



---

## **SOLUTION OF MATHEMATICAL PROBLEMS BY ANCIENT VEDIC MATHEMATICAL TECHNIQUES**

**<sup>1</sup>Shubham, <sup>2</sup>Dr. Mahender Poonia**

<sup>1</sup>Research Scholar, <sup>2</sup>Supervisor

<sup>1-2</sup> Department of Mathematics, Om Sterling Global University, Hisar (Haryana)

### **Abstract**

Vedic Mathematics represents a time-honored framework of numerical understanding, deeply embedded in the Vedas, which are the revered scriptures of ancient India. It offers a collection of methods for executing numerical and algebraic computations with efficiency and ease. In the early 20th century, Bharati Krishna Tirthaji brought forth these innovative techniques, rooted in 16 primary sutras and 13 supplementary ones. These principles simplify intricate calculations, enabling effortless mental execution. Although Vedic Mathematics has found extensive application in academic settings, especially for competitive assessments, its possibilities within contemporary computational domains are still predominantly uncharted. Recent studies have revealed that these time-honored methods can be transformed for application in cryptography, artificial intelligence (AI), and advanced computing, providing remarkable enhancements in computational effectiveness. This paper aims to delve into the utilization of Vedic Mathematics methods within the realm of elliptic curve cryptography (ECC), with a particular emphasis on the Huff and twisted Huff elliptic curves. This document delves into the mathematical foundations of these curves, explores the utilization of Vedic Mathematics to enhance algorithms for point addition and point doubling, and highlights the performance advancements realized. The findings indicate that employing ancient methodologies can lead to a remarkable decrease in both the quantity of calculations and the duration needed for elliptic curve computations. The findings indicate the promise of integrating ancient mathematical techniques into modern computational systems, paving the way for further research in this area.

**Keywords:** Vedic Mathematics, Cryptography, Huff Curves, AIVM, Elliptic Curves, Point Addition, Point Doubling

### **1 INTRODUCTION**

In this scholarly exploration, elliptic curves have garnered significant attention within the realms of algebraic geometry and number theory, tracing their extensive examination back to the mid-nineteenth century. Subsequently, numerous frameworks such as the Edwards curve [1], Hessian curves [2], and Jacobi curves [3] have been introduced by a range of scholars to enhance the efficacy of cryptographic systems reliant on these elliptic curves. In 1948, Huff [4] introduced a specific model for these elliptic curves to explore a Diophantine problem. In recent times, elliptic curves have swiftly gained traction in the development of effective algorithms for decomposing substantial integers and in the creation of streamlined cryptographic systems, particularly for mobile devices and wireless communication networks. In the year 2010, a novel advancement of the Huff curve was introduced by Joye and colleagues in a publication titled "Huff's model for elliptic curves." This document introduces rapid, clear expressions for the addition and doubling of points on Huff curves. In the year 2011, Devigne and Joye [6] elucidated the principles governing the addition law pertaining to binary Huff curves. Meanwhile, Ciss and Sow [7] introduced an extension of Huff curves, and in the following year, they showcased the computation of Tate pairing on these extended Huff curves.

In 2015, Gu and colleagues proposed a highly effective method for pairing computation utilizing Huff curves. In the year 2017, Jafri and Islam proposed a refined framework for cohesive binary Huff curves.



Subsequently, Sadek and colleagues [10] employed Huff curves to assess the Gaussian hypergeometric series. Not long ago, Drylo and colleagues [11] introduced effective Montgomery-style equations on the generalized Huff curve, aimed at their use in isogeny-based cryptography. This study employs various methodologies derived from the ancient wisdom of Vedic Mathematics to enhance the efficiency of cryptosystems utilizing Huff curves.

Vedic Mathematics represents a mathematical framework rooted in the ancient Indian scriptures known as the Vedas, which have intrigued scholars, educators, and mathematicians for centuries. The Vedas, revered as the most ancient texts of human culture, encompass a vast reservoir of wisdom, laying the groundwork for mathematics, scientific principles, spiritual insights, and philosophical thought, among numerous other domains. Within these compositions, the numerical concepts were conveyed not through conventional methods but rather through enigmatic verses or maxims, the deciphering of which, in essence, forms a coherent framework for addressing mathematical challenges.

The emergence of Vedic Mathematics as a distinct framework is credited to Bharati Krishna Tirthaji, a renowned Indian intellectual and spiritual figure, who brought these ancient techniques back to life in the early 20th century. Tirthaji showcased these approaches with remarkable clarity in his groundbreaking work, Vedic Mathematics, released in 1911. In this influential text, he asserted that the methods were unearthed within the Vedic scriptures, embodying a timeless Indian-Hindu legacy of numerical insight. In his reproduction, he asserts that the 16 notable sutras and the 13 supplementary sutras are designed to simplify remarkably complex mathematical operations through mental computation, offering not only swiftness but also a comprehensive understanding of mathematical principles [1]. In contrast to conventional methods of arithmetic and algebra that often rely on sequential steps and written calculations, Vedic Mathematics proposes a variety of techniques that can be performed mentally. These approaches not only expedite calculations but also enhance the comprehension of the mathematical frameworks derived from them. The system's design is elegant and straightforward; it presents methods that require minimal steps, while also empowering the practitioner to address challenges instinctively. Given that Vedic Mathematics presents a different approach to calculation compared to Western techniques, one might find it appealing to incorporate it into contemporary practices.

The adaptability is the unique strength of Vedic Mathematics. The methods can be applied broadly in various mathematical endeavors such as adding, taking away, multiplying, and dividing, as well as in more advanced areas like algebra, geometry, and even calculus [3]. The approaches enable effective processing within the mind, especially regarding competition, particularly in educational assessments. In reality, both Indian and global enthusiasts of Vedic Mathematics have attracted a significant number of adherents, recognizing it as an effective approach for educating students to excel in various competitive assessments, particularly those demanding swift problem-solving skills.

Beyond its role in education, Vedic Mathematics is increasingly being utilized in various modern domains of computation, particularly within cryptography, artificial intelligence, and numerical algorithms. The ancient Vedic methods of multiplication hold the potential to enhance the efficacy of encryption techniques in the realm of cryptography, where rapidity and safety are paramount considerations. For instance, the Vedic technique for multiplication, such as the widely recognized Urdhva Tiryagbhyam (vertical and crosswise) method, can yield enhanced computations for cryptographic systems, leading to fortified communications that require minimal computational resources. Furthermore, scholars have embarked on utilizing ancient Vedic techniques within the realm of artificial intelligence, particularly in the development of enhanced algorithms for machine learning and the resolution of optimization challenges. Fields that demand swift and reliable computations are poised to benefit immensely from the time-efficient and precise methodologies offered by



Vedic Mathematics [3]. Integrating ancient Vedic techniques with contemporary computational frameworks is an intriguing area of investigation, with potential applications in advanced computing and perhaps even in the realm of quantum technology. Nonetheless, while Vedic Mathematics presents clear advantages, there are also numerous challenges associated with its application. The absence of comprehensive understanding and training related to the system stands as one of the foremost challenges. While the contemporary resurgence of this tradition draws inspiration from Tirthaji's contributions, a significant portion of the sutras and methodologies remains obscure to the broader public and is not readily accessible. As a result, it is essential to establish more structured educational frameworks aimed at imparting knowledge in these methodologies, alongside conducting further research to evaluate the limitations and potential drawbacks of the Vedic approaches in comparison to contemporary methods. Moreover, while Vedic Mathematics has demonstrated remarkable effectiveness in areas such as basic arithmetic and algebra, its application in more complex mathematical functions, including advanced calculus and differential equations, remains notably limited. Researchers are still arguing the actual limit to which these primitive methods can be used to solve the complicated mathematical problems that arise in contemporary scientific studies.

### **1.1 Problems Addressed and Vedic Techniques Applied**

In this work, two major computational problems associated with elliptic curve cryptography are addressed:

#### **Problem 1: Point Addition on Huff and Twisted Huff Elliptic Curves**

Point addition is a fundamental operation in elliptic curve cryptography and requires several multiplications, squarings, and intermediate arithmetic operations. Using conventional algebraic formulas, these operations are computationally expensive, especially for low-power processors.

#### **Techniques Used**

##### **1. Urdhva-Tiryagbhyam (Vertical-Crosswise Multiplication Sutra)**

- Applied for all multiplications

$$X_1X_2, Y_1Y_2, Z_1Z_2, X_1Z_2, X_2Z_1, Y_1Z_2, Y_2Z_1, IJKL, \text{ etc.}$$

- This sutra reduces multiplication time by performing partial products in parallel.

##### **2. Dvandva-Yoga (Duplex / Squaring Sutra)**

- Applied for computing squares such as

$$I^2, L^2, (Y_1Z_2 + Y_2Z_1)^2$$

- This method shortens squaring operations and decreases total clock cycles.

#### **Problem Solved**

By applying these sutras, the overall number of operations required for point addition is significantly reduced



for:

- **Ordinary Huff Elliptic Curve (OHEC)**
- **Twisted Huff Elliptic Curve (THEC)**

This leads to faster elliptic curve computations, lower energy consumption, and improved cryptographic performance.

### **Problem 2: Point Doubling on Huff and Twisted Huff Curves**

Point doubling is another key operation required in key generation, scalar multiplication, and digital signatures. Conventional doubling formulas require expensive multiplications and higher-power computations.

#### **Techniques Used**

##### **1. Dvandva–Yoga Sutra**

- Used to compute all squares:

$$X_1^2, Y_1^2, Z_1^2, H^2, J^2, (dZ_1^2 + X_1^2)^2$$

- Efficiently computes squared values using duplex structures.

##### **2. Urdhva–Tiryagbhyam Sutra**

- Used for multiplications:

$$X_1D, Y_1D, 2Z_1, 2dZ_1, GHIJ$$

- Greatly reduces the number of individual multiplication steps.

#### **Problem Solved**

Applying these Vedic techniques results in faster point-doubling operations on both:

- **Ordinary Huff Elliptic Curves**
- **Twisted Huff Elliptic Curves**

This optimization is crucial for enhancing scalar multiplication, which is the core of ECC operations.



**Table 1: Vedic Techniques and Their Role**

| Problem        | Required Operation | Vedic Technique Used | Purpose                      |
|----------------|--------------------|----------------------|------------------------------|
| Point Addition | Multiplications    | Urdhva-Tiryagbhyam   | Fast parallel multiplication |
| Point Addition | Squarings          | Dvandva-Yoga         | Efficient squaring           |
| Point Doubling | Multiplications    | Urdhva-Tiryagbhyam   | Reduced number of steps      |
| Point Doubling | Squarings          | Dvandva-Yoga         | Faster power computation     |

#### **How These Techniques Help in ECC**

- Reduce the number of multiplication operations
- Reduce squaring time
- Provide parallel computation through vertical-crosswise structure
- Lower processing time on **16-bit** and **32-bit** processors
- Improve efficiency for mobile and IoT cryptographic systems

## **2. MATHEMATICAL FORMULATIONS**

This section discusses the mathematical background of ordinary Huff, twisted Huff curves and addition law for the points on these curves.

**2.1 Ordinary Huff Elliptic Curve (OH\*EC) [4]:** An ordinary Huff elliptic curve  $H_{a,b}^*$ , in two-parameter  $a$  and  $b$  over a finite field  $F$  with  $\text{char}(F) \neq 2$ , is defined as

$$ax(y^2 - 1) = by(x^2 - 1) \quad 2.1$$

where,

$$0 \neq a, b \in F \text{ and } a^2 - b^2 \neq 0.$$

In the set-builder form, the curve (2.1) can be written as



$$H_{a,b}^* = \left\{ (x, y) : ax(y^2 - 1) = by(x^2 - 1), a^2 - b^2 \neq 0 \text{ and } a, b \neq 0 \right\} \quad 2.2$$

## 2.2 Addition law for the points on Ordinary Huff Elliptic Curve [4]

Let  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  be any two points (may be equal or may be different) on the curve  $H_{a,b}^*$ . Then the addition of P and Q denoted by the point  $R(x_3, y_3)$  is defined as

$$x_3 = \frac{(x_1 + x_2)(1 + y_1 y_2)}{(1 + x_1 x_2)(1 - y_1 y_2)} \quad 2.3$$

and

$$y_3 = \frac{(y_1 + y_2)(1 + x_1 x_2)}{(1 + x_1 x_2)(1 - y_1 y_2)} \quad 2.4$$

**Remark- 2.2.1:** Equation (2.3) and (2.4) show that two points  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  on  $H_{a,b}^*$  can be added only when  $|x_1 x_2| \neq 1$  and  $|y_1 y_2| \neq 1$ .

**Remark- 2.2.2:** It can be easily verified that the set  $H_{a,b}^*$  forms an abelian group under the addition operation defined by (2.3) and (2.4), with identity element (0,0), and  $-P = (-x, -y)$  as the additive inverse of P.

## 2.3 Twisted Huff Elliptic Curve (TH\*EC) [12]: A twisted Huff elliptic curve

$H_{a,b}^*$  in three parameters a, b and d over a field F with char  $(F) \neq 2$ , is defined as

$$ax(y^2 - d) = by(x^2 - d) \quad 2.5$$

where,

$$a, b, d \in F \text{ with } a, b \neq 0 \text{ and } (a^2 - b^2) \neq 0.$$

In the set-builder form, the curve (2.5) can be written as

$$H_{a,b,d}^* = \left\{ (x, y) : ax(y^2 - d) = by(x^2 - d) \text{ and } abd(a^2 - b^2) \neq 0 \right\} \quad 2.6$$

## 2.4 Addition of the Points on Twisted Huff Elliptic Curve [12]

Let  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  be any two points (may be equal or may be different) on the curve



$H_{a,b,d}^*$ . Then the addition of P and Q denoted by the point  $R(x_3, y_3)$  is defined as

$$x_3 = \frac{d(x_1 + x_2)(d + y_1 y_2)}{(d + x_1 x_2)(d - y_1 y_2)} \quad 2.7$$

and

$$y_3 = \frac{d(y_1 + y_2)(d + x_1 x_2)}{(d - x_1 x_2)(d + y_1 y_2)} \quad 2.8$$

**Remark- 2.2.3:** Equation (2.3) and (2.4) show that two points  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  on  $H_{a,b,d}^*$  can be added only when  $|x_1 x_2| \neq d$  and  $|y_1 y_2| \neq d$ .

## 2.5 Projective Coordinates Systems for Ordinary Huff Elliptic Curve [4] and Twisted Huff Elliptic Curve [7]

Using the following transformation

$$(x, y) \rightarrow \left( \frac{X}{Z}, \frac{Y}{Z} \right) \quad 2.9$$

the Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve in projective coordinates system, respectively can be rewritten as

$$aX(Y^2 + Z^2) = bY(X^2 - Z^2) \quad 2.10$$

$$aX(Y^2 - dZ^2) = bY(X^2 - dZ^2) \quad 2.11$$

## 2.6 Proposed Schemes

In this section, we will explain the schemes proposed for adding and doubling points on ordinary Huff and twisted Huff elliptic curves.

### Algorithm A1: Addition of two distinct points P and Q on Ordinary Huff Elliptic Curve

Using equations (2.9) to (2.10) and (2.11) the addition  $(X_3, Y_3, Z_3)$  of the points  $(X_1, Y_1, Z_1)$  and  $(X_2, Y_2, Z_2)$  is given by

i.e.,

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

Where:

$$X_3 = (X_1 Z_2 + X_2 Z_1)(Z_1 Z_2 - X_1 X_2)(Y_1 Y_2 + Z_1 Z_2)^2$$



$$Y_3 = (Y_1Z_2 + Y_2Z_1)(Z_1Z_2 - Y_1Y_2)(X_1X_2 + Z_1Z_2)^2$$

$$Z_3 = (Z_1^2Z_2^2 - X_1^2X_2^2)(Z_1^2Z_2^2 - Y_1^2Y_2^2)$$

Now corresponding algorithm using AIVM techniques is explained as follows:

**Input**

$$P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$$

**Output:**

$$R = P + Q = (X_3, Y_3, Z_3)$$

**Steps:**

| Step | Operation                            |
|------|--------------------------------------|
| 1    | $A = X_1 \times X_2$                 |
| 2    | $B = Y_1 \times Y_2$                 |
| 3    | $C = Z_1 \times Z_2$                 |
| 4    | $D = X_1 \times Z_2$                 |
| 5    | $E = X_2 \times Z_1$                 |
| 6    | $F = Y_1 \times Z_2$                 |
| 7    | $G = Y_2 \times Z_1$                 |
| 8    | $H = D + E$                          |
| 9    | $I = B + C$                          |
| 10   | $J = C - A$                          |
| 11   | $K = C - B$                          |
| 12   | $L = A + C$                          |
| 13   | $M = F + G$                          |
| 14   | $X_3 = M \times J \times I^2$        |
| 15   | $Y_3 = M \times K \times L^2$        |
| 16   | $Z_3 = I \times J \times K \times L$ |
| 17   | Return $(X_3 : Y_3 : Z_3)$           |

where both squares  $I^2$  and  $L^2$  can be calculated using Dvandra-yoga technique and all computations  $X_1 \cdot X_2$ ,  $Y_1 \cdot Y_2$ ,  $Z_1 \cdot Z_2$ ,  $X_1 \cdot Z_2$ ,  $X_2 \cdot Z_1$ ,  $Y_1 \cdot Z_2$ ,  $Y_2 \cdot Z_1$ , and  $I \cdot J \cdot K \cdot L$  can be calculated using Urdhva-tiryagbhyam technique of AIVM.

#### **Algorithm-A2: Doubling of a point on Twisted Huff Elliptic Curve**

Using equations (2.9) to (2.10) and (2.11) the doubling of a point  $P = (X_1, Y_1, Z_1)$  on the ordinary Huff elliptic curve  $E_d$  is  $R(X_3, Y_3, Z_3)$ , given by:

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

Where:

$$X_3 = 2X_1Z_1(Z_1^2 - X_1^2)(Z_1^2 + Y_1^2)^2$$

$$Y_3 = 2Y_1Z_1(Z_1^2 - Y_1^2)(X_1^2 + Z_1^2)^2$$



and

$$Z_3 = (Z_1^4 - X_1^4)(Z_1^4 - Y_1^4)$$

Now corresponding algorithm using AIVM techniques can be explained as follows:

**Input**

$$P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$$

**Output:**

$$R = P + Q = (X_3, Y_3, Z_3)$$

| Step | Operation                         |
|------|-----------------------------------|
| 1    | $A = X_1^2$                       |
| 2    | $B = Y_1^2$                       |
| 3    | $C = Z_1^2$                       |
| 4    | $D = 2 \cdot Z_1$                 |
| 5    | $E = X_1 \cdot D$                 |
| 6    | $F = Y_1 \cdot D$                 |
| 7    | $G = C - A$                       |
| 8    | $H = B + C$                       |
| 9    | $I = C - B$                       |
| 10   | $J = A + C$                       |
| 11   | $X_3 = E \cdot G \cdot H^2$       |
| 12   | $Y_3 = F \cdot I \cdot J^2$       |
| 13   | $Z_3 = G \cdot H \cdot I \cdot J$ |
| 14   | Return $(X_3, Y_3, Z_3)$          |

Where all squares  $X_1^2, Y_1^2, Z_1^2, H^2, J^2$  can be computed using Dvandra-yoga technique and All computations  $2 \cdot Z_1, X_1 \cdot D, Y_1 \cdot D, G \cdot H \cdot I \cdot J$  can be calculated using Urdhva-tiryagbhyam technique of AIVM.

**Algorithm B1: Addition of two distinct points  $P$  and  $Q$  on Twisted Huff Elliptic Curve**

Using equations (4.2.13) to (4.2.14) and (4.2.23), the addition  $(X_3, Y_3, Z_3)$  of the points  $(X_1, Y_1, Z_1)$  and  $(X_2, Y_2, Z_2)$  is given by:

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

Where:



$$X_3 = d(X_1Z_2 + X_2Z_1)(dZ_2Z_2 - X_1X_2)(Y_1^2 + dZ_1Z_2)^2$$
$$Y_3 = d(Y_1Z_2 + Y_2Z_1)(dZ_2Z_2 - Y_1Y_2)(X_1X_2 + dZ_1Z_2)^2$$

and

$$Z_3 = (d^2Z_1^2Z_2^2 - X_1^2X_2^2)(d^2Z_1^2Z_2^2 - Y_1^2Y_2^2)$$

Now corresponding algorithm using AIVM techniques can be explained as follows:

| Step | Operation                           |
|------|-------------------------------------|
| 1    | $A = X_1 \cdot X_2$                 |
| 2    | $B = Y_1 \cdot Y_2$                 |
| 3    | $C = d \cdot Z_1 \cdot Z_2$         |
| 4    | $D = X_1 \cdot Z_2$                 |
| 5    | $E = X_2 \cdot Z_1$                 |
| 6    | $F = Y_1 \cdot Z_2$                 |
| 7    | $G = Y_2 \cdot Z_1$                 |
| 8    | $H = D + E$                         |
| 9    | $I = B + C$                         |
| 10   | $J = C - A$                         |
| 11   | $K = C - B$                         |
| 12   | $L = A + C$                         |
| 13   | $M = F + G$                         |
| 14   | $X_3 = d \cdot H \cdot I^2$         |
| 15   | $Y_3 = d \cdot M \cdot K \cdot L^2$ |
| 16   | $Z_3 = I \cdot J \cdot K \cdot L$   |
| 17   | Return $(X_3, Y_3, Z_3)$            |

**Where:**

- All squares  $I^2$  and  $L^2$  can be calculated using Dvandva-yoga technique.
- All computations  $X_1 \cdot X_2$ ,  $Y_1 \cdot Y_2$ ,  $C \cdot Z_1 \cdot Z_2$ ,  $X_1 \cdot Z_2$ ,  $X_2 \cdot Z_1$ ,  $Y_1 \cdot Z_2$ ,  $Y_2 \cdot Z_1$ , and  $I \cdot J \cdot K \cdot L$  are calculated using Urdhva-tiryagbhyam technique of AIVM.



### **Algorithm B2: Doubling of a point Pon Twisted Huff Elliptic Curve**

Using equations (4.2.13) to (4.2.14) and (4.2.23), the doubling of a point  $P = (X_1, Y_1, Z_1)$  on the twisted Huff elliptic curve  $E_d$  is given by  $R(X_3, Y_3, Z_3)$ , as follows:

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

Where:

$$X_3 = 2dX_1Z_1(dZ_1^2 - X_1^2)(dZ_1^2 + X_1^2)^2$$
$$Y_3 = 2dY_1Z_1(dZ_1^2 - Y_1^2)(dZ_1^2 + X_1^2)^2$$

and

$$Z_3 = (d^2Z_1^4 - X_1^4)(d^2Z_1^4 - Y_1^4)$$

Now corresponding schemes using AIVM techniques is evident from the following steps:

| Step | Operation                         |
|------|-----------------------------------|
| 1    | $A = X_1^2$                       |
| 2    | $B = Y_1^2$                       |
| 3    | $C = d \cdot Z_1^2$               |
| 4    | $D = 2 \cdot d \cdot Z_1$         |
| 5    | $E = X_1 \cdot D$                 |
| 6    | $F = Y_1 \cdot D$                 |
| 7    | $G = C - A$                       |
| 8    | $H = B + C$                       |
| 9    | $I = C - B$                       |
| 10   | $J = A + C$                       |
| 11   | $X_3 = E \cdot G \cdot H^2$       |
| 12   | $Y_3 = F \cdot I \cdot J^2$       |
| 13   | $Z_3 = G \cdot H \cdot I \cdot J$ |
| 14   | Return $(X_3, Y_3, Z_3)$          |

**Where:**

- All squares  $X_1^2, Y_1^2, Z_1^2, H^2, J^2$  can be calculated using Dvandra-yoga technique.



- All computations  $2 \cdot d \cdot Z_1, X_1 \cdot D, Y_1 \cdot D, G \cdot H \cdot I \cdot J$  can be calculated using Urdhva-tiryagbhyam technique of AIVM.

## 2.7 Result Analysis and Comparison

A comparative analysis of the number of arithmetic operations such as multiplication, squares, cubes and other higher power used in adding two distinct or similar points in OHEC and Twisted Huff Elliptic Curve using conventional method and techniques of AIVM are tabulated in table-2 and 3.

**Table 2: Comparison of the number of operations required for point addition in Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve**

| Elliptic Curves              | Point Addition (Using the conventional method) |    |    |    |    | Point Addition (Using AIVM techniques) |    |    |    |    |
|------------------------------|------------------------------------------------|----|----|----|----|----------------------------------------|----|----|----|----|
|                              | P1                                             | P2 | P3 | P4 | s  | P1                                     | P2 | P3 | P4 | s  |
| Ordinary Huff Elliptic Curve | 21                                             | 10 | 0  | 0  | 31 | 14                                     | 2  | 0  | 0  | 16 |
| Twisted Huff Elliptic Curve  | 29                                             | 12 | 0  | 0  | 41 | 17                                     | 5  | 0  | 0  | 22 |

where

P<sub>1</sub> - Total number of multiplications,

P<sub>2</sub> - Total number of squares,

P<sub>3</sub> - Total number of cubes,

P<sub>4</sub> - Total number of the fourth power,

S - Sum of P<sub>1</sub>, P<sub>2</sub>, P<sub>3</sub> and P<sub>4</sub>

**Table 3: Comparison of the number of operations required for point doubling on Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve**

| Elliptic Curves              | Point Doubling (Using the Conventional Method) | Point Doubling (Using AIVM Techniques) |
|------------------------------|------------------------------------------------|----------------------------------------|
|                              | $P_1$                                          | $P_2$                                  |
| Ordinary Huff Elliptic Curve | 9                                              | 10                                     |
| Twisted Huff Elliptic Curve  | 14                                             | 12                                     |

Table 2 distinctly demonstrates that the processes required for point doubling on the Ordinary Huff Elliptic Curve and TH\*EC, employing AIVM's techniques, diminish to approximately 48.38% and 46.34%,



correspondingly. Table 3 demonstrates that the processes required for point doubling on the Ordinary Huff Elliptic Curve and the Twisted Huff Elliptic Curve, employing AIVM's techniques, are markedly diminished in number when contrasted with conventional methods, highlighting reductions of approximately 34.78% and 43.33%, respectively. Table 3 presents the time taken for processing and the percentage of time saved during the point addition and point doubling operations on both the Ordinary Huff Elliptic Curve and the Twisted Huff Elliptic Curve while employing a 16-bit processor. In the interim, Table 5 showcases a juxtaposition of the results alongside a 32-bit processor. Furthermore, as demonstrated in Table 4, it is clear that AIVM techniques greatly improve effectiveness in reducing the time required for point addition and point doubling on the Ordinary Huff Elliptic Curve, achieving an impressive decrease of up to 87% when utilizing a 16-bit processor. Concerning the Twisted Huff Elliptic Curve, AIVM techniques remarkably boost performance, reducing the time required for point addition and point doubling by 87.6% and 86.42%, correspondingly. Table 5 demonstrates the time taken for point addition and point doubling on the Ordinary Huff Elliptic Curve, highlighting an impressive decrease of 93.68% and 91.49%, respectively, when utilizing a 32-bit processor. Moreover, the timeframes for handling the Twisted Huff Elliptic Curve can be reduced by an impressive 92.57% and 87%, respectively.

**Table-4: Processing time for arithmetic operations on Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve based on 16-bits processor using conventional and AIVM's techniques**

| Elliptic Curves              | Points Addition          |                           | Point Doubling |                          |
|------------------------------|--------------------------|---------------------------|----------------|--------------------------|
|                              | $T_{ECC}^A$ (In seconds) | $T_{VECC}^A$ (In seconds) | $T_S^A$ (In %) | $T_{ECC}^D$ (In seconds) |
| Ordinary Huff Elliptic Curve | 0.0102450                | 0.0013320                 | 86.9985        | 0.0092544                |
| Twisted Huff Elliptic Curve  | 0.0084565                | 0.0010485                 | 87.6009        | 0.0076318                |

**Where:**

- $T_{ECC}^A$  → Processing time for points addition using the conventional method,
- $T_{VECC}^A$  → Processing time for points addition using AIVM techniques,
- $T_S^A$  → Percentage saving of processing time for points addition using AIVM techniques,
- $T_{ECC}^D$  → Processing time for point doubling using the conventional method,
- $T_{VECC}^D$  → Processing time for point doubling using AIVM techniques,
- $T_S^D$  → Percentage saving of processing time for point doubling using AIVM techniques.

**Table 5: Processing time for arithmetic operations on Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve based on 32-bits processor using conventional and AIVM techniques**

| Elliptic Curves              | Points Addition    |                     |            | Point Doubling     |                     |            |
|------------------------------|--------------------|---------------------|------------|--------------------|---------------------|------------|
|                              | TECCA (In seconds) | TVECCA (In seconds) | TSA (In %) | TECCD (In seconds) | TVECCD (In seconds) | TSD (In %) |
| Ordinary Huff Elliptic Curve | 0.0107600          | 0.00068045          | 93.6760    | 0.010364           | 0.00088221          | 91.4880    |
| Twisted Huff Elliptic Curve  | 0.0097944          | 0.00072795          | 92.5676    | 0.0091592          | 0.00119530          | 86.9499    |

Figure-1 illustrates a comparative examination of the diverse arithmetic operations necessary for point addition on the Ordinary Huff Elliptic Curve and the Twisted Huff Elliptic Curve. Meanwhile, figure-2 explores the comparison of various arithmetic operations vital for point doubling on both the Ordinary and Twisted Huff Elliptic Curves.

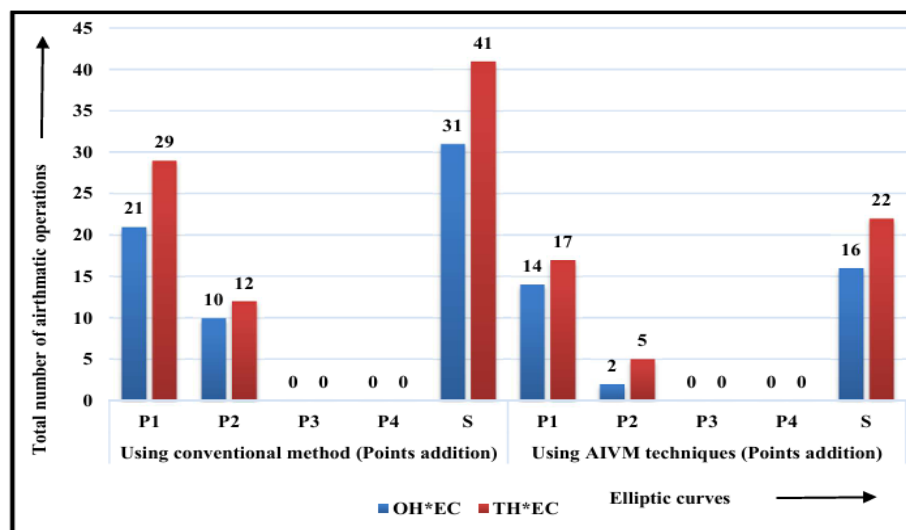


**Figure 1: Comparison of different type of arithmetic operations required for points addition on Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve**

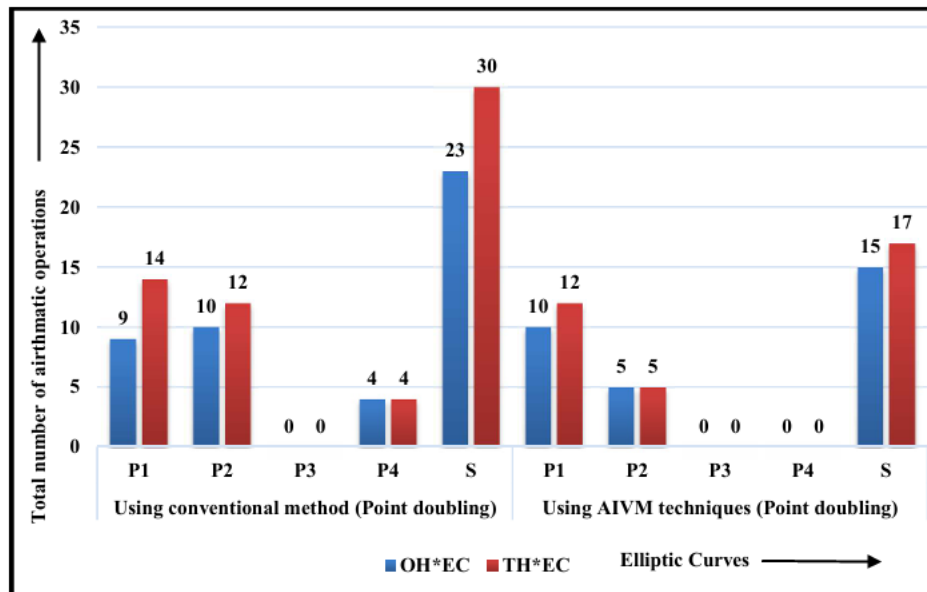


**Figure 2: Comparison of different type of arithmetic operations required for point doubling on Ordinary Huff Elliptic Curve and Twisted Huff Elliptic Curve**

The research outcomes unveil intriguing revelations regarding the utilization of ancient mathematical principles in contemporary encryption frameworks, particularly within the realm of elliptic curve encryption. A notable insight is that the incorporation of Vedic methodologies markedly diminishes the operations needed for point addition and point doubling on both Huff and twisted Huff elliptic curves. The application of ancient Vedic principles, including Urdhva-Tiryagbhyam and Dvandra-Yoga, showcases a significant influence on the effectiveness of computation. The techniques, initially crafted for cognitive computations, demonstrate an ability to simplify intricate processes, reducing both the numerical intricacy and processing demands. This enhancement holds considerable importance when taking into account the processing requirements of contemporary cryptography, where rapid performance and robust security are essential. Through the minimization of multiplication operations, as well as squares, cubes, and advanced powers, the research revealed that ancient mathematical techniques might significantly refine encryption methods, thereby boosting the efficiency of the entire system. Moreover, the results indicate that incorporating Vedic Mathematics within cryptographic frameworks significantly accelerates processing durations. As an illustration, employing a 16-bit processor resulted in a remarkable reduction in the time needed for point addition and point doubling on Huff elliptic curves, achieving a decrease of as much as 87%. In contrast, utilizing a 32-bit processor yielded an even greater improvement, with time savings reaching up to 93% for specific operations. The decrease in processing duration presents a significant benefit, especially for nimble cryptographic frameworks, like those employed in portable gadgets and wireless connectivity, where computational capabilities are constrained. The remarkable efficiency offered by Vedic approaches indicates that these strategies are exceptionally well-suited for enhancing the functionality of systems where rapidity and minimal resource utilization are crucial. The juxtaposition of traditional techniques and AIVM-centric algorithms underscores the potency of Vedic Mathematics. The research reveals that, even within the intricate domain of elliptic curve cryptography, these time-honored approaches can surpass conventional computational strategies, leading to significant savings in both time and resources. Traditional algorithms demand a significant amount of computational effort, whereas AIVM methods streamline the procedure, enabling swifter and more effective encryption and decryption tasks. This benefit becomes especially clear when reflecting on the contemporary cryptographic frameworks' necessity to manage extensive volumes of



information both securely and rapidly.

Nonetheless, the research underscores various obstacles and constraints associated with the integration of Vedic Mathematics into modern computational frameworks. A significant hurdle recognized is the insufficient comprehension and structured learning regarding Vedic methodologies, potentially hindering their extensive acceptance. In light of this, the study encourages additional investigation into the fusion of ancient mathematical principles with contemporary technology, highlighting the necessity for organized educational structures and scholarly inquiry to fully grasp the system's vast capabilities. Furthermore, although the research emphasizes ECC, the potential for these methodologies to extend to various cryptographic frameworks and cutting-edge domains, including quantum computing and artificial intelligence, is still a matter of exploration. Prospective investigations may delve into these pathways, illuminating the potential for Vedic Mathematics to be more extensively tailored and woven into the fabric of advancing technologies. This research showcases Vedic Mathematics as an effective and encouraging resource for enhancing contemporary cryptographic frameworks. The results indicate that, with additional exploration and advancement, these time-honored techniques might offer a groundbreaking answer to the escalating needs for swifter, more robust cryptographic algorithms, particularly within the framework of resource-limited settings such as mobile gadgets and wireless communication networks.

### **3. CONCLUSION**

The principles of Vedic Mathematics present an intriguing method for enhancing the speed and effectiveness of calculations within contemporary cryptographic frameworks. The amalgamation of ancient Vedic methodologies with elliptic curve cryptography, especially concerning the Huff and twisted Huff curves, reveals significant decreases in the operational count and processing duration necessary for point addition and point doubling. An analysis of traditional techniques alongside AIVM-driven algorithms reveals that Vedic Mathematics has the potential to greatly boost the efficiency of these cryptographic systems, particularly by alleviating computational demands and accelerating processing times. Utilizing time-honored concepts of cognitive computation and pattern identification, Vedic Mathematics enhances the efficiency of computational assets, rendering it an essential instrument for contemporary fields such as artificial intelligence, machine learning, and cryptographic systems. This study illustrates that utilizing Vedic Mathematics results in optimal hardware resource utilization for both 16-bit and 32-bit processors, achieving remarkable time reductions of up to 93% for specific operations. Furthermore, the findings suggest that these methods are especially advantageous for nimble cryptographic frameworks, like those implemented in smartphones and wireless connectivity. With the escalating requirements of computation, the amalgamation of time-honored mathematical techniques and state-of-the-art technology unveils fresh pathways for enhancing algorithm performance, presenting an encouraging trajectory for forthcoming investigations in computational mathematics and cryptography.

### **REFERENCES**

- [1]. Edwards H., A normal form for elliptic curves, In Bulletin of the American Mathematical Society, 44 (3), 393-422, 2007.
- [2]. Joye M. and Quisquater J., Hessian elliptic curves and side-channel attacks, Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science, Springer, 2162, 402-410, 2001.
- [3]. Liardet P. and Smart N., Preventing SPA / DPA in ECC systems using the Jacobi form, Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science, Springer-Verlag, 2162, 391-401, 2001.
- [4]. Huff G. B., Diophantine problems in geometry and elliptic ternary forms, Duke Math. J, 15, 443-453, 1948.



- [5]. Joye M., Tibouchi M. and Vergnaud D., Huff's model for elliptic curves, ANTSIX. LNCS, Springer, Heidelberg, 6197, 234-250, 2010.
- [6]. Devigne J. and Joye M., Binary Huff Curves, Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science, Springer, 6558, 340-355, 2011.
- [7]. Ciss A. A. and Sow D., On a new generalization of Huff curves, Journal IACR Cryptology ePrint Archive, 1-17, 2011. <https://eprint.iacr.org/2011/580.pdf>.
- [8]. Gu H., Gu D., Xie W. and Cheung R. C. C., Efficient Pairing Computation on Huff Curves, Taylor and Francis, Cryptologia, 39 (3), 270–275, 2015.
- [9]. Jafri A. R. and Islam M. N., Towards an Optimized Architecture for Unified Binary Huff Curves, Journal of Circuits, Systems and Computers, 26 (11), 1-14, 2017.
- [10]. Sadek M., El-Sissi N., Zargar A. S. and Zamani N., Evaluation of Gaussian hypergeometric series using Huff's models of elliptic curves, The Ramanujan Journal, 48 (2), 357-368, 2018.
- [11]. Drylo R. Kijko T. and Wronski M., Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogenybased cryptography, Journal IACR Cryptol ePrint Arch, 1-27, 2020. <https://eprint.iacr.org/2020/526.pdf>.
- [12]. Joye M., Tibouchi M. and Vergnaud D., Huff's model for elliptic curves, ANTSIX. LNCS, Springer, Heidelberg, 6197, 234-250, 2010.

