Pi International Journal of Mathematical Sciences
© PIJMS | Volume 1 | Issue 2 | October 2025 | ISSN: 3107-9830 (Online)
Available online at: https://pijms.com/
DOI: https://doi.org/10.59828/pijms.v1i2.9

PERFORMANCE ANALYSIS OF EDWARDS ELLIPTIC CURVES USING VEDIC MATHEMATICS FOR SECURE AUTHENTICATION PROTOCOLS IN ECC

Chani Saini[1], Dr. Sandeep Kumar Tiwari[2], Dr. Ankur Nehra[3]

[1]Research Scholar, Department of Mathematics, Faculty of Science, Motherhood University, Haridwar, Uttarakhand, 24766, India

Email ID: sainichani67@gmail.com

[2]Supervisor, Department of Mathematics, Faculty of Science, Motherhood University, Roorkee, Uttarakhand, 247667, India

Email ID: fos.sandeep@motherhooduniversity.edu.in

[3]Co-supervisor, Department of Mathematics, Dhanauri P.G. College, Dhanauri, Haridwar, Uttarakhand, 247667, India

Email ID: drankurnehra648@gmail.com

Corresponding Author: Chani Saini, Research Scholar (sainichani67@gmail.com)

Received: 01 October 2025 | **Accepted:** 25 October 2025 | **Published:** 30 October 2025

ABSTRACT

In order to create effective implementations of point addition and point doubling algorithms for Edwards elliptic curves, this paper investigates the use of Vedic mathematical approaches. The goal of the suggested approach is to improve Edwards elliptic curve cryptography (ECC) procedures processing efficiency. In particular, the Urdhva-Tiryagbhyam sutra is used to optimize multiplication procedures, and the Dvandva-yoga method is used to speed up squaring operations. These methods are used to provide two optimized cryptographic formulations for Edwards elliptic curves: point addition and point doubling. In terms of execution speed, processing time, and lower multiplier power consumption, experimental evaluations show that the Vedic mathematics-based methodology performs noticeably better than traditional arithmetic methods. Point addition and scalar operations are implemented in MATLAB utilizing 16-bit and 32-bit operands. Additionally, a number of Vedic mathematical methods are examined to determine how they affect elliptic curve calculations; the findings are displayed using detailed tables and graphical representations. The results demonstrate how Vedic mathematics can significantly increase the effectiveness and performance of elliptic curve cryptography systems.

Keywords: *Finite field, UTT, DYT, EEC, Points addition, Point doubling.*

MSC: *94A60, 14G50*

1. Introduction

Elliptic curves have been essential to the development of cryptography methods for a number of decades. Elliptic curves can be represented in a variety of ways, such as Weierstrass, Edwards, Hessian, Huff, and Jacobi forms. These alternative models are particularly significant in cryptography because they enable effective computational operations like point addition and point doubling. This work focuses on two such alternative models: the Edwards curve and the twisted Edwards curve. The Edwards curve, introduced by Harold Edwards in 2007, represents a family of elliptic curves characterized by simple and efficient arithmetic operations. The twisted Edwards curve, proposed and analyzed by Bernstein, Birkner, Joye, Lange, and Peters in 2008, generalizes the Edwards curve and significantly broadens its applicability. Subsequently, Hisil et al. (2008) derived explicit and complete addition formulas for twisted Edwards curves, enabling uniform and secure implementations. In 2015, Kim, Yoon, Kwon, Park, and Hong proposed a hybrid isogeny-based cryptosystem employing Edwards curves, reflecting the growing interest in isogeny-based approaches due to their compatibility with classical elliptic curve structures and relatively small key sizes. Further advancements include the coordinate system for twisted Edwards curves introduced by Shirase (2016), which utilizes extended coordinates and achieves scalar doubling costs comparable to the lowest known mixed-coordinate methods while simplifying scalar multiplication. In parallel, Bianco and Gorla (2016) presented optimal representations for elements of prime-order subgroups on twisted Edwards curves, along with efficient compression and decompression algorithms and a comparative performance analysis against Weierstrass-form curves. Addressing practical security concerns, Dugardin, Guilley, Moreau, Najm, and Rauzy (2017) examined extension fault attack models and proposed effective countermeasures for elliptic curve scalar multiplication, demonstrating protected implementations on Edwards and twisted Edwards curves. In the same year, Bessalova and Tsygankova (2017) investigated points of orders 2, 4, and 8 on generalized Edwards curves and classified these curves into three distinct categories. The applicability of Edwards curves to post-quantum cryptography was further explored by Azarderakhsh, Lang, Jao, and Koziel (2018), who implemented the supersingular isogeny Diffie–Hellman (SIDH) key exchange protocol on Edwards curves, achieving improved resistance to side-channel attacks through complete curves and unified addition formulas. Moreover, Kim, Yoon, Park, and Hong (2019) demonstrated the advantages of Edwards curves in isogeny computations by employing degree-invariant odd-degree isogenies, particularly in recovering image curve coefficients. Meanwhile, Hu, Gnatyuk, Kovtun, and Seilova (2019) proposed an efficient and secure method for analyzing birationally equivalent Edwards curves over finite fields, contributing to optimized digital signature schemes. Furthermore, Fournaris, Dimopoulos, Moschos, and Koufopavlou (2019) introduced an organized framework for scalar multiplication and elliptic curve digital signature algorithms based on twisted Edwards curves, highlighting their completeness, uniform execution behavior, and resistance to side-channel attacks. Collectively, these studies underscore the significant role of Edwards and twisted Edwards curves in modern public-key cryptographic systems. Motivated by these findings, the present work explores the application of multiple Ancient Indian Vedic Mathematics (AIVM) techniques to Edwards and twisted Edwards curves to enhance the performance of ECC-based cryptosystems.

2. Literature Review

Elliptic Curve Cryptography (ECC) ka aaghaz Miller (1986) aur Koblitz (1987) ke kaam se hua, jisme elliptic curves ko public key cryptosystems ke liye ek efficient aur secure framework ke roop me prastut kiya gaya; baad me Edwards (2007) ne elliptic curves ka ek naya normal form introduce kiya jisme point addition aur doubling ke liye saral aur fast formulas uplabdh hue, jise Bernstein aur Lange (2007) aur Bernstein et al. (2008) ne aage badhate hue Twisted Edwards curves ke roop me generalize kiya, jo zyada elliptic curves ko cover karti hain aur cryptographic implementations me behtar performance deti hain. Iske baad kai researchers ne in curves ke mathematical aur structural aspects par kaam kiya, jaise Ashraf aur Kirlar (2012) ka alternate models ka study, Moody (2010) ke mean value formulas, aur Bessalova aur Tsygankova (2017) ka minimal even cofactor par analysis, jo security parameters ke liye mahatvapurn hai. Implementation efficiency badhane ke liye Bianco aur Gorla (2016) ne point compression, Yu et al. (2016) ne deterministic encoding, aur Shirase (2016) ne optimized coordinate systems propose kiye, jabki practical security ke liye Dugardin et al. (2017) aur Fournaris et al. (2019) ne fault aur side-channel attack resistant Edwards curve architectures par kaam kiya. Recent research me Edwards curves ka role post-quantum cryptography me bhi ubhar kar aaya, jahan Azarderakhsh et al. (2018) ne EdSIDH scheme ke madhyam se supersingular isogeny Diffie–Hellman ko Edwards curves par implement kiya aur Kim et al. (2015, 2019) ne isogeny computation ke optimized methods develop kiye, saath hi Hu et al. (2019) ne binary fields me birationally equivalent Edwards curves search karne ke techniques di; 2020 se 2025 tak ke studies me hardware acceleration, lightweight aur IoT applications, secure parameter selection, aur quantum-resistant cryptographic schemes par focus raha, jisse yeh spasht hota hai ki Edwards aur Twisted Edwards curves aaj bhi modern cryptography ka ek mahatvapurn aur sakriya research area bani hui hain.

3. Fundamentals of Dvandva-Yoga and Urdhva-Tiryagbhyam Techniques

This section introduces selected Ancient Indian Vedic Mathematics (AIVM) techniques, namely the Dvandva-yoga and Urdhva-Tiryagbhyam methods. These approaches are subsequently employed to improve the computational efficiency of the proposed ECC-based cryptosystem.

3.1. Urdhva Tiryagbhyam [14]

The general multiplication technique known as the **Urdhva-Tiryagbhyam** method can be applied to a wide range of arithmetic operations. The terms *Urdhva* and *Tiryagbhyam* respectively mean “vertically” and “crosswise.” This multiplication approach is based on an Ancient Indian Vedic Mathematics (AIVM) algorithm that performs calculations simultaneously in vertical and crosswise directions. The Urdhva-Tiryagbhyam method enables efficient and parallel computation, making it well-suited for high-speed arithmetic operations. The following section presents illustrative models and step-by-step procedures demonstrating the application of the Urdhva-Tiryagbhyam technique.

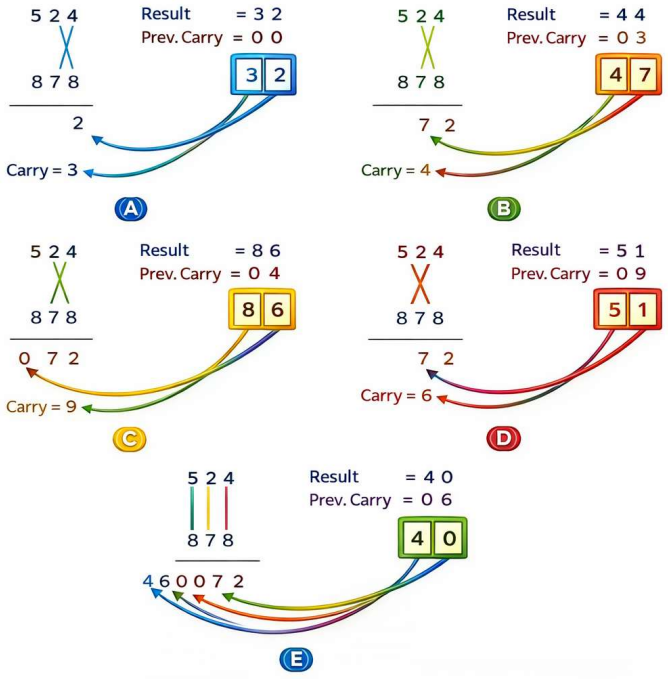

Figure 1: Urdhva-tiryagbhyam Technique for three digits

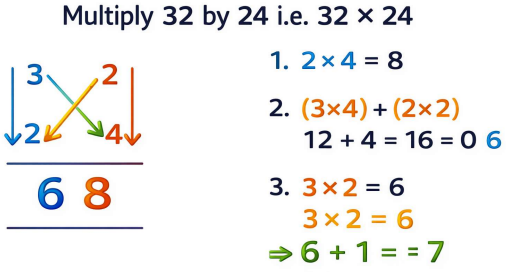

Figure 2: Urdhva-tiryagbhyam Technique for two digits

3.2. Dvandva-Yoga Sutra

The Dvandva-yoga sutra is a principle from Vedic Mathematics that provides an efficient method for performing squaring operations, especially for binary and digital numbers. The term Dvandva means pair or duality, and yoga means combination or addition. Together, the sutra focuses on computing the square of a number by systematically combining pairs of digits and summing their products.

Explanation:

In the Dvandva-yoga method, the square of a number is calculated by:

1. Squaring each digit.
2. Adding twice the product of every possible pair of digits.
3. Arranging these partial results according to their positional weights.
4. Combining the results to obtain the final square efficiently.

This approach reduces the number of intermediate steps compared to conventional squaring methods, making it faster and more hardware-efficient.

Importance in ECC: In elliptic curve cryptography (ECC), squaring operations are frequently used in point addition and point doubling algorithms. By applying the Dvandva-yoga sutra, squaring operations can be

executed with lower computational complexity, reduced processing time, and decreased power consumption. This makes the sutra particularly valuable for high-performance and low-power cryptographic implementations.

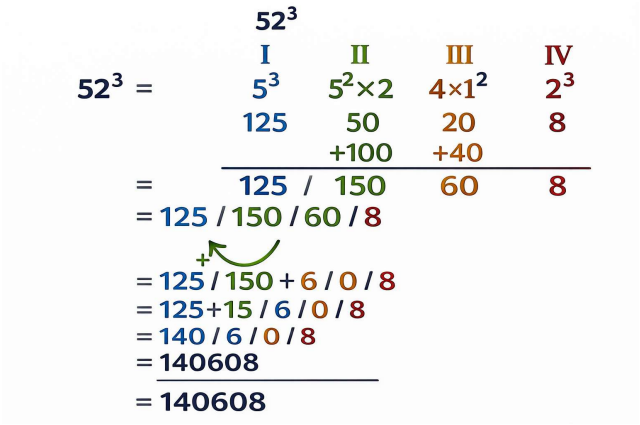

Figure 3: Dvandva-yoga Technique for two digits

4. Edwards Elliptic Curves (EEC)

The mathematical foundation of Edwards' elliptic curves, that is, regular and twisted Edwards elliptic curves, will be discussed in this section.

4.1. OEEC (Ordinary Edwards Elliptic Curve)

A typical elliptic curve for Edwards E_d across a field F in one boundary d is described as

$$x^2 + y^2 = 1 + d\,x^2 y^2 \tag{1}$$

where $d \in F - \{0,1\}$ and $char(F) \neq 2$.

In a set-builder form, the curve (3.1.1) can be composed as

$$E_d = \left\{ (x,y) : x^2 + y^2 = 1 + d\,x^2 y^2 \right\} \tag{2}$$

Another summarized form of an Edwards elliptic curve with two boundaries, c and d, is described as

$$x^2 + y^2 = c^2 \left(1 + d\,x^2 y^2\right) \tag{3}$$

In set-builder form, the curve (3.1.3) can be written as

$$E_{c,d} = \left\{ (x,y) : x^2 + y^2 = c^2 \left(1 + d\,x^2 y^2\right) \text{ and } c\,d\left(1 - c^4 d\right) \neq 0 \right\} \tag{4}$$

Edwards Elliptic Curve Set Addition Law E_d

Let P = (x_1, y_1), Q = (x_2, y_2), and R = (x_3, y_3). Then, R = P + Q, then R is provided by

$$x_3 = \frac{(x_1\,y_2 + x_2\,y_1)}{(1 + d\;x_1\,x_2\,y_1\,y_2)} \tag{5}$$

$$y_3 = \frac{(y_1\,y_2 - x_1\,x_2)}{(1 - d\,x_1\,x_2\,y_1\,y_2)} \tag{6}$$

$$x_3 = \frac{(x_1\,y_1 + x_2\,y_2)}{(x_1\,x_2 + y_1\,y_2)} \tag{7}$$

$$y_3 = \frac{(x_1\,y_1 - x_2\,y_2)}{(x_1\,y_2 - x_2 y_1)} \tag{8}$$

4.2. TEEC (Twisted Edwards Elliptic Curve)

An Edwards curve that is twisted $T_{a,d}$ is an Edwards curve's location. E_d, and is distinguished by the configuration of focuses (x,y) satisfying the requirement

$$a x^2 + y^2 = 1 + d x^2 y^2 \tag{9}$$

4.2.1. Addition of P and Q on $T_{a,d}$

Let P = (x_1, y_1), Q = (x_2, y_2), and R = (x_3, y_3). Then, R = P + Q, then R is provided by

i.e. $R = P + Q$

where $$x_3 = \frac{(x_1 y_2 + x_2 y_1)}{(1 + d\, x_1 x_2 y_1 y_2)} \tag{10}$$

and $$y_3 = \frac{(y_1 y_2 - a\, x_1 x_2)}{(1 - d\, x_1 x_2 y_1 y_2)} \tag{11}$$

Remark-.1: If we put

$$d = \frac{\left(x_1^2 - x_2^2\right) - \left(x_1^2 y_2^2 - y_1^2 x_2^2\right)}{x_1^2 x_2^2 \left(y_1^2 - y_2^2\right)} \text{ and } a = \frac{\left(x_1^2 y_1^2 - x_2^2 y_2^2\right) - y_1^2 y_2^2 \left(x_1^2 - x_2^2\right)}{x_1^2 x_2^2 \left(y_1^2 - y_2^2\right)}$$

They then decrease to the corresponding d-autonomous structure in the aforementioned formulas.

$$x_3 = \frac{(x_1\, y_1 + x_2\, y_2)}{(a\, x_1\, x_2 + y_1\, y_2)} \tag{12}$$

$$y_3 = \frac{(x_1\, y_1 - x_2\, y_2)}{(x_1\, y_2 - x_2 y_1)} \tag{13}$$

5. COORDINATES SYSTEM FOR EEC [17]

The homogeneous projective for EEC is employed in cryptography to prevent the Edwards extension formulas from being inverted. Each unique elliptic curve point P with affine coordinates (x, y) is mapped to a point P' with projective coordinates (X, Y, Z) using the following adjustments in the projective direction framework, a three-dimensional coordinate system:

$$(x,\, y) \to \left(\frac{X}{Z}, \frac{Y}{Z}\right) \tag{14}$$

E_d and $T_{a,d}$ curves in the projective directions framework, separately, can be addressed as follows, utilizing the change (2.4) above.

$$\left(X^2 + Y^2\right) Z^2 = Z^4 + d\, X^2 Y^2 \tag{15}$$

$$\left(a\, X^2 + Y^2\right) Z^2 = Z^4 + d\, X^2 Y^2 \tag{16}$$

6. Proposed Schemes

We will discuss some efficient cryptographic schemes in this section that use projective homogeneous directions and AIVM techniques to add and multiply Edwards elliptic curves, specifically the normal OEEC and TEEC.

Addition of P and Q on OEEC: Algorithm 1

With the help of the above equations, we get,

$$P(X_1,Y_1,Z_1)+Q(X_2,Y_2,Z_2)=R(X_3,Y_3,Z_3)$$

where $X_3=Z_1Z_2\left(Z_1^2Z_2^2-d\,X_1X_2Y_1Y_2\right)\left(X_1Y_2+X_2Y_1\right)$

$Y_3=Z_1Z_2\left(Z_1^2Z_2^2-d\,X_1X_2Y_1Y_2\right)\left(Y_1Y_2-X_1X_2\right)$

and $Z_3=\left(Z_1^2Z_2^2-d\,X_1X_2Y_1Y_2\right)\left(Z_1^2Z_2^2+d\,X_1X_2Y_1Y_2\right).$

Using AIVM techniques, the related algorithm is now explained as follows:

Input:	$P\equiv(X_1,Y_1,Z_1)$, $Q\equiv(X_2,Y_2,Z_2)$ and d	
Output:	$R=P+Q\equiv(X_3,Y_3,Z_3)$	
1		$A=Z_1\cdot Z_2$
2		$B=X_1\cdot Y_2$
3		$C=X_2\cdot Y_1$
4		$D=Y_1\cdot Y_2$
5		$E=X_1\cdot X_2$
6		$F=d\cdot D\cdot E$
7		$G=B+C$
8		$H=A^2-F$
9		$I=A^2+F$
10		$J=D-E$
11		$X_3=A\cdot G\cdot H$
12		$Y_3=A\cdot I\cdot J$
13		$Z_3=H\cdot I$
14		$X_3=A\cdot G\cdot H$
15		$Y_3=A\cdot I\cdot J$
16		*Return* $(X_3:Y_3:Z_3)$

where A^2 is processed utilizing the AIVM Urdhva-tiryagbhyam strategy and A, B, C, D, E, F is figured utilizing the Dvandva-yoga procedure.

Doubling P on OEEC: Algorithm 2

With the help of the above equations, we get,

$$P(X_1,Y_1,Z_1)+P(X_1,Y_1,Z_1)=R(X_3,Y_3,Z_3)$$

where $X_3=2X_1Y_1Z_1^2\left(Z_1^4-d\,X_1^2Y_1^2\right)$

$Y_3=Z_1^2\left(Y_1^2-X_1^2\right)\left(Z_1^4+d\,X_1^2Y_1^2\right),$

and $Z_3=\left(Z_1^4+d\,X_1^2Y_1^2\right)\left(Z_1^4-d\,X_1^2Y_1^2\right)$

Using AIVM techniques, the appropriate algorithm is now explained as follows.

Input :	$P \equiv (X_1, Y_1, Z_1)$, 'd'	
Output :	$R = P + P = 2P \equiv (X_3, Y_3, Z_3)$	
1		$A = X_1^2$
2		$B = Y_1^2$
3		$C = Z_1^2$
4		$D = d \cdot A \cdot B$
5		$E = 2 \cdot X_1 \cdot Y_1$
6		$F = C^2 - D$
7		$G = C^2 + D$
8		$H = B - A$
9		$X_3 = E \cdot C \cdot F$
10		$Y_3 = C \cdot G \cdot H$
11		$Y_3 = F \cdot G \cdot F$
12		$X_3 = F \cdot G \cdot H$
11		$Z_3 = F \cdot G \cdot H$
12		*Return* (X_3, Y_3, Z_3)

Where D, E is computed using the AIVM Urdhva-tiryagbhyam approach and C^2, X_1^2, Y_1^2, Z_1^2 is computed using the Dvandva-yoga technique.

Addition of P & Q on TEEC: Algorithm 3

With the help of the above equations, we get,

$$P(X_1, Y_1, Z_1) + Q(X_2, Y_2, Z_2) = R(X_3, Y_3, Z_3)$$

where $X_3 = (X_1Y_2 - X_2Y_1)(X_1Y_1Z_2^2 - X_2Y_2Z_1^2)$

$Y_3 = (Y_1Y_2 - a\,X_1X_2)(X_1Y_1Z_2^2 - X_2Y_2Z_1^2)$

And $Z_3 = Z_1Z_2(X_1Y_2 - X_2Y_1)(Y_1Y_2 - a\,X_1X_2)$.

The matching method that makes use of AIVM techniques is now explained as follows.

Input :	$P \equiv (X_1, Y_1, Z_1), Q \equiv (X_2, Y_2, Z_2),\ a$	
Output :	$R = P + Q \equiv (X_3, Y_3, Z_3)$	
1		$A = X_1 \cdot Y_1$
2		$B = X_2 \cdot Y_2$
3		$C = X_1 \cdot Y_2$
4		$D = X_2 \cdot Y_1$
5		$E = Y_1 \cdot Y_2$
6		$F = X_1 \cdot X_2$
7		$G = Z_1 \cdot Z_2$
8		$H = Z_1^2$
9		$I = Z_2^2$
10		$J = C - D$
11		$K = E + a \cdot F$
12		$L = A \cdot I$
13		$M = B \cdot H$
14		$X_3 = J \cdot (L + M)$
15		$Y_3 = K \cdot (L - M)$
16		$Z_3 = J \cdot K \cdot G$
17		$X_3 = J \cdot (L + M)$
17		$Z_3 = J \cdot K \cdot G$
17		*Return* (X_3, Y_3, Z_3)

Above all calculation can be calculated by the Vedic Formulae

Doubling of P on TEEC: Algorithm 4

With the help of the above equations, we get,

$$P(X_1,Y_1,Z_1)+P(X_1,Y_1,Z_1)=R(X_3,Y_3,Z_3)$$

where $X_3=2X_1Y_1\left(a\,X_1^2+Y_1^2-2Z_1^2\right)$

$$Y_3=\left(a\,X_1^2+Y_1^2\right)\left(a\,X_1^2-Y_1^2\right)$$

and $Z_3=\left(a\,X_1^2+Y_1^2\right)\left(a\,X_1^2+Y_1^2-2Z_1^2\right)$

Using AIVM techniques, the related algorithm is now explained as follows:

Input:	$P\equiv(X_1,Y_1,Z_1)$ and 'α'
Output:	$R=2P\equiv(X_3,Y_3,Z_3)$
1	$A=X_1$
2	$B=Y_1$
3	$C=Z_1^2$
4	$D=\alpha\cdot A^2$
5	$E=D+B^2$
6	$F=E-2\cdot C$
7	$G=D-B^2$
8	$X_3=2\cdot A\cdot B\cdot F$
9	$Y_3=E\cdot G$
10	$Z_3=E\cdot F$
11	$X_3=2\cdot A\cdot B\cdot F$
10	$Y_3=E\cdot G$
11	*Return* (X_3,Y_3,Z_3)

Where D, E, F, 2ABF is computed using the UTT technique and A^2, B^2, Z_1^2 is computed using the DTT.

7. Result Analysis and Comparison

Tables 6.1 and 6.2 provide a close look at the number of math tasks, such as duplication, squares, three-dimensional forms, and other higher powers that are used to add two specific or comparative focuses in OEEC and TEEC using both classic strategy and AIVM methods.

Table 1 shows how many operations are required for point addition on OEEC and TEEC.

Curves	Conventional Method for Point Addition					AIVM techniques for Point Addition				
	P_1	P_2	P_3	P_4	S	P_1	P_2	P_3	P_4	S
TEEC	23	4	0	0	27	14	2	0	0	16
OEEC	31	8	0	0	39	12	1	0	0	13

Table 2. The number of steps required in OEEC and TEEC to double a point is compared

Curves	Conventional method for Point Doubling					AIVM techniques for Point Doubling				
	P_1	P_2	P_3	P_4	S	P_1	P_2	P_3	P_4	S
TEEC	12	12	0	0	24	7	3	0	0	10
OEEC	14	2	0	4	20	9	4	0	0	13

Table 1 shows that the percentage of jobs involved in point expansion using AIVM techniques decreased to around 40% and 66% for OEEC and TEEC, respectively. Table 2 illustrates that the number of juggling activities used, specifically when multiplication employing AIVM procedures for OEEC and TEEC, is 35% and 58% less than that of standard techniques, respectively. Tables 3 and 4 show the maintenance and time savings for center extension and point duplication in the OEEC and TEEC, using 8-piece and 16-cycle processors independently. AIVM techniques reduce handling time for focus expansion by 89.53% in OECC and 88.1433% in TEEC for 8-bit processors. Point multiplication reduces handling time, reserves funds by 86.5324% in TEEC and 86.5656% in OEEC. AIVM techniques reduce handling time savings for focus expansion by 92.2065% in OECC and 92.1158% in TEEC for 16-bit processors, and point multiplying reduces handling time reserve funds by 91.3922% in E_d curve and 91.4011% in $T_{a,d}$ curve.

Table 3. Processing times for mathematical operations in EEC and TEEC based on an 8-bit CPU using traditional and AIVM methods

Curves	Points Addition			Point Doubling		
	T^{A}_{ECC} (In seconds)	T^{A}_{VECC} (In Seconds)	T^{A}_{S} (In %)	T^{D}_{ECC} (In seconds)	T^{D}_{VECC} (In Seconds)	T^{D}_{S} (In %)
OEEC	0.0100961	0.00101582	89.93934	0.00802286	0.0010788	86.56307
TEEC	0.0093021	0.00110263	88.14625	0.00756117	0.00102579	86.43471

Table 4: Shows the processing times for arithmetic operations in EEC and TEEC based on a 16-bit CPU using both traditional and AIVM approaches.

Curves	Points Addition			Point Doubling		
	T^{A}_{ECC} (In seconds)	T^{A}_{VECC} (In Seconds)	T^{A}_{S} (In %)	T^{D}_{ECC} (In seconds)	T^{D}_{VECC} (In Seconds)	T^{D}_{S} (In %)
OEEC	0.0105821	0.000824673	92.20687	0.00797328	0.000685790	91.39881
TEEC	0.00933162	0.000735544	92.11784	0.00787529	0.000677214	91.40071

Different types of arithmetic assignments expected in OEEC and TEEC for focus expansion and point multiplying separately are shown in Figures 1 and 2. The fig.1 and 2 make it evident that solid form activities for focus expansion and point multiplication in the two Edwards elliptic curves are not used in AIVM methods, demonstrating the value of AIVM strategies in accelerating the speed of ECC-based cryptosystems.

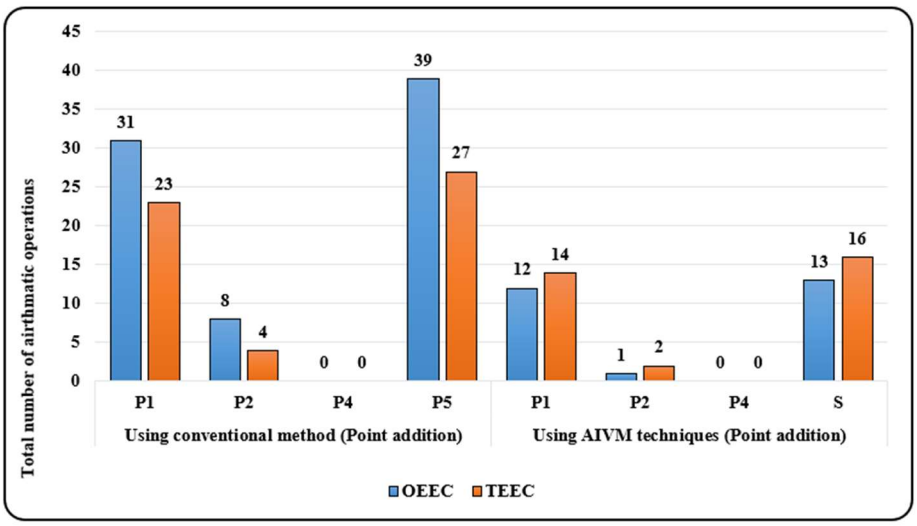

Fig.1. Comparison of different types of arithmetic operations required for point addition in OEEC and TEEC

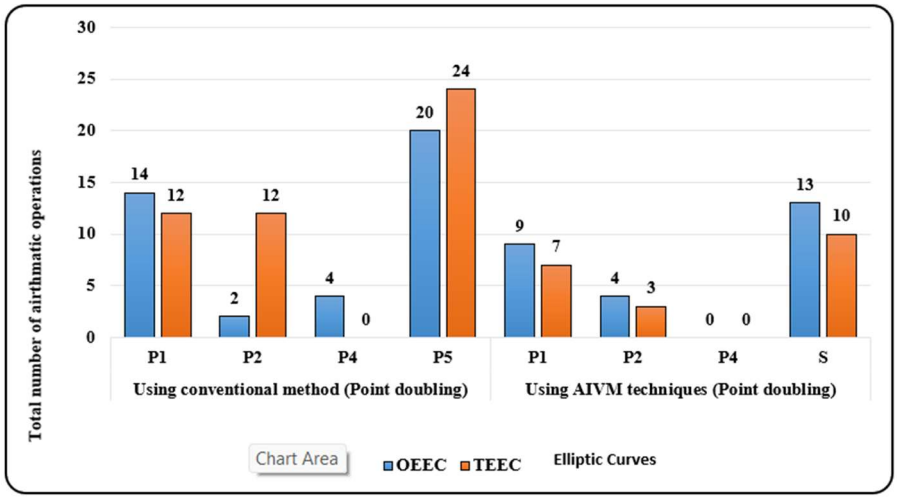

Figure 2: A comparison of the various arithmetic operations needed for point doubling in TEEC and OEEC

8. Conclusion

This paper presented a comprehensive performance analysis of Edwards elliptic curves using Vedic mathematics to enhance secure authentication protocols in elliptic curve cryptography (ECC). By integrating Vedic mathematical techniques into core ECC operations, efficient implementations of point addition and point doubling algorithms were developed. The Urdhva-Tiryagbhyam sutra was employed to optimize multiplication operations, while the Dvandva-yoga method was utilized to accelerate squaring computations, both of which are critical to elliptic curve arithmetic. Experimental results obtained through MATLAB simulations using 16-bit and 32-bit operands demonstrate that the proposed Vedic mathematics–based approach significantly outperforms conventional arithmetic methods. Improvements were observed in execution speed, processing time, and power efficiency of multipliers, highlighting the suitability of the proposed techniques for resource-constrained cryptographic environments. The comparative analysis, supported by detailed tables and graphical representations, confirms that Vedic arithmetic effectively reduces computational complexity without compromising cryptographic security. Overall, the findings establish that incorporating Vedic mathematics into Edwards elliptic curve operations offers a promising pathway for developing high-performance and energy-efficient ECC-based authentication protocols. The proposed approach can be effectively extended to hardware implementations and advanced elliptic curve models, making it a valuable contribution to secure and efficient cryptographic system design.

References

[1]. Ashraf M., and Kirlar B. B., “On the Alternate Models of Elliptic Curves”, International Journal of Information Security Science, 1(2), 49-66, 2012.

[2]. Azarderakhsh R, Lang E. B, Jao D, Koziel B., EdSIDH: Supersingular Isogeny Diffie-Hellman Key Exchange on Edwards Curves, Springer Nature Switzerland AG 2018, SPACE 2018, LNCS 11348, pp. 125–141, 2018.

[3]. Bernstein D. J and Lange T., “Faster addition and doubling on elliptic curves. Progress in Cryptology - Africacrypt 2007”, Lecture Notes in Computer Science Vol. 4833, Springer, 29-50, 2007.

[4]. Bernstein D. J, Birkner P., Joye M., Lange T., and Peters Ch., “Twisted Edwards curves,” Progress in Cryptology AFRICACRYPT 2008; LNCS 5023, 389–405, Springer (2008).

[5]. Bessalova A. V., Tsygankova O. V., "Number of Curves in the Generalized Edwards Form with Minimal Even Cofactor of the Curve Order", Problems of Information Transmission, 53(1), 92-101, 2017.

[6]. Bianco G, Gorla E., "Compression for trace zero points on twisted Edwards curves," J. Math. Cryptol, 10 (1), 15-34, 2016.

[7]. Dugardin M, Guilley S, Moreau M, Najm Z, Rauzy P., "Using a modular extension to provably protect Edwards curves against fault attacks Springer-Verlag Berlin Heidelberg, Journal of Cryptographic Engineering. 7, 321-330, 2017.

[8]. Edwards H., "A normal form for elliptic curves. In: Bulletin of the American Mathematical Society, 44(3), 393-422, 2007.

[9]. Fournaris A. P., Dimopoulos C, Moschos A., Koufopavlou O., "Design and leakage assessment of side-channel attack resistant binary Edwards Elliptic Curve digital signature algorithm architectures", Microprocessors and Microsystems (Elsevier), 64, 73-87, 2019.

[10]. Hu Z, Gnatyuk S, Kovtun M, Seilova N., "Method of Searching Birationally Equivalent Edwards Curves Over Binary Fields, International Conference on Computer Science", Engineering and Education Applications, Advances in Computer Science for Engineering and Education, 309-319, 2019.

[11]. Kim S, Yoon K, Kwon J, Park Y H, Hong S., "New hybrid method for isogeny-based cryptosystems using Edwards curves, Journal of LATEX class files", 14(8),1-10, 2015.

[12]. Kim S, Yoon K, Park Y, Hong S., "Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves, International Conference on the Theory and Application of Cryptology and Information Security", ASIACRYPT 2019: Advances in Cryptology – ASIACRYPT, 273-292, 2019.

[13]. Koblitz N., "Elliptic curve cryptosystems", Mathematics of Computation, 48, 203–209, 1987.

[14]. Maharaja J. S. S. B. K. T., "Vedic Mathematics or Sixteen Simple Mathematical Formulae from Veda", Motilal Banarsidas, Varanasi (India,1965). J. Clerk Maxwell. A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 68-73, 1892.

[15]. Miller V. S., "Use of elliptic curves in cryptography", Advances in Cryptology Proceedings of Crypt' 85, Lecture Notes in Computer Science, 218, Springer-Verlag, 417–426, 1986.

[16]. Moody D, "Mean value formulas for twisted Edwards curves", Journal of Combinatorics and Number Theory, 3(2), 1-11, 2010.

[17]. Shirase M., "Coordinate System for Elliptic Curve Cryptosystem on Twisted Edwards Curve", International Conference on Consumer Electronics-Taiwan, 978-1-5090-2073-7/16, 2016.

[18]. Yu W, Wang K, Li B, He X, Tian S., "Deterministic Encoding into Twisted Edwards Curves", International Publishing Switzerland, (Springer), ACISP 2016, Part II, LNCS 9723, 285-297, 2016.

Cite this Article:

Chani Saini, Dr. Sandeep Kumar Tiwari, Dr. Ankur Nehra, PERFORMANCE ANALYSIS OF EDWARDS ELLIPTIC CURVES USING VEDIC MATHEMATICS FOR SECURE AUTHENTICATION PROTOCOLS IN ECC", Pi International Journal of Mathematical Sciences, ISSN: *3107-9830 (Online), Volume 1, Issue 2, pp. 44-55, October 2025.*

Journal URL: *https://pijms.com/*

DOI: *https://doi.org/10.59828/pijms.v1i2.9*