ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **10** (2021), no.1, 353–366
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.35

LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS FOR POINTS ADDITION AND POINT DOUBLING ON JACOBI ELLIPTIC CURVES USING ANCIENT MATHEMATICAL TECHNIQUES

Manoj Kumar and Suryya Farhat [1]

ABSTRACT. This paper includes lightweight cryptography efficient algorithms for point additions and point doubling on Jacobi elliptic curve using Ancient Mathematics Techniques (AMT). AMT reduces the time complexity occurring in point doubling and point addition in Jacobi elliptic curves namely, Jacobi Intersections curve, Jacobi Quartic curve and twisted Jacobi Intersections curve. To get the square of any numbers we have used the Dvandva-yoga technique and Urdhva-tiryagbhyam technique is used for the multiplications of any numbers. MATLAB for 16-bits and 32-bits multiplications and squares is used for coding and synthesis. The results we obtained indicated that the AMT based methodology shows better and reliable operational performance compared to conventional methods, in the term of speed, processing time and power consumption of multipliers. The benefits or effect of using some AMT over Jacobi elliptic curves was examined and explained with graphs and tables.

[1] *corresponding author*

2020 *Mathematics Subject Classification.* 94A60, 14G50.

Key words and phrases. elliptic Curves, Elliptic Curve Cryptography, Urdhva-tiryagbhyam technique, Dvandva-yoga technique, Twisted Jacobi Intersection Elliptic Curve, Jacobi Quartic Elliptic Curve, Jacobi Intersection Elliptic Curve, Lightweight cryptography.

1. Introduction

For many years, the elliptic curves were studied by pure mathematicians and the results were exclusively used in mathematics like number theory and algebraic geometry, but later it was found that elliptic curve has extensive use in applied cryptography and in the year 1985 Miller [10] and Koblitz [5] invented the use of elliptic curve in cryptography and named it as Elliptic Curve Cryptography (ECC). Later it was realized that the process is slow and need to speed-up, several researchers proposed different algorithms, formulae, point presentations and various other suggestions. However, the limitation of speed to perform the computational steps of arithmetic on elliptic curve is still a question. For solving these arithmetical problems in ECC, various researchers have used many techniques in the past few decades. In the cryptosystem, the Jacobi elliptic curves is a representation of the elliptic curve different from the Weierstrass curve. Sometimes Jacobi elliptic curves are used in cryptographic systems instead of the Weierstrass curve form because it provides protection against simple power analysis (SPA) and Differential Power Analysis (DPS) attacks [4]. The Jacobi elliptic curves offer also faster arithmetic compared to the Weierstrass elliptic curves [2]. The Jacobi elliptic curves can be of three types the Jacobi Intersection elliptic curve (that is given by an intersection of two surfaces), the twisted Jacobi intersection elliptic curve (that is given by an intersection of two surfaces as a special case), the Jacobi Quartic elliptic curve (this curve is faster than the Jacobi Intersections elliptic curve), jacobi form of elliptic curves by Liarder and Smartin [8] (In projective space of 3-dimentions, the intersection of two quadric). The proposed that these elliptic curves in jacobi form could provide a protection against Differential Power Analysis (DPA) and Simple Power Analysis (SPA) style attacks. Feng et. al. [9] introduced the twisted jacobi intersections, in which jacobi intersection is assumed as a special case. They explained that the addition law is derived directly from underlying Quartic. Hisil et. al. [3] introduced the new terminology 'extended twisted Edwards Coordinates' and proposed the fastest coding ever in the literature using an efficient point addition algorithm. These algorithms are naturally protected from side channel attacks using Simple Power Analysis. Later Bernstein et. al. [1] modified the previous mechanism and introduced Edward Curves and obtained doubling and addition formulae over finite field of characteristic 2. They have developed the model to study Diophantine problem in this paper using elliptic curve model introduced by Jacobi [7] and developed a fast-clear-cut formula for doubling and adding points on Jacobi curves. They also obtained some extensions and generalization in this model and analysed the effect on Cryptography application using these curves. Few addition formulae were unified (remain valid for doubling a point) and they are valid for all the inputs even when restricted to the cyclic subgroup in Cryptographic settings [6].

This paper includes lightweight cryptography efficient algorithms for points addition and point doubling on Jacobi elliptic curve using ancient mathematics techniques. Ancient mathematical techniques (AMT) reduce the time complexity occurring in point doubling and point addition in Jacobi elliptic curves namely, Jacobi Intersections curve, Jacobi Quartic curve, and twisted Jacobi Intersections curve. To get the square of any numbers we have used the Dvandva-yoga technique and Urdhva-tiryagbhyam technique is used for for the multiplications of any numbers. MATLAB for 16-bits and 32-bits multiplications and squares is used for coding and synthesis. The results we obtained indicated that the AMT based methodology shows better and reliable operational performance compared to conventional methods, in the term of speed, processing time and power consumption of multipliers.

This paper is organized as follows. The section I consist of brief introduction about the topic.In section II, we gave a literature survey about some elliptic curves using some Ancient techniques of mathematics. In section III, we explained the Jacobi Intersections elliptic curves, the twisted Jacobi Intersections elliptic curves, the Jacobi Quartic elliptic curves and also their variants are discussed. In section IV, we analyzed and compared the number of required operations and performances in the Jacobi elliptic curves. In section V, we gave the conclusion of this paper.

2. Mathematical Background Of Jacobi Elliptic Curves

In this section, we will through some light on the salient features of the various forms of Jacobi elliptic curves namely, twisted Jacobi Intersections elliptic curve (TJIEC), Jacobi Intersections elliptic curve (JIEC), and Jacobi Quartic elliptic curve (JQEC) and its variants for the lightweight cryptographic operations such as point doubling and point adding.

2.1. **Jacobi Intersections Elliptic Curve (JIEC).** Liardet and Smart [8] introduced a new model of elliptic curves over the field $char(F) \neq 2$, in 2001. The Jacobi Intersections elliptic curve over the field F with $char(F) \neq 2$ which is defined as

$$E_{j,b} : \begin{cases} (x^2 + y^2 = 1) \\ (bx^2 + t^2 = 1) \end{cases}$$

where $E_{j,b}$ is the notation of Jacobi Intersections elliptic curve, $x, y, t$are the affine coordinates, $b$is an element of the field F, and $b\,(1 - b) \neq 0$. Liardet and Smart [8] obtained an efficient explicit formula for point doubling and point addition of the Jacobi Intersections elliptic curve $(E_{j,b})$ as follows:
The addition of two distinct points $P = (x_1, y_1, t_1)$ and $Q = (x_2, y_2, t_2)$ on the Jacobi elliptic curve $(E_{a,b})$ is given by the point$R(x_3, y_3, t_3)$.
Algebraically addition of two points is defined as:

$$P(x_1, y_1, t_1) + Q(x_2, y_2, t_2) = R(x_3, y_3, t_3)$$

where

$$(2.1) \qquad x_3 = \frac{x_1y_2t_2 + x_2y_1t_1}{y_2^2 + x_2^2t_1^2},\ y_3 = \frac{y_1y_2 - x_1x_2t_1t_2}{y_2^2 + x_2^2t_1^2} \text{ and } t_3 = \frac{t_1t_2 - bx_1x_2y_1y_2}{y_2^2 + x_2^2t_1^2}.$$

The addition of two points gives the doubling of point P

$$2P = P + P.$$

Algebraically it is defined as:

$$2P = P + P = R(x_3, y_3, t_3)$$

where

$$(2.2) \qquad x_3 = \frac{2x_1y_1t_1}{y_1^2 + x_2^2t_1^2},\ y_3 = \frac{y_1^2 - x_1^2t_1^2}{y_1^2 + x_2^2t_1^2} \text{ and } t_3 = \frac{t_1^2 - bx_1^2y_1^2}{y_1^2 + x_1^2t_1^2},$$

where $E_{j,b}$ is the notation of Jacobi Intersections elliptic curve, X, Y, T, Z are the projective coordinate system and b is an element of the field F.

2.2. **Twisted Jacobi Intersections Elliptic Curve (TJIEC).** In this subsection, we will discuss the features of generalized Jacobi elliptic curve and its variants respectively point addition and point doubling. Feng et al. [9] in 2006 introduced the special case of Jacobi intersection in the twisted Jacobi Intersection.

The twisted Jacobi Intersections elliptic curve over the field with which is defined as:

$$E_{j,a,b} : \begin{cases} \left(ax^2 + y^2 = 1\right) \\ \left(bx^2 + t^2 = 1\right) \end{cases} \tag{2.3}$$

where $E_{j,a,b}$ is the notation of twisted Jacobi Intersections elliptic curve, $x, y, t$are the affine coordinates,$a, b$are the elements of the field F, and $ab\,(a-b)?0$. They obtained an efficient explicit formula for point addition and point doubling of the twisted Jacobi Intersections elliptic curve $(E_{j,a,b})$ as follows:
The addition of two distinct points $P = (x_1, y_1, t_1)$ and $Q = (x_2, y_2, t_2)$ on the twisted Jacobi Intersections elliptic curve $(E_{j,a,b})$ is given by the point$R(x_3, y_3, t_3)$, then
Algebraically addition of two points is defined as:
i.e. $P(x_1, y_1, t_1) + Q(x_2, y_2, t_2) = R(x_3, y_3, t_3)$
where

$$x_3 = \frac{x_1y_2t_2 + x_2y_1t_1}{y_2^2 + ax_2^2t_1^2}, y_3 = \frac{y_1y_2 - ax_1x_2t_1t_2}{y_2^2 + ax_2^2t_1^2}, t_3 = \frac{t_1t_2 - bx_1x_2y_1y_2}{y_2^2 + ax_2^2t_1^2}\,. \tag{2.4}$$

The doubling of a point $P$is nothing but it is the addition of two identical points i.e. $2P = P + P$.
Algebraically doubling of a point P is defined as:

$$2P = P + P = R(x_3, y_3, t_3)\,,$$

where

$$x_3 = \frac{2x_1y_1t_1}{y_1^2 + ax_2^2t_1^2}, y_3 = \frac{y_1^2 - ax_1^2t_1^2}{y_1^2 + ax_2^2t_1^2}t_3 = \frac{t_1^2 - bx_1^2y_1^2}{y_1^2 + ax_1^2t_1^2}\,, \tag{2.5}$$

where $E_{j,a,b}$ is the notation of twisted Jacobi Intersections elliptic curve, $X, Y, T, Z$are the projective coordinate system and a, b are the elements of the field F.

2.3. **The Modified Jacobi Quartic Elliptic Curve (MJQEC).** In 2003, Billet and Joey [7] introduced first time the Jacobi Quartic elliptic curve over the finite field F with $char(F) \neq 2, 3$ and which is defined as:

$$E_{j,k} : y^2 = k^2x^4 - \left(k^2 + 1\right)x^2 + 1 \tag{2.6}$$

where $E_{j,k}$ is the notation of Jacobi Quartic elliptic curve, $(x, y)$are the affine coordinates and $k?0, \pm 1$. To improve the security parameter, Hisil et al. [3] in

2009 introduced the modified Jacobi Quartic elliptic curves which are defined as:

$$E_{j,d,a} : y^2 = dx^4 + 2ax^2 + 1 \tag{2.7}$$

where $E_{j,d,a}$ is the notation of modified Jacobi Quartic elliptic curves, (x, y) are the affine coordinates, (a, d) are the elements of the field F, with $char(F) \neq 2, 3$. They obtained an efficient explicit formula for point addition and point doubling of the modified Jacobi Quartic elliptic curves $E_{j,d,a}$ as follows:
The addition of two distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the modified Jacobi Quartic elliptic curves $E_{j,d,a}$ is given by the point $R(x_3, y_3)$, then
Algebraically addition of two points is defined as:
i.e. $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$
where

$$x_3 = \frac{(x_1y_2 + x_2y_1)}{(1 - dx_1^2x_2^2)}, y_3 = \frac{(y_1y_2 + 2ax_1x_2)\,(1 + dx_1^2x_2^2) + 2dx_1x_2\,(x_1^2 + x_2^2)}{(1 - dx_1^2x_2^2)^2}\,. \tag{2.8}$$

The doubling of a point $P$is nothing but it is the addition of two identical points i.e. $2P = P + P$.
Algebraically doubling of a point P is defined as:

$$2P = P + P = R(x_3, y_3)\,,$$

where

$$x_3 = \frac{2x_1y_1}{2 + 2ax_1^2 - y_1^2}, y_3 = \frac{4y_1^2 - (2 + 2ax_1^2 - y_1^2)\,(2 + 2ax_1^2 + y_1^2)}{(2 + 2ax_1^2 - y_1^2)^2}\,. \tag{2.9}$$

3. Projective Homogeneous Coordinates System

In the cryptography, the projective homogeneous coordinate system is used to avoid the inversion in the Edwards addition formulae. The projective coordinate system is a 3-dimensional coordinate system in which every elliptic curve point P with affine coordinates (x, y, t) is mapped to a unique point P' with projective coordinates (X, Y, Z, T) using the following transformations:

$$(x, y, t) \neq \left(\frac{X}{Z}, \frac{Y}{Z}, \frac{T}{Z}\right), \; (x, y) \neq \left(\frac{X}{Z}, \frac{Y}{Z^2}\right)\,. \tag{3.1}$$

Using the above transformation (3.1), Jacobi Intersections elliptic curve $(E_{j,b})$, twisted Jacobi Intersections elliptic curve $(E_{j,a,b})$ and Jacobi Quartic elliptic curve $(E_{j,d,a})$in projective coordinates system respectively can be represented as

$$E_{j,b} : \begin{cases} (X^2 + Y^2 = Z^2) \\ (bX^2 + T^2 = Z^2) \end{cases}, E_{j,a,b} : \begin{cases} (aX^2 + Y^2 = Z^2) \\ (bX^2 + T^2 = Z^2) \end{cases}, \tag{3.2}$$
$$E_{j,d,a} : Y^2 = dX^4 + 2aX^2Z^2 + Z^4 .$$

4. Proposed Schemes

This section consists of proposed some efficient cryptographic schemes using AMT techniques together with projective homogeneous coordinates for adding and doubling points on Jacobi elliptic curves namely Jacobi Intersections elliptic curve (JIEC), Jacobi Quartic elliptic curve (JQEC), and twisted Jacobi Intersections elliptic curve (TJIEC).

4.1. Proposed Algorithm.

(1) Addition of two distinct points. $\boldsymbol{P}$ **and** $\boldsymbol{Q}$ **in Jacobi Intersections Elliptic Curve** $(\boldsymbol{E_{j,b}})$
Using equations (2.1), (2.2) and (3.1) the addition of two distinct points $P = (X_1, Y_1, T_1, Z_1)$ and $Q = (X_2, Y_2, T_2, Z_2)$ on the Jacobi Intersections elliptic curve $(E_{j,b})$ is given by the point$R(X_3, Y_3, T_3, Z_3)$, then
$P(X_1, Y_1, T_1, Z_1) + Q(X_2, Y_2, T_2, Z_2) = R(X_3, Y_3, T_3, Z_3)$, where

$$\begin{aligned} X_3 &= X_1Y_2Z_1T_2 + X_2Y_1Z_2T_1, Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2 \\ T_3 &= T_1T_2Z_1Z_2 - bX_1X_2Y_1Y_2, Z_3 = Y_2^2Z_1^2 + X_2^2T_1^2 . \end{aligned}$$

Now corresponding algorithm using AMT techniques is explained as under:
Input: : $P = (X_1, Y_1, T_1, Z_1)$, $Q = (X_2, Y_2, T_2, Z_2)$ and $Output : R = P + Q = (X_3, Y_3, T_3, Z_3)$ $\boldsymbol{A = X_1 \cdot X_2}$**,**$\boldsymbol{B = Y_1 \cdot Y_2}$**,** $\boldsymbol{C = Z_1 \cdot Z_2}$**,** $\boldsymbol{D = T_1 \cdot T_2}$**,** $\boldsymbol{E = X_1 \cdot Y_2}$**,**$\boldsymbol{F = Z_1 \cdot T_2}$**,** $\boldsymbol{G = X_2 \cdot Y_1}$**,** $\boldsymbol{H = Z_2 \cdot T_1}$**,** $\boldsymbol{I = Y_2 \cdot Z_1}$**,** $\boldsymbol{J = X_2 \cdot T_1}$**,** $\boldsymbol{X_3 = E \cdot F + G \cdot H}$**,** $\boldsymbol{Y_3 = B \cdot C - A \cdot D}$**,** $\boldsymbol{T_3 = C \cdot D - b \cdot A \cdot B}$**,** $\boldsymbol{Z_3 = I^2 + J^2}$**,** $\boldsymbol{Return}\,(\boldsymbol{X_3 : Y_3 : T_3 : Z_3})$

Where all squares values $\left(\boldsymbol{I^2}, \boldsymbol{J^2}\right)$ are calculated using Dvandva-yoga technique and all multiplications values $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{H}, \boldsymbol{I}, \boldsymbol{J}, \boldsymbol{X_3}, \boldsymbol{Y_3}, \boldsymbol{Z_3})$ are calculated using Urdhva-tiryagbhyam technique of AMT.

(2) Addition of two distinct points $\boldsymbol{P}$ **and** $\boldsymbol{Q}$ **in twisted Jacobi Intersections Elliptic Curve** $(\boldsymbol{E_{j,b}})$

Using equations (2.3), (2.4), (2.8) and (3.1) the addition of two distinct points $P = (X_1, Y_1, T_1, Z_1)$ and $Q = (X_2, Y_2, T_2, Z_2)$ on the twisted Jacobi Intersections elliptic curve $(E_{j,b})$ is given by the point$R(X_3, Y_3, T_3, Z_3)$, then

i.e. $P(X_1, Y_1, T_1, Z_1) + Q(X_2, Y_2, T_2, Z_2) = R(X_3, Y_3, T_3, Z_3)$, where

$$\begin{aligned} X_3 &= X_1Y_2Z_1T_2 + X_2Y_1Z_2T_1, Y_3 = Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2, \\ T_3 &= T_1T_2Z_1Z_2 - bX_1X_2Y_1Y_2, Z_3 = Y_2^2Z_1^2 + aX_2^2T_1^2. \end{aligned}$$

Now corresponding algorithm using AMT techniques is explained as under:

Input: P = (X_1, Y_1, T_1, Z_1), Q = (X_2, Y_2, T_2,Z_2), a and b, Output: R = P + Q = (X_3, Y_3, T_3,Z_3), A = X_1 . X_2, B = Y_1 . Y_2, C = Z_1 . Z_2, E = X_1 . Y_2, F = Z_1 . T_2, G = X_2 . Y_1, H = Z_2 . T_1, I = Y_2 . Z_1, J = X_2 . T_1, X_3 = E. F + G. H, Y_3 = B. C – a . A. D, T_3 = C. D – b . A. B, Z_3 = I^2 + a . J^2, Return(X_3: Y_3: T_3: Z_3).

Where all squares values $\left(\boldsymbol{I^2}, \boldsymbol{J^2}\right)$ are calculated using Dvandva-yoga technique and all multiplications values $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{H}, \boldsymbol{I}, \boldsymbol{J}, \boldsymbol{X_3}, \boldsymbol{Y_3}, \boldsymbol{Z_3})$ are calculated using Urdhva-tiryagbhyam technique of AMT.

(3) Doubling of a point $\boldsymbol{P}$**in Twisted Jacobi Intersections Elliptic Curve** $(\boldsymbol{E_{j,a,b}})$

Using equations (2.3), (2.4), (2.8) and (3.1) the doubling of a point $P = (X_1, Y_1, T_1, Z_1)$ on the Jacobi Intersections elliptic curve $(E_{j,a,b})$ is given by the point$R(X_3, Y_3, T_3, Z_3)$, then $P(X_1, Y_1, T_1, Z_1) + P(X_1, Y_1, T_1, Z_1) = R(X_3, Y_3, T_3, Z_3)$

Where$X_3 = 2X_1Y_1Z_1T_1$,$Y_3 = Y_1^2Z_1^2 - aX_1^2T_1^2$, $T_3 = Z_1^2T_1^2 - b \cdot X_1^2Y_1^2$, and$Z_3 = Y_1^2Z_1^2 + aX_1^2T_1^2$.

Now corresponding algorithm using AMT techniques is explained as under:

Input: P = (X$_1$*, Y*$_1$*, T*$_1$*, Z*$_1$*), a and b, Output: R = P + P = 2P = (X*$_3$*, Y*$_3$*, T*$_3$*, Z*$_3$*), A = X*$_1$ *.Y*$_1$*, B = Z*$_1$ $_.$ *T*$_1$*, C = Y*$_1$ *.Z*$_1$*, D = X*$_1$ *.T*$_1$*, X*$_3$ *= 2 . A . B, Y*$_3$ *= C*^{2} *– a . D*^{2}*, T*$_3$ *= B*^{2} *– b. A*^{2}*, Z*$_3$ *= C*^{2} *+ a. D*^{2}*, Return(X*$_3$*, Y*$_3$*, T*$_3$*, Z*$_3$*).*
Where all squares values $\left(\boldsymbol{A^2}, \boldsymbol{B^2}, \boldsymbol{C^2}, \boldsymbol{D^2}\right)$ are calculated using Dvandva-yoga technique and all multiplications values $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{X_3}, \boldsymbol{Y_3}, \boldsymbol{Z_3})$ are calculated using Urdhva-tiryagbhyam technique of AMT.

(4) Addition of two distinct points $\boldsymbol{P}$ **and** $\boldsymbol{Q}$ **in Modified Jacobi Quartic elliptic curves** $(\boldsymbol{E_{j,d,a}})$
Using equations (2.6), (2.7), (2.9) and (3.2) the addition of two distinct points $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ on the modified Jacobi Quartic elliptic curves $E_{j,d,a}$ are given by the point$R(X_3, Y_3, Z_3)$, then i.e. $P(X_1, Y_1, Z_1) + Q(X_2, Y_2, Z_2) = R(X_3, Y_3, Z_3)$

$$\begin{aligned} X_3 &= X_1Y_2Z_1 + X_2Y_1Z_2, \\ Y_3 &= \left[(Z_1Z_2)^2 + d(X_1X_2)^2\right](Y_1Y_2 - 2aX_1X_2Z_1Z_2) + \\ &\quad + \left[(X_1Z_1)^2 + d(X_2Z_1)^2\right](2dX_1X_2Z_1Z_2) \\ Z_3 &= \left[(Z_1Z_2)^2 + d(X_1X_2)^2\right]. \end{aligned}$$

Now corresponding algorithm using AMT techniques is explained as under:
Input: P = (X$_1$*, Y*$_{1,}$ *Z*$_1$*), Q = (X*$_2$*, Y*$_2$*, Z*$_2$*), a and d, Output: R = P + Q = (X*$_3$*, Y*$_{3,}$ *Z*$_3$*), A = X*$_1$*. X*$_2$*, B = Y*$_1$*. Y*$_2$*, C = Z*$_1$*. Z*$_2$*, D = X*$_1$*. Z*$_1$*, E = X*$_2$*. Z*$_2$*, F = X*$_1$*. Z*$_2$*, G = X*$_2$*. Z*$_3$*, H = C*^{2}*, I = d. A*^{2}*, J = H + I, K = 2. A. C, L = E*^{2} *+ G*^{2}*, M = d. L – a. J, X*$_3$ *= Y*$_1$*. E + Y*$_2$*. D, Y*$_3$ *= J. B + K. M, Z*$_3$ *= H – I, Return(X*$_3$*: Y*$_3$*: Z*$_3$*)*
Where all squares values $\left(\boldsymbol{A^2}, \boldsymbol{C^2}, \boldsymbol{F^2}, \boldsymbol{G^2}\right)$ are calculated using Dvandva-yoga technique and all multiplications values $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{I}, \boldsymbol{K}, \boldsymbol{M}, \boldsymbol{X_3}, \boldsymbol{Y_3})$ are calculated using Urdhva-tiryagbhyam technique of AMT.

5. 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 Jacobi Intersections elliptic curve $(E_{j,b})$, Modified Jacobi Quartic elliptic curve $(E_{j,d,a})$, and twisted Jacobi Intersections elliptic curve $(E_{j,a,b})$ for Jacobian coordinates systems using conventional method and AMT techniques are tabulated in Table 1 and Table 2.

TABLE 1. Comparison of the number of operations required for point addition in the curves $(E_{j,b})$, $(E_{j,a,b})$, $(E_{j,d,a})$

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
$E_{j,b}$	21	4	0	0	25	17	2	0	0	19
$E_{j,a,b}$	23	4	0	0	27	19	2	0	0	21
$E_{j,d,a}$	25	12	0	0	37	16	4	0	0	20

Here
$P_1 \rightarrow$ Total number of multiplications, $P_2 \rightarrow$ Total number of squares,$P_3 \rightarrow$ Total number of cubes,$P_4 \rightarrow$ Total number of the fourth power, S →Sum ofP_1,P_2,P_3 and P_4.

TABLE 2. Comparison of the number of operations required for point doubling in the curves $(E_{j,b})$, $(E_{j,a,b})$, $(E_{j,d,a})$

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
$\boldsymbol{E_{j,b}}$	11	12	0	0	23	7	4	0	0	11
$\boldsymbol{E_{j,a,b}}$	12	12	0	0	24	9	4	0	0	13
$\boldsymbol{E_{j,d,a}}$	19	10	0	5	34	10	5	0	0	15

It is obvious from Table 1 that for the curves$(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ the number of used operations in point addition using AMT techniques respectively reduced to 48 %, 50 %, and 52 % approximately. Table 6.2 shows that the number of used arithmetic operations, in point doubling using AMT techniques for the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ are respectively 51 %, 62 %, and 48 % lesser than that of conventional methods. Tables 3 and 4 describe the processing time and percentage saving of time occurring for points addition and point doubling in the previous said the curves$(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ using 8-bits and 16-bits processor respectively. AMT techniques help to reduce 86 % to 88 % saving of processing time for points addition in the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ while for point doubling it reduce 86 % to 87 % savings of processing time in above said the system for 8-bit processor. For 16-bits processor AMT techniques improve percentage savings of time 92 % to 93 % in points addition and point doubling improve percentage savings of time 86 % to 91 %.

TABLE 3. Processing time for arithmetic operations in the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ based on 8-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 %)
$\boldsymbol{E_{j,b}}$	0.010245	0.001332	86.9985	0.0092544	0.0011833	87.2141
$\boldsymbol{E_{j,a,b}}$	0.0084565	0.0010485	87.6009	0.0076318	0.0010366	86.4175
$\boldsymbol{E^{1}{}_{j,d,a}}$	0.0097944	0.00072795	92.5676	0.0091592	0.0011953	86.9499

Where
$\boldsymbol{T^{A}_{ECC}}$ →Processing time for points addition using the conventional method, $\boldsymbol{T^{A}_{VECC}}$ → Processing time for points addition using AMT techniques, $\boldsymbol{T^{A}_{S}}$ → Percentage saving of processing time for point addition using AMT techniques, $\boldsymbol{T^{D}_{ECC}}$ → Processing time for point doubling using the conventional method, $\boldsymbol{T^{D}_{VECC}}$ → Processing time for point doubling using AMT techniques, $\boldsymbol{T^{D}_{S}}$ → Percentage saving of processing time for point doubling using AMT techniques.

Figure 1 and 2 comprise the different type of arithmetic operations required in the curves$(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ for point addition and point doubling respectively. It is obvious from Figures 1 and 2 that AMT techniques do not use cube operations for point addition and point doubling in each elliptic curves,

TABLE 4. Processing time for arithmetic operations in the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$ based on 16-bits processor using conventional and AMT 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 %)
$\boldsymbol{E_{j,b}}$	0.01076	0.00068045	93.6760	0.010364	0.00088221	91.4880
$\boldsymbol{E_{j,a,b}}$	0.0087956	0.00072795	92.5676	0.0091592	0.0011953	86.9499
$E_{j,d,a}$	0.0087900	0.00075797	90.5670	0.0086712	0.0018966	85.5477

which shows that AMT techniques are helpful to accelerate the speed of ECC, based cryptosystem.

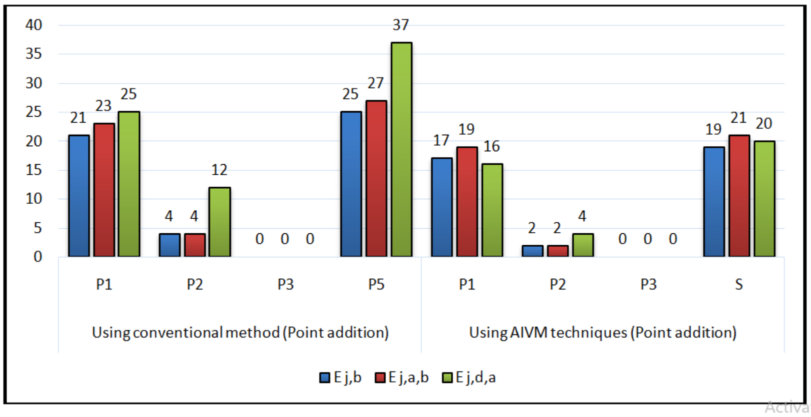

FIGURE 1. Comparison of different type of arithmetic operations required for point: Additions in the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$

6. CONCLUSION

In this paper, some lightweight, efficient and high-performance algorithms, using AMT for adding and doubling points on the curves$(E_{j,b})$, $(E_{j,a,b})$, $(E_{j,d,a})$ and $(E^{*}_{j,d,a})$ are proposed. Although ECC uses less manipulation time for their

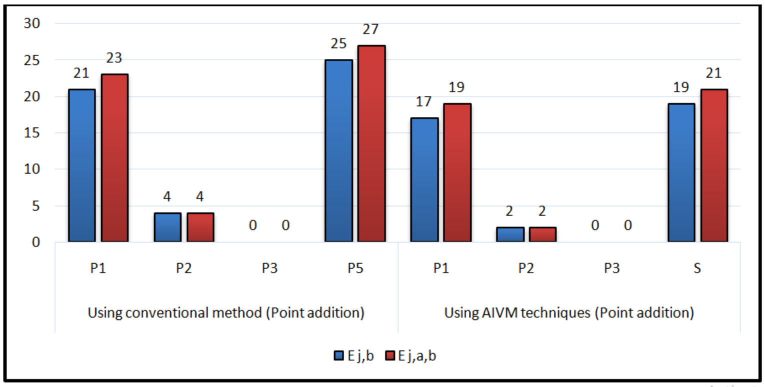

FIGURE 2. Doubling in the curves $(E_{j,b})$, $(E_{j,a,b})$ and $(E_{j,d,a})$

execution, yet using AMT accelerate their speed of execution. As we discussed in the previous section that the use of AMT techniques in Jacobi elliptic curves save the processing time required in points addition and point doubling, it also uses a lesser number of operations which result in terms of higher speed, less memory ,low power consumption when implemented in practice and make it lightweight. The result of comparative analysis indicated that the lightweight algorithms consume less memory, less power and have less operations as compared to conventional algorithms of cryptography.

REFERENCES

[1] D. BERNSTEIN, T. LANGE: *Faster addition and doubling on elliptic curves*, Progress in Cryptology - Africacrypt 2007, Lecture Notes in Computer Science, **4833** (2007), 29-50.

[2] G. FREY, T. LANGE: *Background on Curves and Jacobians*, in CFD05, (2005), 45–85.

[3] H. HISIL, K. KOON-HO WONG, G. CARTER, E. DAWSON: *Jacobi Quartic Curves Revisited*, ACISP, **2009**, (2009), 452-468.

[4] M. ASHRAF, B.B. KıRLAR: *On the Alternate Models of Elliptic Curves,* International Journal of Information Security Science, 49-66, 2012.

[5] N. KOBLITZ: *Elliptic curve cryptosystems*, Mathematics of Computation, **48** (1987), 203–209.

[6] N. SMART, E. J. WESTWOOD: *Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three*, Appl. Algebra Eng. Commun. Comput. , **13** (2003), 485-497.

[7] O. BILLET, M. JOYE: *The Jacobi model of an elliptic curve and side-channel analysis*, AAECC 2003, Lecture Notes in Computer Science, **2643** Springer-Verlag, (2003), 34-42.

[8] P. Liardet, N. Smart: *Preventing SPA/DPA in ECC systems using the Jacobi form*, Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science, **2162** (2001), 391-401.

[9] R. Feng, M. Nie, H. Wu: *Twisted Jacobi Intersections Curves*. Available at http://eprint.iacr.org/2009/597.pdf

[10] V. S. Miller: *Use of elliptic curves in cryptography'*, Advances in Cryptology Proceedings of Crypto' 85, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, 417–426.

Department of Mathematics and Statistics
Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA
Email address: sdmkg1@gmail.com

Department of Mathematics and Statistics
Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA
Email address: suryyafarhat@gmail.com