ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 7191–7199
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.68

PERFORMANCE ANALYSIS OF HUFF AND TWISTED HUFF ELLIPTIC CURVES USING URDHVA TIRYAGBHYAM AND DVANDVA YOGA TECHNIQUES OF ANCIENT MATHEMATICS

MANOJ KUMAR AND ANKUR KUMAR[1]

ABSTRACT. This paper is on some efficient algorithms implementation of points addition and points doubling for the Huff elliptic curves using techniques of ancient mathematics. In particular, we improve timings in the cryptographic operations for the Huff elliptic curves. We use some techniques of ancient mathematics namely Urdhva-triyagbhaym for multiplication, Dvandva-yoga for squaring of any digits. We introduce cryptographic formulae (Point Addition and Point Doubling) for Huff elliptic curves. We discuss that the techniques of the ancient mathematics-based scheme show better performance in speed, processing time and power consumption of multipliers compared to the conventional method. The coding and synthesis are done in MATLAB for the algorithm of multiplications and squaring using 16-bits and 32-bits. The effect of some Ancient Mathematical techniques over elliptic curves was investigated and the obtained results are explained in the form of tables and graphs. We discuss the significance of these optimizations for elliptic curve cryptography.

1. INTRODUCTION

Elliptic curves, as discussed in paper two, have been extensively studied in algebraic geometry and number theory since the middle of the nineteenth century.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A60, 14G50.

Key words and phrases. Urdhva-tiryagbhyam technique,Dvandva-yoga technique, Huff elliptic curve, Twisted Huff elliptic curve, Points addition, Point doubling.

From thereafter, different models like Edwards curve [4], Hessian curves [8], Jacobi curves [10] etc have been proposed by various researchers to improve the performance of the cryptosystems based on these elliptic curves. To study a diophantine problem, such type of model for these elliptic curves was introduced by Huff [6] in 1948. More recently, elliptic curves have been rapidly used to devise efficient algorithms for factoring large integers and in the construction of lightweight cryptosystems such as smartphone and wireless communication systems. In 2010, a development of Huff curve was proposed by Joye et al. [9] in a paper entitled " Huff's model for elliptic curves". In this paper, they presented fast explicit formulae for adding and doubling points on Huff curves. In 2011, Devigne and Joye [2] described the addition law for binary Huff curves. In the mean-time, Ciss and Sow [1] proposed a generalization of Huff curves and in the subsequent year, they presented Tate pairing computation on these generalized Huff curves. Gu et al. [5] also suggested efficient pairing computation on Huff curves in 2015. In 2017, Jafri and Islam [7] suggested an optimized architecture for unified binary Huff curves. Later on, Sadek et al. [11] used Huff curves for evaluating the Gaussian hypergeometric series. Very recently, Drylo et al. [3] proposed efficient Montgomery-like formulae on generalized Huff curve for their applications to isogeny based cryptography. In the present paper, we have used some techniques of AIVM for these Huff curves to speed up the performance of the cryptosystems using these curves. The rest of the paper is organized as follows: section 2 consists of the mathematical background of Huff curves, section 3 describes the proposed improved algorithms for points addition and point doubling on Huff and twisted Huff curves using the AIVM's techniques namely Urdhva-tiraygbhaym and Dvandva-yoga, section 4 explains the analysis and comparison of the results of proposed schemes, and the last section 5 concludes the present research work.

2. Mathematical Background of Huff Elliptic Curves

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

2.1. **Ordinary Huff Elliptic Curve (OHEC) [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

$$a\,x\left(y^2-1\right)=b\,y\left(x^2-1\right)\,, \tag{2.1}$$

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

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

$$H^*_{a,b}=\left\{\,(x,y)\ :\ a\,x\left(y^2-1\right)=b\,y\left(x^2-1\right)\,,\ a^2-b^2\neq 0\ and\, a,b\neq 0\right\}\,.$$

2.1.1. *Addition law for the points on OHEC.* 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

$$x_3=\frac{(x_1+x_2)\,(1+y_1y_2)}{(1+x_1x_2)\,(1-y_1y_2)}\,, \tag{2.2}$$

and

$$y_3=\frac{(y_1+y_2)\,(1+x_1x_2)}{(1-x_1x_2)\,(1+y_1y_2)}\,. \tag{2.3}$$

2.2. **Twisred Huff Elliptic Curve (THEC) [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

$$a\,x\left(y^2-d\right)=b\,y\left(x^2-d\right)\,, \tag{2.4}$$

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

In the set-builder form, the curve (2.4) can be written as

$$H^*_{a,b,d}=\left\{\,(x,y)\ :\ a\,x\left(y^2-d\right)=b\,y\left(x^2-d\right)\ and\ a\,b\,d\left(a^2-b^2\right)\neq 0\,\right\}\,.$$

2.2.1. *Addition law for the points on THEC.* 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

$$x_3=\frac{d\ (x_1+x_2)\,(d+y_1y_2)}{(d+x_1x_2)\,(d-y_1y_2)}\,, \tag{2.5}$$

and

$$y_3=\frac{d\ (y_1+y_2)\,(d+x_1x_2)}{(d-x_1x_2)\,(d+y_1y_2)}\,, \tag{2.6}$$

$$(x,\ y)\ \rightarrow\ \left(\frac{X}{Z},\ \frac{Y}{Z}\right)\,. \tag{2.7}$$

Using the above transformation the **OHEC**and **THEC**in projective coordinates system, respectively can be rewritten as

$$\begin{aligned} a\,X\left(Y^2+Z^2\right) &= b\,Y\left(X^2-Z^2\right), \\ a\,X\left(Y^2-d\,Z^2\right) &= b\,Y\left(X^2-d\,Z^2\right). \end{aligned}$$

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 OHEC
Using equations (2.2) to (2.3) and (2.7) 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 $Z_3 = (Z_1^2Z_2^2 - X_1^2X_2^2)\,(Z_1^2Z_2^2 - Y_1^2Y_2^2)$.
Now corresponding algorithm using AIVM techniques is explained as follows:
$Input:\ P \equiv (X_1, Y_1, Z_1)$ **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 OHEC
Using equations (2.2) to(2.3) and (2.7) 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 $X_3 = 2X_1Z_1\,(Z_1^2 - X_1^2)\,(Z_1^2 + Y_1^2)^2Y_3 = 2Y_1Z_1\,(Z_1^2 - Y_1^2)\,(X_1^2 + Z_1^2)^2$ and $Z_3 = (Z_1^4 - X_1^4)\,(Z_1^4 - Y_1^4)$
Now corresponding algorithm using AIVM techniques 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 THEC
Using equations (2.5) to(2.6) and (2.7) 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 $X_3 = d\,(X_1Z_2 + X_2Z_1)\,(d\,Z_1Z_2 - X_1X_2)\,(Y_1Y_2 + d\,Z_1Z_2)^2Y_3 = d\,(Y_1Z_2 + Y_2Z_1)\,(d\,Z_1Z_2 - Y_1Y_2)\,(X_1X_2 + d\,Z_1Z_2)^2$
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:
$Input:\ P \equiv (X_1, Y_1, Z_1)$, $Q \equiv (X_2, Y_2, Z_2)$ and $'d'$,
$Output: R = P + Q \equiv (X_3, Y_3, Z_3)$, $A = X_1 \cdot X_2$, $B = Y_1 \cdot Y_2$, $C = d \cdot Z_1 \cdot Z_2$, $D = X_1 \cdot Z_2$,$E = X_2 \cdot Z_1$,$F = Y_1 \cdot Z_2$,$G = Y_2 \cdot Z_1$,$H = D + E$, $I = B + C$,$J = C - A$,$K = C - B$,$L = A + C$,$M = F + G$,$X_3 = d \cdot H \cdot J \cdot I^2$, $Y_3 = d \cdot M \cdot K \cdot L^2$,$Z_3 = I \cdot J \cdot K \cdot L$,
$Return\ (X_3 : Y_3 : Z_3)$
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 THEC
Using equations (2.5) to(2.6) and (2.7) 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 $X_3 = 2\,d\,X_1Z_1\,(d\,Z_1^2 - X_1^2)\,(d\,Z_1^2 + Y_1^2)^2$, $Y_3 = 2\,d\,Y_1Z_1\,(d\,Z_1^2 - Y_1^2)\,(d\,Z_1^2 + X_1^2)^2$
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:
$Input:\ P \equiv (X_1, Y_1, Z_1)$, $Q \equiv (X_2, Y_2, Z_2)$ and $'d'$,
$Output:\ R = P + P = 2P \equiv (X_3, Y_3, Z_3)$, $A = {X_1}^2$,$B = {Y_1}^2$,$C = d \cdot {Z_1}^2$,$D = 2 \cdot d \cdot Z_1$,$E = X_1 \cdot D$,$F = Y_1 \cdot D$,$G = C - A$,$H = B + C$,$I = C - B$,$J = A + C$,$X_3 = E \cdot G \cdot H^2$,$Y_3 = F \cdot I \cdot J^2$,$Z_3 = G \cdot H \cdot I \cdot J$,
$Return\ (X_3 : Y_3 : Z_3)$
where all squares ${X_1}^2$, ${Y_1}^2$, ${Z_1}^2$, H^2, J^2 can be calculated using 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 power used in adding two distinct or similar points in OHEC and THEC using conventional method and techniques of AIVM are tabulated in Table 1 and Table 2.

Table 1. Comparison of the number of operations required for point addition in OHEC and THEC

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

It is obvious from Table 1 that number of operations, required for point doubling on OHEC and THEC using AIVM's techniques respectively reduce to 48.38% and 46.34% approximately. Table 2 shows that the number of operations, required for point doubling on OHEC and THEC using AIVM's techniques are lesser than that of conventional methods and respectively reduce to 34.78% and 43.33% approximately.

TABLE 2. Comparison of the number of operations required for point doubling on OHEC and THEC

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

Table 3 describes the processing time and percentage saving of time occurring in points addition and point doubling on OHEC and THEC using 16-bits processor, while Table 4 compares the said results using 32-bits processor. Furthermore, from Table 3 it is obvious that AIVM techniques help to reduce processing time for points addition and point doubling on OHEC up to 87 % approximately using 16-bits processor.

In the case of THEC AIVM techniques help to reduce processing time for points addition and point doubling up to 87.6% and 86.42% respectively. Table-4.4 represents that processing time for points addition and point doubling on OHEC can be increased up to 93.68% and 91.49% respectively, using 32-bits processor. Moreover, these processing times onTHEC can be increased up to 92.57% and 87% approximately.

TABLE 3. Processing time for arithmetic operations on OHEC and THEC based on 16-bits 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 %)
$OHEC$	0.0102450	0.0013320	86.9985	0.0092544	0.0011833	87.2141
$THEC$	0.0084565	0.0010485	87.6009	0.0076318	0.0010366	86.4175

TABLE 4. Processing time for arithmetic operations on OHEC and THEC based on 32-bits 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	0.0107600	0.00068045	93.6760	0.010364	0.00088221	91.4880
THEC	0.0097944	0.00072795	92.5676	0.0091592	0.00119530	86.9499

5. CONCLUSION

In this paper, some efficient and high-performance algorithms, using AIVM techniques for adding and doubling points on OHEC and THEC proposed. Although ECC uses less manipulation time for their execution, yet using AIVM techniques accelerate their speed of execution. As we have discussed in the previous section that the use of AIVM techniques for OHEC and THEC save the processing time required in points addition and point doubling. These techniques also improve conventional methods to use a lesser number of operations which result in terms of higher speed, less memory and low power consumption when implemented in practice.

REFERENCES

[1] A. A. CISS, D. SOW : *On a new generalization of Huff curves*, Journal IACR Cryptology ePrint Archive, (2011), 1–17. https://eprint.iacr.org/2011/580.pdf

[2] J. DEVIGNE, M. JOYE: *Binary Huff Curves*, Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science, Springer, **6558** (2011), 340–355.

[3] R. DRYLO, T. KIJKO, M. WRONSKI: *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, **2020** (2020), 1–27.

[4] H. EDWARDS: *A normal form for elliptic curves*, Bulletin of the American Mathematical Society, **44**(3) (2007), 393–422.

[5] H. GU, W. XIE, R. C. C. CHEUNG: *Efficient Pairing Computation on Huff Curves*, Cryptologia, **39**(3) (2015), 270–275.

[6] G. B. HUFF: *Diophantine problems in geometry and elliptic ternary forms*, Duke Math. J, **15** (1948), 443–453.

[7] A. R. JAFRI, M. N. ISLAM: *Towards an Optimized Architecture for Unified Binary Huff Curves*, Journal of Circuits, Systems, and Computers, **26**(22) (2017), 1–4.

[8] M. JOY, J. QUISQUATER: *Hessian elliptic curves and side-channel attacks*, Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science, **2162** (2001), 402–410.

[9] M. JOY, TIBOUCHI, D. VERGNAUD: *Huff's model for elliptic curves*, LNCS, Springer, Heidelberg, bf 6197 (2010), 234–250.

[10] P. LIARDET, N. SMART: *Preventing SPA or DPA in ECC systems using the Jacobi form*, Cryptographic Hardware and Embedded Systems CHES 2001, Lecture Notes in Computer Science, **2162** (2001), 391–401.

[11] M. SADEK, N. ELSISSI, A. S. ZARGAR, N. ZAMANI: *Evaluation of Gaussian hypergeometric series using Huff's models of elliptic curves*, The Ramanujan Journal, **48**(2) (2018), 357–368.

DEPARTMENT OF MATHEMATICS
GURUKULA KANGRI VISHWAVIDYALAYA
HARIDWAR (UTTARAKHAND) 249404, INDIA
Email address: sdmkg1@gmail.com

DEPARTMENT OF MATHEMATICS
GURUKULA KANGRI VISHWAVIDYALAYA
HARIDWAR (UTTARAKHAND) 249404, INDIA
Email address: ankurnehra123@gmail.com