International Journal of Cryptology Research 10(1): 22 - 36 (2020)

Improvement of Scalar Multiplication on Elliptic Curve with j-invariant 0

Siti Noor Farwina Mohamad Anwar Antony[*1] and **Hailiza Kamarulhaili**[1]

[1]*School of Mathematical Sciences, Universiti Sains Malaysia,11800 Penang, Malaysia*

E-mail: farwina@usm.my
[*]*Corresponding author*

ABSTRACT

Scalar multiplication plays a vast role in elliptic curve cryptography (ECC). It consumes numerous operation cost, especially when dealing with a large prime field. Many methods were proposed to reduce the cost of computing scalar multiplication in an elliptic curve. One of the introduced methods is the Integer Sub-Decomposition (ISD) method which applies bilayer decomposition on the scalar multiplication. In this paper, we derive the efficiently computable endomorphisms (or fast endomorphism) based on the concept of isomorphism and isogeny by using Velu's formulae. These fast endomorphisms are applied in the ISD method to accelerate the scalar multiplication on elliptic curves with j-invariant 0. Also, we further discuss the number of operations of the derived fast endomorphisms and compare the number of operations between original ISD method and the improved ISD method.

Keywords: Elliptic curve, efficient endomorphism, scalar multiplication, ISD method, j-invariant 0.

1 INTRODUCTION

Elliptic Curve Cryptography (ECC) is one of the cryptographic protocol in Public Key Cryptography (PKC), other than Diffie-Hellman (DH) and Rivest-Shamir-Adleman (RSA) cryptosystem Galbraith (2012). The use of elliptic curve in cryptography was first discovered by Miller and Koblitz Gallant et al. (2001). Cryptography is a platform that provides secure communication between two parties to pass information in public networks. It provides authentication of one party to another from being traced by eavesdroppers Galbraith (2012).

An ordinary elliptic curve E is defined by

$$E : y^2 = x^3 + Ax + B$$

where A, B are scalars defined in a field K (Silverman, 2009). ECC always considered K as a finite field F_p. The order of an elliptic curve defined over F_p is denoted as $\#E(F_p) = nh$ with prime number n and cofactor h. Note that, $h \leq 4$ for cryptographic purposes. The set of points in E form an abelian group with a single prime subgroup. One important properties of an elliptic curve is the discriminant, Δ defined by the constant $\Delta = -16(4A^3 + 27B^2)$. Δ is used to determine the smoothness of an elliptic curve. Another important properties of an elliptic curve is the j-invariant, which is defined by $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$. The j-invariant of an elliptic curve can be used to distinguish the family of curves as any two elliptic curves with the same j-invariant are belong to the same family of curves and they are said to be isomorphic to each other. One of the types of family of curves is the elliptic curve with j-invariant 0, E_0.

Having same security level with a shorter key attract attention to ECC as compared with other cryptosystems such as RSA (Salah and Said, 2014). A 160-bit ECC have equivalent level of security as 2048-bit RSA (Bafandehkar et al., 2013, Kwon et al., 2018). The security of ECC is based on the hardness to solve the discrete logarithm problem, where one needs to find scalar k such that

$$Q = kP$$

where Q is the public key, P is the parameter that has been agreed by both

parties and k is the secret key. In ECC, the parameter P and Q are referring to points on an elliptic curve which belongs to the prime subgroup of order n, while k is the private key such that $k \in [1, n]$.

There are two methods to compute kP. The first method is by encoding k into a few forms such as binary form. From the binary form of k, we can identify the number of point additions and point doublings needed to compute kP, where each point addition $P + S$ such that $S \neq P$ costs $2M + 1S + 1I$ while each point doubling $2P$ costs $2M + 2S + 1I$ such that M, S, I denote multiplication, squaring and inversion operation, respectively. However, as k getting larger, the operation cost of kP will be numerous. This will later affect the efficiency of ECC. Therefore, many researchers are trying to reduce the computational cost by proposing new approaches and algorithms.

The second method is by using endomorphism. One of the approaches that has been proposed is the Gallant-Lambert-Vanstone (GLV) method where it decomposes scalar k into two shorter scalars k_1, k_2 with the help of efficient endomorphisms (or also known as fast endomorphisms) such that $max\{\mid k_1 \mid, \mid k_2 \mid\} \leq \sqrt{n}$ (Gallant et al., 2001). This method able to reduce the cost of scalar multiplication by 50% as long as they able to decompose k and satisfy the GLV condition $max\{\mid k_1 \mid, \mid k_2 \mid\} \leq \sqrt{n}$. In 2010, Zhou et. al (Zhou et al., 2010) came up with three-dimensional GLV method on elliptic curves with j-invariant 0, E_0. However, if the GLV condition is not satisfied, the cost of computing scalar multiplication by using the GLV method will be numerous. Therefore, in 2013, Ajeena and Kamarulhaili proposed the Integer Sub-Decomposition (ISD) method which applies a bilayer decomposition on the scalar multiplication with the help of another two endomorphisms (Ajeena and Kamarulhaili, 2014). In spite of using fast endomorphism, the original ISD method used endomorphism $\Phi = \lambda$ where λ is chosen randomly from $[1, n-1]$. As a result, the computational cost will remain to be high if one chooses a bigger λ as the cost of computing λP will be big as well.

Our Contribution. This paper derived the fast endomorphism defined in elliptic curve with j-invariant 0, E_0 by studying the algebraic structure of an elliptic curve. Previously, in Antony and Kamarulhaili (2018), we used different approach to derive the fast endomorphisms in E_0. This paper proposed the endomorphism Φ to be defined as $\Phi = \psi\phi$ where ψ is the isomorphism

mapping and ϕ is the isogeny mapping defined on an elliptic curve. We first identify the set of torsion points existed in E_0 which later being used in the Velu's algorithm to construct the isogeny of E_0. However, not all isogeny represents the computable endomorphism. The derived fast endomorphism can be used in both GLV and ISD method to speed up their computation. We also compute the operation counts for each of the derived fast endomorphism. Next, we apply the derived fast endomorphisms into the ISD method and do the comparison with and without using fast endomorphism to compute scalar multiplication.

Outline of This Paper. This paper divided into five sections, starting with a brief introduction on elliptic curve cryptography and previous works on elliptic scalar multiplication methods in Section 1. Section 2 listing out a few theorems related to this work. Next, we briefly explain on the elliptic curve with j-invariant 0, E_0 in Section 3. Section 4 derives the fast endomorphism in E_0 and its respective operation counts. Finally, Section 5 concludes the paper.

2 PRELIMINARIES

We adopted a few concepts related to this study as follows:

Theorem 2.1. *(Hankerson et al., 2004) Define elliptic curves over a field K as $E(K) : y^2 = x^3 + Ax + B$ and $\bar{E}(K) : y'^2 = x'^3 + A'x' + B'$. E and $\bar{E}$ are said to be isomorphic over $\bar{K}$, the algebraic closure of K, if every isomorphism ψ satisfy the restricted form of change of variables*

$$x = u^2x' \quad and \quad y = u^3y',$$

for some $u \in \bar{K}*$ where $\bar{K}*$ is the multiplicative group of $\bar{K}$.

Definition 2.1. *(Ribenboim, 2001) An algebraic integer is a complex number which is a root of a monic polynomial $X^2 + rX + s = 0$ where $r, s \in \mathbb{Z}$.*

An endomorphism Φ is a homomorphism that maps E to itself. An endomorphism acted on point $P = (x, y)$ can be defined by rational function

$$\Phi(x, y) = (f_1(x, y), f_2(x, y)) = (x', y')$$

where $Q = (x', y')$ and $P, Q \in E$. Every endomorphism satisfy a quadratic polynomial with integer coefficient. The polynomial of algebraic integer can be used to represent the endomorphism's polynomial. The endomorphism's polynomial can also be defined as $\Phi^2 - t_\Phi \Phi + n_\Phi = 0$ where $t_\Phi = \Phi + \hat{\Phi}$ and $n_\Phi = \Phi \cdot \hat{\Phi}$ are the trace and norm of the endomorphism, respectively. An isogeny ϕ is a homomorphism that maps E to $\tilde{E}$ such that $\phi(\mathcal{O}_E) = \mathcal{O}_{\tilde{E}}$. The isogeny $\phi : E \to \tilde{E}$ can be computed using Velu's formulae Washington (2007). Velu's formulae construct the mapping for the isogeny based on the torsion points exist in the elliptic curve. The isogeny's mapping from E to $\tilde{E}$ can be used to represent the endomorphism's mapping from E and E if it is able to preserve the structure of the elliptic curve by having the same j-invariant of E and $\tilde{E}$.

3 ELLIPTIC CURVES WITH J-INVARIANT 0

Elliptic curve with j-invariant 0 is curve in the form of

$$E_0 : y^2 = x^3 + B.$$

According to (Cohen, 1996), E_0 has discriminant of quadratic field $D = -3$ where $K = \mathbb{Q}(\sqrt{-3})$. The largest subring of K or also known as the maximal order is given by $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. The integral basis of $K = \mathbb{Q}(\sqrt{-3})$ are $\{1, \delta\}$ where $\delta = \frac{1+\sqrt{-3}}{2}$. The first endomorphism ring in E_0 is chosen to be isomorphic to its maximal order. The following proposition defines the first endomorphism in E_0.

Proposition 3.1. *(Antony and Kamarulhaili, 2018) Let $E_0 : y^2 = x^3 + B$ be an elliptic curve where $B \in F_p$ and $p \equiv 1$ (mod 3). There exists a point $P \in E_0(F_p)$ with order n (prime), then the endomorphism Φ satisfies $\Phi(P)^2 + \Phi(P) + P \equiv \mathcal{O}_{E_0}$ (mod n) where*

$$\begin{array}{rcccc} \Phi & : & E_0(F_p) & \to & E_0(F_p) \\ & : & (x, y) & \mapsto & (\gamma x, y) \\ & : & \mathcal{O}_{E_0} & \to & \mathcal{O}_{E_0} \end{array}$$

where $\gamma \in F_p$ *satisfies* $\gamma^2 + \gamma + 1 \equiv 0$ *(mod p).*

Clearly, the first endomorphism represents complex multiplication by $\beta = \frac{-1+\sqrt{-3}}{2}$ on E_0.

4 CONSTRUCTING THE FAST ENDOMORPHISM

Define $E_0 : y^2 = x^3 + B$. Solving E_0, we obtained the set of points of order two and three denoted by $E[2]$ and $E[3]$ where $E[2] = \{(\sqrt{B}, 0), \infty\}$ and $E[3] = \{(0, \sqrt{B}), (0, -\sqrt{B}), \infty\}$. These are the torsion points exist in E_0. As mentioned earlier, these points used to construct the isogeny from E_0 to $\tilde{E}_0$ by using Velu's formulae. Before constructing the isogeny, it is important to highlight that the ISD method needs three endomorphisms to decompose scalar k. Thus, we suggested that the second and third endomorphisms should also belong to the same imaginary quadratic field $K = \mathbb{Q}(\sqrt{-3})$ as shown in Figure 1.

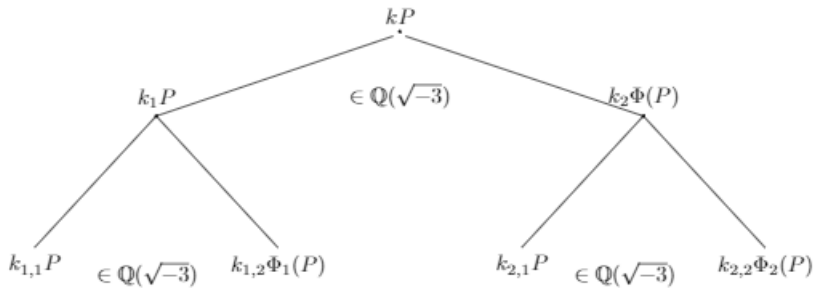

Figure 1: ISD decomposition for $K = \mathbb{Q}(\sqrt{-3})$.

From the figure above, the second layer of decomposition are choose to be defined over the same imaginary quadratic field as the curve itself, which is $K = \mathbb{Q}(\sqrt{-3})$. Since the ring for the first endomorphism is isomorphic to maximal order $\mathcal{O}_K$ and we want the second and third endomorphisms' ring belong to the same imaginary quadratic field, then the rings formed by the second and third endomorphisms should be the subrings of $\mathcal{O}_K$.

The following lemma describes the construction of the other two non-maximal orders which belong to the same complex quadratic field.

Lemma 4.1. *Define* $E_0 : y^2 = x^3 + B$. *Let* $kP = k_1P + k_2\Phi(P)$ *defined over a field* $K = \mathbb{Q}\left(\sqrt{-3}\right)$ *with a maximal order,* $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. *Then, there exists two other non-maximal orders in* $K = \mathbb{Q}\left(\sqrt{-3}\right)$ *which are given by* $\mathbb{Z}\left[\sqrt{-3}\right]$ *and* $\mathbb{Z}\left[\frac{3+\sqrt{-3}}{2}\right]$.

Proof. The largest subring for $K = \mathbb{Q}\left(\sqrt{-3}\right)$ is given by $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\delta]$ with the integral basis for $\mathcal{O}_K$ as $\{1, \delta\}$. Any algebraic integer in $\mathcal{O}_K$ can be written as the linear combination of its basis in the form of $Z = a(1) + b\left(\frac{1+\sqrt{-3}}{2}\right)$ where $a, b \in \mathbb{Z}$. By choosing $a = -1, b = 2$ and $a = 1, b = 1$, there exist algebraic integers $Z_{\Phi_1} = \sqrt{-3}$ and $Z_{\Phi_2} = \frac{3+\sqrt{-3}}{2}$ in $\mathcal{O}_K$. Let the integral basis for the first non-maximal order to be $\{1, Z_{\Phi_1}\}$. Any algebraic integer formed by the linear combination of this basis are belong to $\mathbb{Z}[Z_{\Phi_1}] = \mathbb{Z}\left[\sqrt{-3}\right]$. Similarly, by letting the integral basis for the second non-maximal order as $\{1, Z_{\Phi_2}\}$, any algebraic integer form by the linear combination of this basis are belong to $\mathbb{Z}[Z_{\Phi_2}] = \mathbb{Z}\left[\frac{3+\sqrt{-3}}{2}\right]$. These rings are the subrings of the maximal order, thus they are the non-maximal order of $\mathbb{Q}\left(\sqrt{-3}\right)$. □

Z_{Φ_1} and Z_{Φ_2} later become the generator for the subrings $\mathbb{Z}\left[\sqrt{-3}\right]$ and $\mathbb{Z}\left[\frac{3+\sqrt{-3}}{2}\right]$ which are isomorphic to the second and third endomorphisms' ring. The algebraic integers are chosen to be $Z_{\Phi_1} = \sqrt{-3}$ and $Z_{\Phi_2} = \frac{3+2\sqrt{-3}}{2}$ as it is the lowest form of linear combination with the smallest norm that can be obtained from the integral basis of the largest subring in $\mathbb{Q}\left(\sqrt{-3}\right)$. Follow Definition 2.1, Z_{Φ_1} and Z_{Φ_2} should satisfy a polynomial of degree two respectively. The characteristic polynomial for the second and third endomorphisms are given in the following lemma.

Lemma 4.2. *Let* $E_0 : y^2 = x^3 + B$ *be an elliptic curve over* F_p. *Given the non-maximal order for the second and third endomorphisms as* $\mathbb{Z}\left[\sqrt{-3}\right]$ *and* $\mathbb{Z}\left[\frac{3+\sqrt{-3}}{2}\right]$, *respectively. Then, the characteristic polynomial for the endomorphisms are given as* $\Phi_1^2 + 3 = 0$ *and* $\Phi_2^2 - 3\Phi_2 + 3 = 0$.

Proof. Let $Z_{\Phi_1} = \sqrt{-3}$ be root of a monic polynomial, where its conjugate $\hat{Z}_{\Phi_1} = -\sqrt{-3}$. Then we have the trace and norm of endomorphism as $t_\Phi = Z_{\Phi_1} + \hat{Z}_{\Phi_1} = 0$ and $n_\Phi = Z_{\Phi_1} + \hat{Z}_{\Phi_1} = 3$. Since Z_{Φ_1} is an algebraic integer, by Definition 2.1 it satisfy characteristic polynomial $\Phi_1^2 + 3 = 0$. Similarly, for $Z_{\Phi_2} = \frac{3+\sqrt{-3}}{2}$, where it should satisfy the characteristic polynomial $\Phi_2^2 - t_{\Phi_2}\Phi + n_{\Phi_2} = \Phi_2^2 - \left(Z_{\Phi_2} + \hat{Z}_{\Phi_2}\right)\Phi + \left(Z_{\Phi_2} \cdot \hat{Z}_{\Phi_2}\right) = \Phi_2^2 - 3\Phi_2 + 3 = 0$ such that $\hat{Z}_{\Phi_2} = \frac{3+\sqrt{-3}}{2}$. □

In this paper, we adopted the concept of isogeny ϕ and isomorphism ψ to derive our fast endomorphism where $\Phi = \psi\phi$. As mentioned in preliminaries section, $\phi : E_0 \to \tilde{E}_0$ and $\psi : \tilde{E}_0 \to E_0$ where

$$\begin{array}{ccccc} E_0 & \xrightarrow{\phi} & \tilde{E}_0 & \xrightarrow{\psi} & E_0 \\ (x,y) & \xrightarrow{\phi} & (X,Y) & \xrightarrow{\psi} & (x',y'). \end{array}$$

The following theorem derives the second and third endomorphisms' mapping in $E_0 : y^2 = x^3 + B$ by using a point which belong to the kernel of $E[3]$.

Theorem 4.1. *Define $E_0 : y^2 = x^3 + B$ over F_p where $p \equiv 1$ (mod 3). There exists a point $Q \in E[3]$ and point $P \in E_0(F_p)$ with prime order n. Given the polynomial for the second and third endomorphisms as $\Phi_1^2 + 3 = 0$ and $\Phi_2^2 - 3\Phi_2 + 3 = 0$, respectively. Then, the second and third endomorphisms's mappings are defined by*

$$\Phi_{1,2}(x,y) = \left(\frac{x^3 + 4B}{\epsilon_{1,2}^2 x^2}, y\frac{x^3 - 8B}{\epsilon_{1,2}^3 x^3}\right)$$

where $\Phi_1 \equiv \epsilon_1$ (mod p) and $\Phi_2 \equiv \epsilon_2$ (mod p).

Proof. Choose a torsion point with order three, Q where $E[3] = \left\{(0,\sqrt{B}), (0,-\sqrt{B}), \mathcal{O}_{E_0}\right\}$. Let $Q = \left(0,\sqrt{B}\right)$ and $P = (x,y)$

where $P \notin Ker\left(E\left[3\right]\right)$. Following Velu's formulae, we have

$$\begin{aligned} F\left(x,y\right) &= x^3 + B - y^2 = 0 \\ F_x &= 3x^2 \\ F_y &= -2y \\ u_Q &= \left(F_y\left(Q\right)\right)^2 = 4B \\ v_Q &= 2F_x\left(Q\right) - a_1F_y\left(Q\right) = 0. \end{aligned}$$

The isogeny is defined by $\phi : (x, y) \to (X, Y)$ where

$$X = x + \frac{v_Q}{x - x_Q} + \frac{u_Q}{\left(x - x_Q\right)^2} = \frac{x^3 + 4B}{x^2}$$

and

$$\begin{aligned} Y &= y - u_Q\frac{2y + a_1x + a_3}{\left(x - x_Q\right)^3} - v_Q\frac{a_1\left(x - x_Q\right) + y - y_Q}{\left(x - x_Q\right)^2} \\ &- \frac{a_1u_Q - F_x\left(Q\right)F_y\left(Q\right)}{\left(x - x_Q\right)^2} \\ &= y\left[\frac{x^3 - 8B}{x^3}\right]. \end{aligned}$$

The separable isogeny $\phi : (x, y) \to (X, Y)$ from E to $\tilde{E}$ where

$$\tilde{E} : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

and $A_1 = a_1 = 0$, $A_2 = a_2 = 0$, $A_3 = a_3 = 0$, $A_4 = a_4 - 5v = 0$, $A_6 = a_6 - \left(a_1^2 + 4a_2\right)v - 7w = B - 7(4B) = -27B$. This implies $\tilde{E}_0 : y^2 = x^3 - 27B$ and $\phi(x, y) = \left(\frac{x^3+4B}{x^2}, y\frac{x^3-8B}{x^3}\right)$ as the isogeny $\phi : E_0 \to \tilde{E}_0$. Since $j(E_0) = j(\tilde{E}_0)$, then $E_0 \cong \tilde{E}_0$. According to Theorem 2.1 , $\tilde{E}_0$ satisfies $X = u^2x'$ and $Y = u^3y'$ where $u \in \bar{K}^*$ and $(x', y') \in E_0$. Then, we have

$$\begin{array}{ccccc} E_0 & \xrightarrow{\phi} & \tilde{E}_0 & \xrightarrow{\psi} & E_0 \\ (x,y) & \xrightarrow{\phi} & (X,Y) & \xrightarrow{\psi} & (x',y') \end{array}$$

where $\phi : E_0 \to \tilde{E}_0$ is the isogeny map and $\psi : \tilde{E}_0 \to E_0$ is the isomorphism map. By definition of an endomorphism, an endomorphism Φ is a homormorphism which maps E_0 to E_0. Since $(x', y') \in E_0$, then we have

$$\begin{array}{rccc} \Phi\colon & E_0 & \longrightarrow & E_0 \\ & (x,y) & \longrightarrow & (x',y') \end{array}$$

such that $x' = \frac{X}{u^2}$ and $y' = \frac{Y}{u^3}$. Let u denotes the roots for the polynomial of endomorphisms modulo p implies $\Phi_{1,2}(x,y) = (\frac{X}{\epsilon^2}, \frac{Y}{\epsilon^3})$ where

$$\Phi_{1,2}\,(x,y) = \left(\frac{x^3 + 4B}{\epsilon_{1,2}^2 x^2}, y \frac{x^3 - 8B}{\epsilon_{1,2}^3 x^3} \right)$$

such that $\Phi_1 \equiv \epsilon_1 \pmod{p}$ and $\Phi_2 \equiv \epsilon_2 \pmod{p}$. □

To ensure that our fast endomorphism able to accelerate the scalar multiplication, we compute the number of operations needed for each of the endomorphisms. Next proposition describes the operation counts of the fast endomorphisms that has been defined earlier in this paper. Example 3.1 illustrates the improvement of the ISD method by using fast endomorphism.

Proposition 4.1. *Let $E_0 : y^2 = x^3 + B$ defined over a prime field, F_p. Let P be a point in $E_0(F_p)$ with prime order n. Given the first endomorphism's mapping as $\lambda(x,y) = (\gamma x, y)$. And the second and third endomorphisms' mapping are given as*

$$\lambda_{1,2}(x,y) = \left(\frac{x^3 + 4B}{\epsilon_{1,2}^2 x^2}, y \left[\frac{x^3 - 8B}{\epsilon_{1,2}^3 x^3} \right] \right)$$

where $\lambda_{1,2}, \gamma$ and ϵ are the roots of the polynomial of the endomorphism congruent to n and p, respectively. Note that, $\lambda_{1,2}, \epsilon_{1,2} \not\equiv \frac{1+\sqrt{-3}}{2} \pmod{n}$ and $\lambda_{1,2}, \epsilon_{1,2} \not\equiv \frac{1+\sqrt{-3}}{2} \pmod{p}$. Then, the number of operations needed to compute λP is $1M$ while the number of operations needed to compute $\lambda_{1,2} P$ is $4M + 1S + 2I$ where M, S, I denote multiplication, squaring and inversion, respectively.

Proof. The number of operations for the scalars correspond to each fast endomorphism is calculated in the following table:

The first endomorphism needs $1M$ to compute λP while the second and third endomorphisms need $4M+1S+2I$ where M, S, I denote multiplication, squaring and inversion, respectively. □

Operation \Endomorphism	First	Second	Third
Multiplication	1	4	4
Squaring	0	1	1
Inversion	0	2	2
Total	1M	4M+1S+2I	4M+1S+2I

Table 1: Number of Operations for Scalars correspond to each Fast Endomorphisms.

Example 4.1. *Let* $E_0 : y^2 = x^3 + 3$ *be a curve defined over* F_{463} *where* $p = 463 \equiv 1$ *(mod* 3*). There exists a point* $P = (201, 120)$ *in* E_0 *with order* $n = 487$ *(a prime number). The first endomorphism given as* $\Phi^2 + \Phi + 1 = 0$ *which corresponds to* $232P$ *and* $254P$*. While the second and third endomorphisms correspond to* $22P, 465P$ *and* $234P, 256P$*, respectively. The following table compares the cost of computing in term of their operation counts for each scalar multiplications obtained from the endomorphisms using the repeated additions and doublings via binary form approach and the fast endomorphisms' mapping where* mP *denotes values obtained from these three endomorphisms on* E_0*.*

mP \Approaches	Repeated additions and doublings	Fast endomorphism
$232P$	$20M + 17S + 10I$	$1M$
$254P$	$26M + 20S + 13I$	$1M$
$22P$	$12M + 10S + 6I$	$4M + 1S + 2I$
$465P$	$24M + 20S + 12I$	$4M + 1S + 2I$
$234P$	$22M + 18S + 11I$	$4M + 1S + 2I$
$256P$	$14M + 14S + 7I$	$4M + 1S + 2I$

Table 2: Comparison of Operation Counts between Repeated Additions and Doublings and Fast Endomorphisms' Mapping.

Choose scalar $k = 365$ *and we want to compute* $365P$*, where* $k = (101101101)_2$*. The cost of computing* kP *by using repeated addition and dou-*

bling operations involve 26 multiplications, 21 squarings and 13 inversions. Next table compares the operation counts in the ISD method without and with fast endomorphism.

ISD method	With fast endomorphism	Without fast endomorphism
$-5P + (-11)\Phi_1(P)$	$-8P - 11(465P)$	$-8P - 11(465P)$
$-3P + (-9)\Phi_2(P)$	$-9(256P)$	$-9(256P)$
where		
$k_{1,1} = -5$, $k_{2,1} = -3$	$= (6M + 6S + 3I)$	$= (6M + 6S + 3I)$
$k_{1,2} = -11$,	$+(10M + 8S + 5I)$	$+(10M + 8S + 5I)$
$k_{2,2} = -9$,	$+(8M + 7S + 4I)$	$+(8M + 7S + 4I)$
given		
$\Phi_1(P) = 465P$	$+(4M + 1S + 2I)$	$+(24M + 20S + 12I)$
and		
$\Phi_2(P) = 256P$.	$+(4M + 1S + 2I)$	$+(14M + 14S + 7I)$
Note that:		
there are two addition processes	$+2(2M + 1S + I)$	$+2(2M + 1S + I)$
Total	$36M + 25S + 18I$	$66M + 57S + 33I$

Table 3: Comparison between Number of Operations for ISD Method without and with Fast Endomorphism to compute $365P$.

From Table 3, the number of operations needed to compute $8P$ *where* $8 = (1000)_2$ *is* $3(2M + 2S + I) = 6M + 6S + 3I$. *Meanwhile, the number of operations needed to compute* $11P$ *and* $9P$ *are* $10M + 8S + 5I$ *and* $8M + 7S + 4I$, *respectively. The operation counts for* $465P$ *and* $256P$ *without using endomorphism are taken from Table 2.*

Since the inversion operation consumes highest running time among all three operations causing it to be the most expensive operation, the speed up percentage between the inversion operations in the ISD method using both approaches in Table 3 is computed, where $\frac{33-18}{33} \times 100\% \approx 45\%$. *For this case, it is clear that using fast endomorphisms able to speed up the ISD method by reducing the number of operations needed approximately by* 45%.

5 CONCLUSION

Elliptic curve plays a vast role in modern cryptography; mainly ECC. One of the drawbacks in ECC is the operation cost consumed by the scalar multiplication. The GLV and ISD method are some of the approaches that have been proposed to enhance the computational speed and reduce the computational cost. However, the number of operations needed by the ISD method still need to be reduced. By working on the imaginary quadratic field with $D = -3$, the ISD method can accelerate the scalar multiplication problem in E_0. The largest ring which consists of all algebraic integers in E_0 defined over K is denoted by $\mathcal{O}_K$. To solve scalar multiplication, the ISD method requires three endomorphisms. In this paper, the first endomorphism's ring is chosen to be isomorphic to $\mathcal{O}_K$ corresponds to a unique polynomial, $\Phi^2 + \Phi + 1 = 0$. The cost of computing this endomorphism only involve one multiplication operation. The second and third endomorphisms are chosen to be as $\Phi_1^2 + 3 = 0$ and $\Phi_2^2 - 3\Phi_2 + 3 = 0$, where their endomorphisms' rings are isomorphic to the subrings in $\mathbb{Z}(\sqrt{-3})$. Velu's formulae and isomorphism concept are used to construct the endomorphisms' mapping for the second and third endomorphisms. The Velu's formulae applied on torsion points with order three that exists in E_0. The number of operations needed by the scalars correspond to these endomorphisms is four multiplications, one squaring and two inversions. Even with a larger field, the operation cost will remain unchanged. As a result, the operation cost of computing kP is greatly reduced especially when k is getting larger.

ACKNOWLEDGMENTS

The author would like to thank Universiti Sains Malaysia for the financial support under the Research University Grant Scheme,
account no. 1001/PMATHS/AUPS001.

REFERENCES

Ajeena, R. K. K. and Kamarulhaili, H. (2014). Point multiplication using integer sub-decomposition for elliptic curve cryptography. *Applied Mathematics & Information Sciences*, 8(2):517–525.

Antony, S. N. F. M. A. and Kamarulhaili, H. (2018). ISD method implementation over curves with j-invariant 0. In *Simposium Kebangsaan Sains Matematik ke-25*, Pahang. AIP.

Bafandehkar, M., Yasin, S. M., Mahmod, R., and Hanapi, Z. M. (2013). Comparison of ECC and RSA algorithm in resource constrained devices. *2013 International Conference on IT Convergence and Security*, pages 1–3.

Cohen, H. (1996). *A Course in Computatonal Algebraic Number Theory*. Springer-Verlag, Berlin, Heidelberg, New York.

Galbraith, S. D. (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press, UK.

Gallant, R. P., Lambert, R. J., and Vanstone, S. A. (2001). Faster point multiplication on elliptic curves with efficient endomorphisms. *CRYPTO2001*, 2139:190–200.

Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York.

Kwon, J., Seo, S. C., and Hong, S. (2018). Efficient implementations of four-dimensional GLV-GLS scalar multiplication on 8-bit, 16-bit and 32-bit microcontrollers. *Applied Sciences*, 8(6):1–23.

Ribenboim, P. (2001). *Classical Theory of Algebraic Numbers*. Springer-Verlag, New York, Berlin, Heidelberg.

Salah, N. F. H. A. and Said, M. R. M. (2014). High performance methods of elliptic curve scalar multiplication. *International Journal of Computer Science*, 108(20):39–45.

Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer Science & Business Media, Dordrecht, Heidelberg, London, New York, 2nd edition.

Washington, L. C. (2007). *Elliptic Curves Number Theory and Cryptography*. CRC Press, London, New York, 2nd edn edition.

Zhou, Z., Hu, Z., Xu, M., and Song, W. (2010). Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves. *Information Processing Letter*, 110:1003–1006.