AN EFFICIENT ALGORITHMIC APPROACH TO HUFF ELLIPTIC CURVES USING VEDIC MATHEMATICS

[1]Dr. Ankur Nehra, [2]Abhishek Kumar and [3]Khushboo Saini
Assistant Professor, Department of Mathematics, Dhanauri P.G. College (Govt. Aided), Dhanauri, Haridwar, Uttarakhand, India
[2]Research Scholar, Department of Mathematics, Coer University, Roorkee, Haridwar, Uttarakhand, India, 247667
[3]Research Scholar, Department of Mathematics, Coer University, Roorkee, Haridwar, Uttarakhand, India, 247667
[1]Email ID: drankurnehra@gmail.com [2]Email ID: abhishek07032018@gmail.com
[3]Email ID: abs8171800203@gmail.com

Abstract: This paper presents efficient algorithms based on Ancient Indian Vedic Mathematics (AIVM) to optimize the computational performance of point addition and point doubling operations on Huff Elliptic Curves (HEC), Generalized Huff Elliptic Curves (GHEC), and New Generalized Huff Elliptic Curves (NGHEC). To accelerate arithmetic operations, the Dvandva-Yoga sutra is employed for fast squaring, while the Urdhva-Tiryagbhyam sutra is used for high-speed multiplication. The proposed AIVM-based algorithms significantly reduce the time complexity involved in elliptic curve computations. Experimental evaluation, carried out through MATLAB implementations for 8-bit and 16-bit multiplication and squaring operations, demonstrates the superior performance of the Vedic-mathematics-based approach compared to conventional methods. The results show a notable improvement in processing speed, reduced computation delay, and lower power consumption. The impact of the AIVM techniques on Huff-curve operations has been thoroughly analyzed, and the findings are presented through comparative tables and graphical illustrations. Overall, the proposed methods offer an effective and high-performance solution for enhancing arithmetic operations in Huff-based elliptic curve cryptography.

[Nehra, A., Kumar, A. and Saini, K. **AN EFFICIENT ALGORITHMIC APPROACH TO HUFF ELLIPTIC CURVES USING VEDIC MATHEMATICS.** *The International Journal of Interpretation, Observation and Analysis*, 2025; Volume 4, Issue 1:118-123 (October-December). ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 6.205

Key Words: Urdhva-tiryagbhyam technique, Dvandva-yoga technique, HEC, GHEC, NGHEC

Mathematics Subject Classification: 94A60, 14G50

1. INTRODUCTION

The concept of elliptic curves over finite fields plays a fundamental role in modern elliptic curve cryptography (ECC). The arithmetic of elliptic curves has attracted extensive interest from cryptographic researchers, leading to the development of numerous methods aimed at accelerating elliptic curve operations. In recent years, various alternative curve models such as Huff curves, Edwards curves, and Hessian curves have gained significant attention due to their simplicity, elegant structure, and faster point addition and point doubling procedures. Elliptic curves have been studied for several decades, and many well-known curve forms, such as the Weierstrass, Huff, Hessian, and Jacobi curves, are widely recognized in cryptographic applications. Among these, the Huff elliptic curve, introduced by Huff in 1948 over the rational field, and its plane generalization, the Generalized Huff Curve, have emerged as promising models due to their efficient arithmetic properties. In 2010, Joye et al. extended the applicability of Huff curves to fields of characteristic not equal to two and presented improved formulas for point addition and point doubling. The generalized form of the Huff curve was further developed by Feng and Wu in 2010, and subsequently, the New Generalized Huff Curve was introduced by Ciss and Sow in 2011. Devigne and Joye later proposed unified point addition formulas for Huff curves over fields of characteristic 2. In this work, we focus on Huff Elliptic Curves (HEC), Generalized Huff Elliptic Curves (GHEC), and their variants. These curve models support efficient computation and exhibit advantageous properties such as resistance to side-channel attacks. Side-channel attacks exploit physical leakages such as power consumption, timing behavior, electromagnetic emissions, or induced faults to recover secret information during ECC-based scalar multiplication. Scalar multiplication, typically implemented via the double-and-add algorithm, involves performing a point doubling for every bit of the scalar and a point addition whenever the corresponding bit is 1. If point addition and point doubling operations are distinguishable through side-channel analysis, an adversary may be able to recover the secret key. To counter such vulnerabilities, unified formulas that compute point addition and doubling using identical sequences of field operations

have been proposed, making the two processes indistinguishable. This paper introduces efficient algorithms based on Ancient Indian Vedic Mathematics (AIVM) to reduce the computational time required for point addition and point doubling on HEC, GHEC, and NGHEC. For fast squaring operations, the Yavadunam and Dvandva-Yoga techniques are employed, while the Ekadhikina-Purvena and Urdhva-Tiryagbhyam sutras are used to accelerate multiplication.

The paper is organized as follows:

- **Section II** presents the necessary preliminaries on Vedic Mathematics techniques relevant to ECC.
- **Section III** provides an overview of Huff elliptic curves and describes ECC operation algorithms for these curves and their variants.
- **Section IV** discusses the generalized Huff elliptic curves and their associated ECC algorithms.
- **Section V** introduces the new generalized Huff elliptic curves along with their operation algorithms.
- **Section VI** presents a detailed comparison and performance analysis of arithmetic operations on HEC and GHEC models.
- **Section VII** concludes the work with key findings.

2. MATHEMATICAL BACKGROUND OF HUFF ELLIPTIC CURVES

In this section, we will discuss the mathematical background of ordinary Huff, twisted Huff curves, and the addition law for the points on these curves.

2.1. Ordinary Huff Elliptic Curve $\left(\mathbf{OH^*EC}\right)$ [9]: An ordinary Huff elliptic curve $H^*_{a,b}$ in two-parameter a and b over a finite field F with char$(F)\neq 2$, is defined as

$$a\,x\left(y^2-1\right)=b\,y\left(x^2-1\right) \tag{1}$$

where $0\neq a,b\in F$ and $a^2-b^2\neq 0$.

2.1.1. Addition law for the points on $\mathbf{OH^*EC}$ [9]

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

$$x_3=\frac{\left(x_1+x_2\right)\left(1+y_1y_2\right)}{\left(1+x_1x_2\right)\left(1-y_1y_2\right)} \tag{2}$$

and

$$y_3=\frac{\left(y_1+y_2\right)\left(1+x_1x_2\right)}{\left(1-x_1x_2\right)\left(1+y_1y_2\right)} \tag{3}$$

2.2. Twisted Huff Elliptic Curve $\left(\mathbf{TH^*EC}\right)$ [9]: A twisted Huff elliptic curve $H^*_{a,b,d}$ in three parameters a, b and d over a field F with char $(F)\neq 2$, is defined as

$$a\,x\left(y^2-d\right)=b\,y\left(x^2-d\right) \tag{4}$$

where $a,b,d\in F$ with $a,b\neq 0$ and $a\,b\,d\left(a^2-b^2\right)\neq 0$.

2.2.1. Addition of the Points on $\mathbf{TH^*EC}$ [9]

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

$$x_3=\frac{d\left(x_1+x_2\right)\left(d+y_1y_2\right)}{\left(d+x_1x_2\right)\left(d-y_1y_2\right)} \tag{5}$$

and

$$y_3=\frac{d\left(y_1+y_2\right)\left(d+x_1x_2\right)}{\left(d-x_1x_2\right)\left(d+y_1y_2\right)} \tag{6}$$

$$(x,\ y) \rightarrow \left(\frac{X}{Z}, \frac{Y}{Z}\right) \qquad (7)$$

Using the above transformation, the OH^*EC and TH^*EC in the projective coordinates system, respectively, can be rewritten as

$$a\,X\left(Y^2+Z^2\right) = bY\left(X^2-Z^2\right) \qquad (8)$$

$$a\,X\left(Y^2-d\,Z^2\right) = bY\left(X^2-d\,Z^2\right) \qquad (9)$$

3. 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 OH^*EC

Using equations (3) to (4) and (9), 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 $X_3=(X_1Z_2+X_2Z_1)(Z_1Z_2-X_1X_2)(Y_1Y_2+Z_1Z_2)^2$

$Y_3=(Y_1Z_2+Y_2Z_1)(Z_1Z_2-Y_1Y_2)(X_1X_2+Z_1Z_2)^2$, and $Z_3=\left(Z_1^2Z_2^2-X_1^2X_2^2\right)\left(Z_1^2Z_2^2-Y_1^2Y_2^2\right)$.

Now corresponding algorithm using AIVM techniques is explained as follows:

$Input: P\equiv(X_1,Y_1,Z_1)$ and $Q\equiv(X_2,Y_2,Z_2)$, $Output: R=P+Q\equiv(X_3,Y_3,Z_3)$, $A=X_1\cdot X_2$, $B=Y_1\cdot Y_2$, $C=Z_1\cdot Z_2$, $D=X_1\cdot Z_2$, $E=X_2\cdot Z_1$, $F=Y_1\cdot Z_2$, $G=Y_2\cdot Z_1$, $H=D+E$, $I=B+C$, $J=C-A$, $K=C-B$, $L=A+C$, $M=F+G$, $X_3=M\cdot J\cdot I^2$, $Y_3=M\cdot K\cdot L^2$, $Z_3=I\cdot J\cdot K\cdot L$, $Return(X_3:Y_3:Z_3)$.

Where both squares I^2 and L^2 can be calculated using Dvandva-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 P on OH^*EC

Using equations (2.3) to (2.4) and (2.9), 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 $X_3=2X_1Z_1\left(Z_1^2-X_1^2\right)\left(Z_1^2+Y_1^2\right)^2$

$Y_3=2Y_1Z_1\left(Z_1^2-Y_1^2\right)\left(X_1^2+Z_1^2\right)^2$ and $Z_3=\left(Z_1^4-X_1^4\right)\left(Z_1^4-Y_1^4\right)$

Now corresponding algorithm using AIVM techniques is explained as follows:

$Input: P\equiv(X_1,Y_1,Z_1)$ and $Q\equiv(X_2,Y_2,Z_2)$, $Output: R=P+P=2P\equiv(X_3,Y_3,Z_3)$, $A=X_1^{\,2}$, $B=Y_1^2$, $C=Z_1^{\,2}$, $D=2\cdot Z_1$, $E=X_1\cdot D$, $F=Y_1\cdot D$, $G=C-A$, $H=B+C$, $I=C-B$, $J=A+C$, $X_3=E\cdot G\cdot H^2$, $Y_3=F\cdot I\cdot J^2$, $Z_3=G\cdot H\cdot I\cdot J$, $Return(X_3:Y_3:Z_3)$

where all squares $X_1^{\,2}$, Y_1^2, $Z_1^{\,2}$, H^2, J^2 can be computed using Dvandva-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 TH^*EC

Using equations (2.7) to (2.8) and (2.9), 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 $X_3=d\left(X_1Z_2+X_2Z_1\right)\left(d\,Z_1Z_2-X_1X_2\right)\left(Y_1Y_2+d\,Z_1Z_2\right)^2$

$Y_3=d\left(Y_1Z_2+Y_2Z_1\right)\left(d\,Z_1Z_2-Y_1Y_2\right)\left(X_1X_2+d\,Z_1Z_2\right)^2$ and $Z_3=\left(d^2Z_1^2Z_2^2-X_1^2X_2^2\right)\left(d^2Z_1^2Z_2^2-Y_1^2Y_2^2\right)$.

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

$Input: P\equiv\left(X_1,Y_1,Z_1\right)$, $Q\equiv\left(X_2,Y_2,Z_2\right)$ and $'d'$, $Output: R=P+Q\equiv\left(X_3,Y_3,Z_3\right)$, $A=X_1\cdot X_2$, $B=Y_1\cdot Y_2$, $C=d\cdot Z_1\cdot Z_2$, $D=X_1\cdot Z_2$, $E=X_2\cdot Z_1$, $F=Y_1\cdot Z_2$, $G=Y_2\cdot Z_1$, $H=D+E$, $I=B+C$, $J=C-A$, $K=C-B$, $L=A+C$, $M=F+G$, $X_3=d\cdot H\cdot J\cdot I^2$, $Y_3=d\cdot M\cdot K\cdot L^2$, $Z_3=I\cdot J\cdot K\cdot L$, $Return\left(X_3:Y_3:Z_3\right)$

Where all squares I^2 and L^2 can be calculated using Dvandva-yoga technique, and 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 P on TH^*EC

Using equations (2.7) to (2.8) and (2.9), the doubling of a point $P=(X_1,Y_1,Z_1)$ on the twisted 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 $X_3=2d\,X_1Z_1\left(d\,Z_1^2-X_1^2\right)\left(d\,Z_1^2+Y_1^2\right)^2$,

$Y_3=2d\,Y_1Z_1\left(d\,Z_1^2-Y_1^2\right)\left(d\,Z_1^2+X_1^2\right)^2$ and $Z_3=\left(d^2Z_1^4-X_1^4\right)\left(d^2Z_1^4-Y_1^4\right)$

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

$Input: P\equiv\left(X_1,Y_1,Z_1\right)$, $Q\equiv\left(X_2,Y_2,Z_2\right)$ and $'d'$, $Output: R=P+P=2P\equiv\left(X_3,Y_3,Z_3\right)$, $A=X_1^2$, $B=Y_1^2$, $C=d\cdot Z_1^2$, $D=2\cdot d\cdot Z_1$, $E=X_1\cdot D$, $F=Y_1\cdot D$, $G=C-A$, $H=B+C$, $I=C-B$, $J=A+C$, $X_3=E\cdot G\cdot H^2$, $Y_3=F\cdot I\cdot J^2$, $Z_3=G\cdot H\cdot I\cdot J$, $Return\left(X_3:Y_3:Z_3\right)$

Where all squares X_1^2, Y_1^2, Z_1^2, H^2, J^2 can be calculated using Dvandva-yoga technique and 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.

4. RESULT ANALYSIS AND COMPARISON

A comparative analysis of the number of arithmetic operations, such as multiplication, squares, cubes, and other higher powers used in adding two distinct or similar points in OHEC and THEC using the conventional method and techniques of AIVM is tabulated in Tables 4.1 and 4.2.

Table 4.1. Comparison of the number of operations required for point addition in OH^*EC and TH^*EC

Elliptic Curves	Point Addition (Using the conventional method)					Point Addition (Using AIVM techniques)				
	P_1	P_2	P_3	P_4	S	P_1	P_2	P_3	P_4	S
OH^*EC	21	10	0	0	31	14	2	0	0	16
TH^*EC	29	12	0	0	41	17	5	0	0	22

Table 4.2. Comparison of the number of operations required for point doubling on OH^*EC and TH^*EC

Elliptic Curves	Point doubling (Using the conventional method)					Point doubling (Using AIVM techniques)				
	P_1	P_2	P_3	P_4	S	P_1	P_2	P_3	P_4	S
OH^*EC	9	10	0	4	23	10	5	0	0	15
TH^*EC	14	12	0	4	30	12	5	0	0	17

It is obvious from Table 4.1 that the number of operations required for point doubling on OH^*EC and TH^*EC using AIVM's techniques, respectively, reduces to 48.38% and 46.34% respectively. Table 4.2 shows that the number of operations required for point doubling on OH^*EC and TH^*EC using AIVM's techniques is less than that of conventional methods, and is approximately reduced to 34.78% and 43.33% respectively. Table 4.3 describes the processing time and percentage saving of time occurring in point addition and point doubling on OH^*EC and TH^*EC using 16-bit processor, while Table 4.4 compares the said results using a 32-bit processor. Furthermore, from Table 4.3, it is obvious that AIVM techniques help to reduce processing time for points addition and point doubling on OH^*EC up to 87 % approximately using a 16-bit processor. In the case of TH^*EC AIVM, techniques help to reduce processing time for point addition and point doubling up to 87.6% and 86.42% respectively. Table 4.4 shows that the processing time for point addition and point doubling on OH^*EC can be increased up to 93.68% and 91.49%, using 32-bit processor. Moreover, these processing times on TH^*EC can be increased up to 92.57% and 87% approximately.

Table 4.3. Processing time for arithmetic operations on OH^*EC and TH^*EC based on 16-bit processor using conventional and AIVM's techniques

Elliptic 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 %)
$OH'EC$	0.0102	0.0013	86.99	0.0092	0.0011	87.21
$TH'EC$	0.0084	0.00104	87.60	0.0076	0.0010	86.41

Table 4.4. Processing time for arithmetic operations on OH^*EC and TH^*EC based on 32-bit processor using conventional and AIVM techniques

Elliptic 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 %)
OHEC	0.0107	0.0006	93.67	0.0103	0.0008	91.48
THEC	0.0097	0.0007	92.56	0.0091	0.0011	86.94

5. CONCLUSION

This study presents efficient algorithms for point addition and point doubling on Huff Elliptic Curves (HEC), Generalized Huff Elliptic Curves (GHEC), and New Generalized Huff Elliptic Curves (NGHEC) by integrating Ancient Indian Vedic Mathematics (AIVM) techniques. The use of the *Dvandva-Yoga* Sutra for squaring operations and the *Urdhva-Tiryagbhyam* Sutra for multiplication significantly reduces computational delay and enhances overall performance. The MATLAB-based implementation for 8-bit and 16-bit operations demonstrates that AIVM-based algorithms provide faster processing, lower power consumption, and improved speed compared to classical arithmetic methods. The reduced total computation delay confirms the effectiveness of Vedic techniques in optimizing cryptographic operations over Huff curves. The performance improvements observed in tables and graphical analysis further validate that AIVM techniques offer a promising and efficient alternative for hardware and software implementations of elliptic curve cryptography.

REFERENCES

1. 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

2. Devigne J. and Joye M., Binary Huff Curves. Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science, Springer, **6558**, 340-355, 2011.
3. 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 isogeny-based cryptography, Journal IACR Cryptol ePrint Arch, 1-27, 2020. https://eprint.iacr.org/2020/526.pdf
4. Edwards H., 'A normal form for elliptic curves'. In: Bulletin of the American Mathematical Society, 44(3), 393-422, 2007.
5. Gu, H., Gu, D., Xie, W., & Cheung, R. C. C., Efficient Pairing Computation on Huff Curves, Taylor and Francis, Cryptologia, 39(3), 270–275, 2015.
6. Huff G. B, Diophantine problems in geometry and elliptic ternary forms. Duke Math. J., 15, pp. 443-453, 1948.
7. 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.
8. Joye M., and Quisquater J., Hessian elliptic curves and side-channel attacks. Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science, 2162, Springer, 402-410, 2001.
9. Joye M., Tibouchi, M., Vergnaud D., Huff's model for elliptic curves. In: Hanrot, G., Morain, F., Thomé, E. (eds.) ANTS-IX. LNCS, Springer, Heidelberg, **6197**, 234-250, 2010.
10. 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.
11. Orhon N. G., and Hisil H., Speeding up Huff form of elliptic curves, Designs, Codes and Cryptography, Springer Nature, **86**, 2807-2823, 1-17, 2018.
12. Sadek M., El-Sissi, N., Zargar, A. S., & Zamani N., Evaluation of Gaussian hypergeometric series using Huff's models of elliptic curves, The Ramanujan Journal, **48** (2), 357-368, 2018.
13. Wu H. and Feng R., Elliptic Curves in Huff's Model, Wuhan University Journal of Natural Sciences, **17**(6), 473-480, 2012.