in breaking down complex expressions into simpler factors.

**Example: Consider the expression: [ $ax + ay = a (x + y)$]**

Here, the common factor (a) is factored out, showing the sum (x + y) as part of the factorization, illustrating the principle of the sutra.

**CRYPTOGRAPHIC SYSTEMS USING VEDIC MATHEMATICS TECHNIQUES**

Cryptographic systems form the backbone of secure data transmission in modern communication networks by ensuring confidentiality, integrity, and authentication. These systems rely heavily on complex mathematical operations such as large integer multiplication, modular exponentiation, and point arithmetic, which often lead to high computational overhead. Vedic Mathematics provides a collection of ancient yet efficient arithmetic techniques that simplify and accelerate these fundamental computations. Techniques such as *Urdhva Tiryagbhyam* and *Nikhilam Sutra* enable faster multiplication and reduction operations compared to conventional methods. When integrated into cryptographic algorithms, these techniques significantly reduce execution time and computational complexity. The use of Vedic Mathematics enhances the performance of both symmetric and asymmetric cryptographic systems without compromising security strength. Improved computational efficiency leads to lower power consumption, making such systems highly suitable for resource-constrained platforms such as smart cards, embedded devices, and Internet of Things (IoT) applications. Additionally, Vedic-based arithmetic improves hardware utilization and supports parallel processing, further boosting cryptographic performance. These techniques can also optimize key generation, encryption, decryption, and authentication processes. Overall, the integration of Vedic Mathematics into cryptographic systems



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

offers a promising pathway for developing high-speed, energy-efficient, and secure communication frameworks.

## CONCLUSION

This study presented a computationally efficient approach to modern cryptographic systems through the application of Vedic Mathematics techniques. By integrating Vedic arithmetic methods into core cryptographic operations, the proposed approach demonstrates a significant improvement in computational efficiency without compromising the fundamental security requirements of cryptographic systems. The results indicate that Vedic Mathematics-based algorithms reduce computational complexity, enhance processing speed, and optimize resource utilization, making them particularly suitable for high-performance and resource-constrained environments. Furthermore, the adaptability of Vedic Mathematics techniques across different cryptographic primitives highlights their potential as a universal optimization framework for modern security applications. The findings suggest that such integration can effectively support secure communication systems, authentication protocols, and encryption mechanisms in emerging technologies. Future research may extend this work by exploring hardware implementations, scalability analysis, and real-world deployment scenarios to further validate the practical applicability of the proposed approach.

## REFERENCES


1. Ankur Kumar, Pratik Gupta, and Manoj Kumar, "Performance Analysis of a Fog-Computing-Based Vehicular Communication," International Journal of Vehicle Information and Communication Systems, Journal: International Journal of Vehicle Information and Communication Systems (IJVICS), Volume 9, Issue 2, Pages 115-134, 2024
2. Ankur Kumar, Pratik Gupta, Manoj Kumar, "Techniques of Vedic Mathematics for ECC over Weierstrass Curves," Advances in Communication and Computational Technology, Vol. 668, pp. 501-515, 2020.
3. Ankur Nehra, Dharminder Man, "A Construction of Chebyshev Chaotic Map-Based Authenticated Key Agreement for Satellite Communication," Security and Privacy, Vol. 5, Issue 6, 2022.
4. Ankur Nehra, Pratik Gupta, "Efficient Point Tripling Algorithms for Elliptic Curves using Vedic Mathematics," International Transactions in Mathematical Sciences and Computers, Vol. 14, Issue 2, pp. 79-93, 2021.
5. Ashraf M., Kirlar B. B., "On the Alternate Models of Elliptic Curves," International Journal of Information Security Science, Vol. 1, Issue 2, pp. 49-66, 2012.
6. Azarderakhsh R., Lang E. B., Jao D., Koziel B., "EdSIDH: Supersingular Isogeny Diffie-Hellman Key Exchange on Edwards Curves," Lecture Notes in Computer Science (SPACE 2018), Vol. 11348, pp. 125-141, 2018.
7. Bernstein D. J., Birkner P., Joye M., Lange T., Peters Ch., "Twisted Edwards Curves," Progress in Cryptology - Africacrypt, LNCS 5023, pp. 389-405, 2008.
8. Bernstein D. J., Lange T., "Faster Addition and Doubling on Elliptic Curves," Progress in Cryptology - Africacrypt, LNCS 4833, pp. 29-50, 2007.
9. Bessalova A. V., Tsygankova O. V., "Number of Curves in the Generalized Edwards Form with Minimal Even Cofactor," Problems of Information Transmission, Vol. 53, Issue 1, pp. 92-101, 2017.
10. Bianco G., Gorla E., "Compression for Trace Zero Points on Twisted Edwards Curves," Journal of Mathematical Cryptology, Vol. 10, Issue 1, pp. 15-34, 2016.
11. Dugardin M., Guilley S., Moreau M., Najm Z., Rauzy P., "Using a Modular Extension to Protect Edwards Curves Against Fault Attacks," Journal of Cryptographic Engineering, Vol. 7, pp. 321-330, 2017.
12. Edwards H., "A Normal Form for Elliptic Curves," Bulletin of the American Mathematical Society, Vol. 44, Issue 3, pp. 393-422, 2007.
13. Fournaris A. P., Dimopoulos C., Moschos A., Koufopavlou O., "Design and Leakage Assessment of Side-Channel Resistant Binary Edwards ECDSA Architectures," Microprocessors and Microsystems, Vol. 64, pp. 73-87, 2019.
14. Hu Z., Gnatyuk S., Kovtun M., Seilova N., "Method of Searching Birationally Equivalent Edwards Curves over Binary Fields," Advances in Computer Science for Engineering and Education, pp. 309-319, 2019.
15. Karthikeyan S., Jagadeeswari M., “Performance Improvement of ECC Using Low-Power High-Speed Vedic Multipliers,” *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, Issue 3, pp. 4161-4170, 2020.
16. Kim S., Yoon K., Kwon J., Park Y. H., Hong S., "New Hybrid Method for Isogeny-Based




Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026

Cryptosystems using Edwards Curves," Journal of LaTeX Class Files, Vol. 14, Issue 8, pp. 1-10, 2015.
17. Kim S., Yoon K., Park Y., Hong S., "Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves," Advances in Cryptology - ASIACRYPT 2019, pp. 273-292, 2019.
18. Koblitz N., "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
19. Maharaja J. S. S. B. K. T., "Vedic Mathematics or Sixteen Simple Mathematical Formulae from Veda," Motilal Banarsidas, Varanasi, 1965.
20. Manoj Kumar, Ankur Kumar, "A Literature Survey on Vedic Mathematics Sutras for ECC," International Journal of Research in Electronics & Computer Engineering, Vol. 7, Issue 2, pp. 1635-1644, 2019.
21. Manoj Kumar, Ankur Kumar, "Algorithms of Projective Coordinate Systems for ECC Using Vedic Mathematics," International Journal of Scientific & Technology Research, Vol. 8, Issue 8, pp. 611-621, 2019.
22. Manoj Kumar, Ankur Kumar, "Efficient and Enhanced Techniques of Ancient Mathematics for ECC," International Journal of Information Technology & Electrical Engineering, Vol. 8, Issue 5, pp. 1-7, 2019.
23. Manoj Kumar, Ankur Kumar, "Improved Cryptographic Schemes Based on Hessian and Twisted Hessian Curves Using AIVM," International Journal of Advanced Science and Technology, Vol. 29, Issue 4, pp. 10190-10202, 2020.
24. Manoj Kumar, Ankur Kumar, "Improved Performance of Cryptosystem Based on Edwards and Twisted Edwards Curves using AIVM," Journal of Critical Reviews, Vol. 7, Issue 19, pp. 5787-5799, 2020.
25. Manoj Kumar, Ankur Kumar, "Performance Analysis of Huff and Twisted Huff Curves Using AIVM Techniques," Journal of Advances in Mathematics: Scientific Journal, Vol. 9, Issue 9, pp. 7191-7199, 2019.
26. Manoj Kumar, Ankur Kumar, "Sutras of Vedic Mathematics for ECC over Jacobian Coordinates," Journal of Analysis and Computation, Vol. 12, Issue 1, pp. 1-13, 2019.
27. Manoj Kumar, Ankur Kumar, "Techniques of Vedic Mathematics for ECC over the Ring A4," International Journal of Computer Sciences and Engineering, Vol. 7, Issue 5, pp. 1330-1337, 2019.
28. Manoj Kumar, Ankur Kumar, "The Tri-Linear Pairing Map Scheme for ECC Using Vedic Mathematics," International Journal of Information Technology & Electrical Engineering, Vol. 8, Issue 3, pp. 83-89, 2019.
29. Manoj Kumar, Sudhanshu Shekhar Dubey, Ankur Kumar, "Order of Convergence by Summation Integral Type Operators," International Journal of Computer & Mathematical Sciences, Vol. 7, Issue 1, pp. 66-79, 2018.
30. Manoj Kumar, Sudhanshu Shekhar Dubey, Ankur Kumar, "Simultaneous Approximation by Mixed Summation Integral Type Operators," International Journal of Innovations & Advancement in Computer Science, Vol. 7, Issue 3, pp. 71-79, 2018.
31. Miller V. S., "Use of Elliptic Curves in Cryptography," Advances in Cryptology - CRYPT'85,
LNCS 218, pp. 417-426, 1986.
32. Moody D., "Mean Value Formulas for Twisted Edwards Curves, Journal of Combinatorics and Number Theory, Vol. 3, Issue 2, pp. 1-11, 2010.
33. Shirase M., "Coordinate System for Elliptic Curve Cryptosystem on Twisted Edwards Curve," International Conference on Consumer Electronics-Taiwan, pp. 1-6, 2016.
34. Yu W., Wang K., Li B., He X., Tian S., "Deterministic Encoding into Twisted Edwards Curves," ACISP 2016, LNCS 9723, pp. 285-297, 2016.



Paper received: 13.12.2025 Reviewed: 19.12.2025 Accepted: 28.12.2025 Published: 01.01.2026