New Quintupling Point Arithmetic 5P Formulas for Lŏpez-Dahab Coordinate over Binary Elliptic Curve Cryptography

Waleed K. AbdulRaheem[1], Sharifah Bte Md Yasin[2], Nur Izura Binti Udzir[3]
Muhammad Rezal Bin Kamel Ariffin[4]
Faculty of Computer Science and Information Technology[1, 2, 3]
Institute for Mathematical Research[4]
University Putra Malaysia, Selangor, Malaysia

***Abstract*—In Elliptic Curve Cryptography (ECC), computational levels of scalar multiplication contains three levels: scalar arithmetic, point arithmetic and field arithmetic. To achieve an efficient ECC performance, precomputed points help to realize a faster computation, which takes away the need to repeat the addition process every time. This paper introduces new quintupling point (5P) formulas which can be precomputed once and can be reused at the scalar multiplication level. We considered mixed addition in Affine and Lŏpez-Dahab since the mixed addition computation cost is better than the traditional addition in Lŏpez-Dahab coordinates over binary curve. Two formulas are introduced for the point quintupling which ($\boldsymbol{Double\ Double\ Add}$) and ($\boldsymbol{Triple\ Add\ Double}$), the cost of the two formulas are $\mathbf{17\ multiplication + 12\ squaring}$ and $\mathbf{23\ multiplication + 13\ squaring}$ respectively. The two formulas are proven as valid points. The new quintupling point can be implemented with different scalar multiplication methods.**

***Keywords*—Elliptic Curve Cryptosystem (ECC); scalar multiplication algorithm; point arithmetic; point quintupling; Lŏpez-Dahab (LD); binary curve**

I. Introduction

Elliptic curves cryptosystem (ECC) was proposed by Neal Koblitz and Victor Miller independently in 1985 for the public-key cryptographic system [1]. Similar to other public key cryptographic algorithms, elliptic curve cryptosystem deploys a public key and private key. The public key is used for encryption to provide data confidentiality during communication. ECC is implemented in smart card because of its smaller key size and less computational complexity relative to RSA cryptosystem [2] and [3]. This makes it attractive and suitable for such applications [4].

Working on ECC, scalar multiplication contains three levels of computation such as scalar arithmetic, point arithmetic and field arithmetic [5] as shown in Fig. 1. Scalar arithmetic is to find the value of kP=P+P+…+P (k times) where k is binary. Point arithmetic contains the operations on the point in ECC such as doubling and addition. Finally, field arithmetic contains the operations to calculate the scalar multiplication such as addition, squaring, multiplication and inverse in the field.

Point arithmetic layer is the operations on the point in ECC. Precomputed points help to realize a faster computation which takes away the need to repeat the addition process every time [6]. The operations comprise of point addition (Q+P), point doubling (2P), point tripling (3P), point quadrupling (4P), point quintupling (5P), point septupling (7P) and so on.

Different precomputed quintupling point 5P have been proposed in different coordinates over different curves. A new 5P is proposed by [7] for Jacobian coordinates over prime field where the coefficient in the general equation $a\ \neq 3$, the cost of the proposed point is $15M\ +\ 10S$, where M and S are multiplication and squaring respectively. This point over the same coordinate, condition and curve has been improved. In [8], they optimized formula is of the cost $8M\ +\ 16$. Recently, two optimized formula are proposed for the previous point in [9] and [10], where the cost of the formulas are $10M\ +\ 14S$ and $8M\ +\ 16S$ respectively.

Over Edward curve in the prime field, different point quintupling 5P formulas are proposed. In [11], the authors proposed a formula of the cost $17M\ +\ 7S$. This formula is improved by [10] with cost of $15M\ +\ 9S$. On the other hand, over the binary field, a new point quintupling is proposed using λ projective coordinate by [12], with the cost of $13M + 8S$, the authors had shown up that there is no point quintupling 5P formula for the general binary curve in López-Dahab (LD) coordinate.

The contributions of this paper are as follows: Two point arithmetic formulas for López-Dahab coordinate are proposed over the general binary curve using mixed addition and doubling [13] method. The first point is of form $5P = 3P + 2P$ (Tripling addition to doubling) of cost $23M + 13S$. An enhancement to this point is proposed using the form $5P = 2(2P) + P$ (Doubling doubling addition to point) of cost $17M + 12S$. The two formulas are validation proved.

The remainder of this paper is organized as follows: Section 2 discusses the related work, while Section 3 introduces the proposed algorithms, cost analysis and the validation proof. While, conclusion and future works are presented in Section 4.

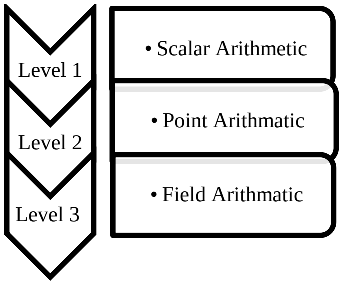

Fig. 1. Computational Levels in ECC Scalar Multiplication.

II. Related Works

General binary curve (short Weierstrass curve) as follows [14]:

$$E: y^2 + \mathrm{x}\mathrm{y} = x^3 + \ ax^2 \ + \ b \qquad (1)$$

where the projective point $(X: Y: Z)$ and $Z \neq 0$ defined over LD projective coordinates has the equation:

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \qquad (2)$$

Point addition for LD first proposed by [15] as in Algorithm 1 of costs $14M + 6S + 8A$.

Algorithm 1: The projective form of two points adding formula in LD coordinate where $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$ is:

$A_0 \leftarrow Y_2Z_1^2$ $\quad D \leftarrow B_0 + B_1$ $\quad H \leftarrow CF$

$A_1 \leftarrow Y_2Z_2^2$ $\quad E \leftarrow Z_0Z_1$ $\quad X_3 \leftarrow C^2 + H + G$

$B_0 \leftarrow X_2Z_1$ $\quad F \leftarrow DE$ $\quad I \leftarrow D^2B_0E + X_3$

$B_1 \leftarrow X_1Z_2$ $\quad Z_3 \leftarrow F^2$ $\quad J \leftarrow D^2A_1 + X_3$

$C \leftarrow A_0 + A_1$ $\quad G \leftarrow D^2(F + aE^2)$

$\mathrm{Y_3 \leftarrow HI + Z_3J}$

For the special case where $Z_2 = 1$, this formula can be improved as:

$\mathrm{(X_1, Y_1, Z_1) + (X_2, Y_2, 1) = (X_3, Y_3, Z_3)}$

$\mathrm{A \leftarrow Y_2Z_1^2 + Y_1}$ $\quad \mathrm{E \leftarrow AC}$

$\mathrm{B \leftarrow X_2Z_1 + X_1}$ $\quad \mathrm{X_3 \leftarrow A^2 + D + E}$

$\mathrm{C \leftarrow Z_1 + B}$ $\quad \mathrm{F \leftarrow X_3 + X_2Z_3}$

$\mathrm{D \leftarrow B^2(C + aZ_1{}^2\ )}$ $\quad \mathrm{G \leftarrow X_3 + Y_2Z_3}$

$\mathrm{Z_3 \leftarrow C^2}$ $\quad \mathrm{Y_3 \leftarrow EF + Z_3G}$

To reduce the cost of point arithmetic, a formula involving parameters such as $A_0, D, T, \ldots$ amongst others can be used to calculate the parameters X_3, Y_3, and Z_3.

This formula has been improved by [16] where the authors reduced the cost to be $13M + 4S + 9A$ using the formula as in Algorithm 2.

Algorithm 2: The projective form of two points adding formula in LD coordinate where $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$ is:

$\mathrm{A \leftarrow X_1Z_2}$ $\quad \mathrm{E \leftarrow A + B}$ $\quad \mathrm{I \leftarrow G + H}$

$\mathrm{B \leftarrow X_2Z_1}$ $\quad \mathrm{F \leftarrow C + D}$ $\quad \mathrm{J \leftarrow IE}$

$\mathrm{C \leftarrow A^2}$ $\quad \mathrm{G \leftarrow Y_1Z_2^2}$ $\quad \mathrm{Z_3 \leftarrow FZ_1Z_2}$

$\mathrm{D \leftarrow B^2}$ $\quad \mathrm{H \leftarrow Y_2Z_1^2}$

$\mathrm{X_3 \leftarrow A(H + D) + B(C + G)}$

$\mathrm{Y_3 \leftarrow (AJ + FG)F + (J + Z_3)X_3}$

A new formula for point addition using mixed addition in affine LD coordinate is proposed by [13], with cost of $9M + 5S + 9A$ as shown in Algorithm 3.

Algorithm 3: The projective form of two points P and Q adding formula where $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$ such that $Z_1 = 1$, $P$is in affine and Q is in LD coordinate is given as:

$\mathrm{A \leftarrow\ Y_2\ +\ Y_1Z_2^2}$ $\quad \mathrm{B \leftarrow\ X_2 +\ X_1Z_2}$

$\mathrm{C \leftarrow BZ_2}$ $\quad \mathrm{Z_3 \leftarrow\ C^2}$ $\quad \mathrm{D \leftarrow\ X_1Z_3}$

$\mathrm{X_3 \leftarrow\ A^2\ +\ C(A\ +\ B^2\ +\ aC)}$

$\mathrm{Y_3 \leftarrow\ (D\ +\ X_3)(AC\ +\ Z_3)\ +\ (Y1\ +\ X1)Z_3^2}$

Doubling of point P is the operation of adding the point to itself as $P + P = 2P$. Over LD coordinate, the first doubling formula is proposed by [15] with cost of $5M + 4S + 5A$ as presented in Algorithm 4.

Algorithm 4: The projective form of point doubling formula in LD coordinates where $2(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$ is given as:

$\mathrm{A \leftarrow Z_1^2}$ $\quad \mathrm{B \leftarrow bA^2}$ $\quad \mathrm{C \leftarrow X_1^2}$

$\mathrm{Z_2 \leftarrow AC}$ $\quad \mathrm{X_2 \leftarrow C^2 + B}$

$\mathrm{Y_2 \leftarrow (Y_1^2 + aZ_2 + B)X_2 + Z_2B}$

The projective form of point doubling formula in LD coordinate given in Definition 4 is modified by [17], by adding one field addition while reducing one field squaring, so the total cost of the improved formula is $5M + 4S + 5A$ as presented in Algorithm 5.

Algorithm 5: The projective form of point doubling $2P$ formula in LD coordinate system is given as:

$\mathrm{A \leftarrow X_1^2}$ $\quad \mathrm{B \leftarrow A + Y_1}$ $\quad \mathrm{C \leftarrow X_1Z_1}$

$\mathrm{D \leftarrow BC}$ $\quad \mathrm{Z_2 \leftarrow C^2}$ $\quad \mathrm{X_2 \leftarrow B^2 + D + aZ_2}$

$\mathrm{Y_2 \leftarrow (Z_2 + D)X_2 + A^2Z_2}$

The operation of adding a point P to itself three times is a point tripling, such that $3P = P + P + P$. Tripling point can also take the form of the addition of a point with a point doubling such that $3P = 2P + P$. The lowest cost point tripling over LD coordinate is proposed by [18], as shown in Algorithm 6, the cost of the tripling formula is $12M + 7S$, where addition operation is neglected since it has the cheapest field arithmetic cost [19].

Algorithm 6: The point $3P = (X_3, Y_3, Z_3)$ is tripling for $P = (X_1, Y_1, Z_1)$ where $3P = 2P + P$ has the formula as:

The point $2P = (X_2, Y_2, Z_2)$ is doubling for $P = (X_1, Y_1, Z_1)$ where [17]:

$S \leftarrow X_1^2 \quad U \leftarrow S + Y_1 \qquad T \leftarrow X_1Z_1$

$R \leftarrow UT \; Z_2 \leftarrow T^2 \qquad X_2 \leftarrow U^2 + R + aZ_2$

$Y_2 \leftarrow (Z_2 + R)X_2 + S^2Z_2$

The point $3P = (X_3, Y_3, Z_3)$ is tripling

$A \leftarrow (Z_2 + E)X_2 + Z_2^2 + U\,B \leftarrow X_2 + X_1X_2$

$C \leftarrow BZ_2\,C \leftarrow BZ_2Z_3 \leftarrow C^2 \qquad D \leftarrow X_1Z_3$

$E \leftarrow UX_1 \qquad X_2 \leftarrow U^2 + E + aZ_2$

$X_3 \leftarrow A^2 + C(A + B^2) + aZ_3$

$Y_2 \leftarrow (X_3 + D)(AC + Z_3) + (Y_1 + X_1)Z_3^2$

Let $Z_3 \rightarrow 0$ then:

$A \leftarrow (Z_2 + E)X_2 + Z_2^2 + U\,B \leftarrow X_2 + X_1X_2$

$C \leftarrow BZ_2\,C \leftarrow BZ_2\,C^2 \leftarrow 1$(Neglected)

$D \leftarrow X_1Z_3 \qquad E \leftarrow UX_1 \qquad X_2 \leftarrow U^2 + E + aZ_2$

$X_3 \leftarrow A^2 + C(A + B^2) + a$

$Y_2 \leftarrow (X_3 + D)(AC + 1) + (Y_1 + X_1)$

III. PROPOSED ALGORITHMS

This paper aims to propose a new quintupling point 5P over general binary curve (short Weierstrass curve) which is given by (1) using LD coordinate. Two forms can be used to formulate the quintupling point 5P, which are $5P = 3P + 2P$ and $5P = 2(2P) + P$. For both cases, point doubling and point addition are required. For point doubling, the minimal form is as mentioned in Algorithm 5. While for point addition, a mixed addition formula using the affine and LD coordinate proposed in Algorithm 3 is usually deployed since the mixed addition is much faster [17].

The first quintupling point formula will be introduced using the formula $5P = 3P + 2P$, which require three operations, point tripling with mixed addition to point doubling. According to [12], the lowest tripling point 3P cost is the formula given in Algorithm 6. The proposed 5P formula is as presented in Algorithm 7.

Algorithm 7: New point quintupling of the form $5P = 3P + 2P$ for general binary curve using LD coordinate.

Let $P = (X, Y, Z)$ be a point on the curve $y^2 + xy = x^3 + ax^2 + b$ on the LD coordinate system, then the point $2P = (X_2, Y_2, Z_2)$ and $3P = (X_3, Y_3, Z_3)$. The 5P formula is given as:

The point $2P = (X_2, Y_2, Z_2)$ is the doubling for $P = (X_1, Y_1, Z_1)$ where:

$S \leftarrow X_1^2 \quad U \leftarrow S + Y_1 \qquad T \leftarrow X_1Z_1$

$R \leftarrow UT \; Z_2 \leftarrow T^2 \qquad X_2 \leftarrow U^2 + R + aZ_2$

$Y_2 \leftarrow (Z_2 + R)X_2 + S^2Z_2$

The point $3P = (X_3, Y_3, Z_3)$ is tripling for $P = (X_1, Y_1, Z_1)$ where:

$A \leftarrow (Z_2 + E)X_2 + Z_2^2 + U\,B \leftarrow X_2 + X_1X_2$

$C \leftarrow BZ_2\,C \leftarrow BZ_2Z_3 \leftarrow C^2 \qquad D \leftarrow X_1Z_3$

$E \leftarrow UX_1 \qquad X_2 \leftarrow U^2 + E + aZ_2$

$X_3 \leftarrow A^2 + C(A + B^2) + aZ_3$

$Y_2 \leftarrow (X_3 + D)(AC + Z_3) + (Y_1 + X_1)Z_3^2$

Let $Z_3 \rightarrow 0$ then:

$A \leftarrow (Z_2 + E)X_2 + Z_2^2 + U\,B \leftarrow X_2 + X_1X_2$

$C \leftarrow BZ_2\,C \leftarrow BZ_2\,D \leftarrow X_1Z_3$

$E \leftarrow UX_1 \qquad X_2 \leftarrow U^2 + E + aZ_2$

$X_3 \leftarrow A^2 + C(A + B^2) + a$

$Y_2 \leftarrow (X_3 + D)(AC + 1) + (Y_1 + X_1)$

The Point $5P = 3P + 2P$ is equivalent to the form $(X_5, Y_5, Z_5) = (X_3, Y_3, 1) + (X_2, Y_2, Z_2)$ using mixed addition:

$G \leftarrow Y_2 + Y_3Z_2^2 \quad H \leftarrow X_2 + X_3Z_2$

$K \leftarrow HZ_2 \qquad Z_5 \leftarrow K^2 \qquad M \leftarrow X_3Z_5$

$X_5 \leftarrow G^2 + K(G + H^2) + aK$

$Y_5 \leftarrow (M + X_5)(GK + Z_5) + (Y_1 + X_1)Z_5^2$

By counting the number of multiplication and squaring, the total cost of the formula 5P is $23M + 13S$. This new point will be proven as valid using the approach [13] and [18] provided in Lemma 1.

Lemma 1: The proposed point 5P of form $5P = 3P + 2P$ is valid.

Proof:

Affine coordinate is used to prove the formula. Adding two points in affine coordinate $(X_5, Y_5, Z_5) = (X_3, Y_3, Z_3) + (X_2, Y_2, Z_2)$ should satisfy the equations:

$$\lambda = {(y_3 + y_2)}\Big/{(x_3 + x_2)}$$

$$x_5 = \lambda^2 + \lambda + x_3 + x_2 + a$$

$$y_5 = \lambda(x_3 + x_5) + x_5 + y_3$$

Using Algorithm 7, it needs to be proven that $\frac{X_5}{Z_5} = x_5$ and $\frac{Y_5}{Z_5^2} = y_5$, the process is:

$$\frac{X_5}{Z_5} = \frac{G^2 + K(G + H^2) + aZ_5}{K^2} = \frac{G^2}{K^2} + \frac{G}{K} + \frac{H^2}{K} + a$$

$$= \frac{[\,Y_2 + Y_3Z_2^2]^2}{(X_2 + X_3Z_2)^2\,Z_2^2} + \frac{Y_2 + Y_3Z_2^2}{(X_2 + X_3Z_2)Z_2} + \frac{(X_2 + X_3Z_2)^2}{(X_2 + X_3Z_2)Z_2} + a$$

Let $Z_3 = 1$

$$= \left[\frac{Y_2/Z_2^2 + Y_3}{X_2/Z_2 + X_3}\right]^2 + \left[\frac{Y_2/Z_2^2 + Y_3}{X_2/Z_2 + X_3}\right] + \frac{X_2}{Z_2} + X_3 + a$$

$$= \left[\frac{y_3 + y_2}{x_3 + x_2}\right]^2 + \frac{y_3 + y_2}{x_3 + x_2} + x_2 + x_3 + a$$

$x_5 = \lambda^2 + \lambda + x_3 + x_2 + a$

$\frac{Y_5}{Z_5^2} = \frac{(M+X_5)(GK+Z_5)+(Y_1+X_1)Z_5^2}{K^4}$

$$= \frac{GK(X_3Z_5 + X_5) + Z_5\,(Y_3Z_5 + X_5)}{K^4}$$

$$= \frac{(Y_2 + Y_3Z_2^2)(X_3Z_5 + X_5)}{K^3} + \frac{X_5}{K^2} + Y_3$$

$$= \frac{(Y_2/Z_2^2 + Y_3)(X_3 + X_5/Z_5)}{(X_2/Z_2 + X_3)} + \frac{X_5}{Z_5} + Y_3$$

$$= \left(\frac{Y_2/Z_2^2 + Y_3}{X_2/Z_2 + X_3}\right)\left(X_3 + X_5/Z_5\right) + \frac{X_5}{Z_5} + Y_3$$

$= \left(\frac{y_3 + y_2}{x_3 + x_2}\right)(x_3 + x_5) + x_5 + y_3$

$y_5 = \lambda(x_3 + x_5) + x_5 + y_3$ (Proven)

While the second quintupling formula will use the form of $5P = 2(2P) + P$, which requires three algebraic operations, i.e. two doubling and one addition, the new formula is as presented in Algorithm 8.

Algorithm 8: New Point Quintupling of the Form $5P = 2(2P) + P$ for General Binary Curve Using LD Coordinate.

Let $P = (X, Y, Z)$ be a point on the curve $y^2 + xy = x^3 + ax^2 + b$ on the LD coordinate system, then the point $2P = (X_2, Y_2, Z_2)$ and $4P = (X_4, Y_4, Z_4)$. The 5P formula is given as:

The point $2P = (X_2, Y_2, Z_2)$ is doubling for $P = (X_1, Y_1, Z_1)$ where:

$S \leftarrow X_1^2$ $U \leftarrow S + Y_1$ $T \leftarrow X_1Z_1$

$R \leftarrow UT$ $Z_2 \leftarrow T^2$ $X_2 \leftarrow U^2 + R + aZ_2$

$Y_2 \leftarrow (Z_2 + R)X_2 + S^2Z_2$

The point $4P = (X_4, Y_4, Z_4)$ is doubling for $2P = (X_2, Y_2, Z_2)$ where:

$S_1 \leftarrow X_2^2$ $U_1 \leftarrow S_1 + Y_2$ $T_1 \leftarrow X_2Z_2$

$R_1 \leftarrow U_1T_1$ $Z_4 \leftarrow T_1^2$ $X_4 \leftarrow U_1^2 + R_1 + aZ_4$

$Y_4 \leftarrow (Z_4 + R_1)X_4 + S_1^2Z_4$

Let $Z_3 \rightarrow 0$, then:

$S_1 \leftarrow X_1^2$ $U_1 \leftarrow S_1 + Y_2$ $T_1 \leftarrow X_2Z_2$

$R_1 \leftarrow U_1T_1$ $T_1^2 \leftarrow 1$ (Neglected)

$X_4 \leftarrow U_1^2 + R_1 + a$

$Y_4 \leftarrow (1 + R_1)X_4 + S_1^2$

The Point $5P = 2(2P) + P$ is equivalent to the form $(X_5, Y_5, Z_5) = (X_4, Y_4, 1) + (X_1, Y_1, Z_1)$ using mixed addition:

$A \leftarrow Y_1 + Y_4Z_1^2$ $B \leftarrow X_1 + X_4Z_1$

$C \leftarrow BZ_1$ $Z_5 \leftarrow C^2$ $D \leftarrow X_4Z_5$

$X_5 \leftarrow A^2 + C(A + B^2) + aC$

$Y_5 \leftarrow (D + X_5)(CA + Z_5) + (Y_4 + X_4)Z_5^2$

By counting the number of multiplication and squaring in the previous formula, the total cost of the formula 5P is $17M + 12S$. As in the previous formula, the new point will be proven as valid as in Lemma 2.

Lemma 2: The proposed point 5P of form $5P = 2(2P) + P$ is valid.

Proof: Affine coordinate is used to prove the formula. Adding two points in affine coordinate $(X_5, Y_5, Z_5) = (X_4, Y_4, Z_4) + (X_1, Y_1, Z_1)$ should satisfy the equations:

$\lambda = {(y_4 + y_1)}/{(x_4 + x_{41})}$

$x_5 = \lambda^2 + \lambda + x_4 + x_1 + a$

$y_5 = \lambda(x_4 + x_5) + x_5 + y_4$

Using Algorithm 8, it needs to be proven that $\frac{X_5}{Z_5} = x_5$ and $\frac{Y_5}{Z_5^2} = y_5$, the process is:

$\frac{X_5}{Z_5} = \frac{A^2 + C(A+B^2) + aC}{C^2} = \frac{A^2}{C^2} + \frac{A}{C} + \frac{B^2}{C} + a$

$$= \frac{[\,Y_1 + Y_4Z_1^2]^2}{(X_1 + X_4Z_1)^2\,Z_1^2} + \frac{Y_1 + Y_4Z_1^2}{(X_1 + X_4Z_1)Z_1} + \frac{(X_1 + X_4Z_1)^2}{(X_1 + X_4Z_1)Z_1} + a$$

Let $Z_4 = 1$

$$= \left[\frac{Y_1/Z_1^2 + Y_4}{X_1/Z_1 + X_4}\right]^2 + \left[\frac{Y_1/Z_1^2 + Y_4}{X_1/Z_1 + X_4}\right] + \frac{X_1}{Z_1} + X_4 + a$$

$$= \left[\frac{y_4 + y_1}{x_4 + x_1}\right]^2 + \left[\frac{y_4 + y_1}{x_4 + x_1}\right] + x_1 + x_4 + a$$

$$x_5 = \lambda^2 + \lambda + x_4 + x_1 + a$$

$$\frac{Y_5}{Z_5^2} = \frac{(D+X_5)(CA+Z_5)+(Y_4+X_4)Z_5^2}{C^4}$$

$$= \frac{CA(X_4Z_5 + X_5) + Z_5(Y_4Z_5 + X_5)}{C^4}$$

$$= \frac{(Y_1 + Y_4Z_1^2)(X_4Z_5 + X_5)}{C^3} + \frac{X_5}{C^2} + Y_4$$

$$= \frac{({}^{Y_{12}}/_{Z_1^2} + Y_4)(X_4 + {}^{X_5}/_{Z_5})}{({}^{X_1}/_{Z_1} + X_4)} + \frac{X_5}{Z_5} + Y_4$$

$$= \left(\frac{{}^{Y_1}/_{Z_1^2} + Y_4}{{}^{X_1}/_{Z_1} + X_4}\right)\left(X_4 + {}^{X_5}/_{Z_5}\right) + \frac{X_5}{Z_5} + Y_4$$

$$= \left(\frac{y_4 + y_1}{x_4 + x_1}\right)(x_4 + x_5) + x_5 + y_4$$

$y_5 = \lambda(x_4 + x_5) + x_5 + y_4$ (Proven)

The cost of the first formula where $5P = 3P + 2P$ is$23M + 13S$, while for the form $5P = 2(2)P + P$, the cost is$17M + 12$. The first formula has a high cost, since it uses four operations, for tripling we should doubling for the point then adding it to the point, i.e. $3P = 2P + P$then doubling the point P and finally adding them together, or $5P = 2P + P + 2P$, which means two doubling and two addition. While for the formula $5P = 2(2)P + P$, we have three operations, which are two doubling and one addition only. So, the preferred formula is $5P = 2(2)P + P$. The new point formula could not be compared to other point quintupling, since it is the first proposed point for the elliptic curve over binary curve using LD coordinates.

IV. Conclusion and Future works

Two new quintupling points are introduced over general binary curve using Lŏpez-Dahab coordinate. Two formulas where used, $5P = 3P + 2P$ (Tripling adding to doubling) and $5P = 2(2)P + P$ (Doubling of doubling adding to point). The cost of the two formulas are $23M + 13S$ and $17M + 12S$ respectively. Therefore, the preferred formula is $5P = 2(2)P + P$ with lowest cost. Using mathematical proofing, these two points are proved as valid. This point can be implemented at scalar multiplication level using different scalar method. For example, for w-NAF method where $w \geq 4$, or with the precomputed quintupling point will save the time and memory at scalar multiplication level in ECC.

This point can be improved using different techniques and coordinate. A higher point also can be implemented such as point septupling 7P and nonupling 9P.

Acknowledgement

This work was supported by the Ministry of Higher Education under FRGS Grant no. 5524822.

References

[1] M. M. Ahmad, S. M. Yasin, R. Mahmod, and M. A. Mohamed, “X-Tract Recoding Algorithm for Minimal Hamming Weight Digit Set Conversion,” J. Theor. Appl. Inf. Technol., vol. 75, no. 1, pp. 109–114, 2015.

[2] Z. U. A. Khan and M. Benaissa, “High Speed and Low Latency ECC Processor Implementation over GF (2 m) on FPGA,” IEEE Trans. Very Large Scale Integr. Syst., vol. 25, no. 1, p. 165–176., 2017.

[3] W. K. A. . Abdulrahem, H. H. O. Nasereddin, and S. M. H. Fares, “Business Continuity Based on RFID,” Am. Acad. Sch. Res. J., vol. 5, no. 3, pp. 223–228, 2013.

[4] N. P. Owoh and M. M. Singh, “Applying Diffie-Hellman Algorithm to Solve the Key Agreement Problem in Mobile Blockchain-based Sensing Applications,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 3, pp. 59–68, 2019.

[5] M. Bafandehkar, S. M. Yasin, and R. Mahmod, “Optimizing (0, 1, 3)-NAF recoding algorithm using block- Method technique in elliptic curve cryptosystem,” J. Comput. Sci., vol. 12, no. 11, pp. 534–544, 2016.

[6] T. Oliveira, J. López, D. F. Aranha, and F. Rodríguez-Henríquez, “Two is the fastest prime: Lambda coordinates for binary elliptic curves,” J. Cryptogr. Eng., vol. 4, no. 1, pp. 3–17, 2014.

[7] P. Mishra and V. Dimitrov, “Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication using Multibase Number Representation,” Cryptol. ePrint Arch. Rep., vol. 040, pp. 1–16, 2007.

[8] P. Giorgi, L. Imbert, and T. Izard, “Optimizing elliptic curve scalar multiplication for small scalars,” Math. Signal Inf. Process., vol. 7444, p. 74440N, 2009.

[9] P. Longa and A. Miri, “New Multibase Non-Adjacent Form Scalar Multiplication and its Application to Elliptic Curve Cryptosystems (extended version).,” IACR Cryptol. ePrint Arch., vol. 1, no. 1, p. 52, 2016.

[10] S. R. S. Rao, “Three Dimensional Montgomery Ladder, Differential Point Tripling on Montgomery Curves and Point Quintupling on Weierstrass’ and Edwards Curves,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, vol. 9646, pp. 84–106.

[11] C. P. Bernstein, D. J., Birkner, P., Lange, T., & Peters, “Optimizing double-base elliptic-curve single-scalar multiplication,” in International Conference on Cryptology in India, 2007, vol. 4859, no. 2007, pp. 384–392.

[12] S. Al Musa and G. Xu, “Fast Scalar Multiplication for Elliptic Curves over Binary Fields by Efficiently Computable Formulas,” in International Conference in Cryptology in India, Springer, Cham, 2017, pp. 206–226.

[13] E. Al-Daoud, R. Mahmod, M. Rushdan, and A. Kilicman, “A new addition formula for elliptic curves over GF(2n),” IEEE Trans. Comput., vol. 51, no. 8, pp. 972–975, 2002.

[14] H. Cohen, G. Frey, and R. Avanzi, Handbook of Elliptic and Hyperelliptic Curve Cryptography. 2006.

[15] R. López, J., & Dahab, “Improved Algorithms for Elliptic Curve Arithmetic in GF (2 n),” Springer-Verlag Berlin Heidelb., vol. 97, no. 107, pp. 201–212, 1999.

[16] A. Higuchi and N. Takagi, “Fast addition algorithm for elliptic curve arithmetic in GF(2n) using projective coordinates,” Inf. Process. Lett., vol. 76, no. 3, pp. 101–103, 2000.

[17] T. Lange, “A note on L´opez-Dahab coordinates,” https://eprint.iacr.org/2004/323.pdf, vol. 24, pp. 1–7, 2004.

[18] S. Yasin and Z. Muda, “Tripling formulae of elliptic curve over binary field in Lopez-Dahab model,” J. Theor. Appl. Inf. Technol., vol. 75, no. 2, pp. 212–216, 2015.

[19] B. A. Forouzan, Cryptography and Network Security. McGraw-Hill, Inc. New York, NY, USA, 2007.