Journal of Control Science and Engineering 2 (2015) 91-101
doi:10.17265/2328-2231/2015.02.004

Upper Bound of Scalars in the Integer Sub-decomposition Method: The Theoretical Aspects

Ruma Kareem K. Ajeena
Babylon University, Department of Mathematics, Education College for Pure Sciences, Babil 51002, Iraq

Abstract: The focal point of this paper is to present the theoretical aspects of the building blocks of the upper bounds of ISD (integer sub-decomposition) method defined by $kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P)$ with $\max\{|k_{11}|,|k_{12}|\} \le C\sqrt{n}$ and $\max\{|k_{21}|,|k_{22}|\} \le C\sqrt{n}$, where $C = 1$ that uses efficiently computable endomorphisms ψ_j for $j = 1,2$ to compute any multiple kP of a point P of order n lying on an elliptic curve E. The upper bounds of sub-scalars in ISD method are presented and utilized to enhance the rate of successful computation of scalar multiplication kP. Important theorems that establish the upper bounds of the kernel vectors of the ISD reduction map are generalized and proved in this work. The values of C in the upper bounds, that are greater than 1, have been proven in two cases of characteristic polynomials (with degree 1 or 2) of the endomorphisms. The upper bound of ISD method with the case of the endomorphism rings over an integer ring Z results in a higher rate of successful computations kP. Compared to the case of endomorphism rings, which is embedded over an imaginary quadratic field $Q = [\sqrt{D}]$. The determination of the upper bounds is considered as a key point in developing the ISD elliptic scalar multiplication technique.

Key words: Elliptic curve cryptography, scalar multiplication, ISD method, efficiently computable endomorphism, upper bounds.

1. Introduction

For over a hundred years, mathematicians have used the desirable features of elliptic curves to solve a variety of problems. Elliptic curves serve as a traditional asymmetric cryptosystem, such as the RSA (Rivest, Shamir and Adleman). However, their performance found important application in security level [1].

This study presents the computation of the scalar multiplication kP for a point P, which lies on an elliptic curve E that has a large prime order n. This computation is performed using a scalar k randomly chosen from the $[1, n-1]$ interval, which is the key to controlling the execution time in elliptic curve cryptosystems.

Gallant et al. [2] initially proposed the GLV (Gallant, Lambert and Vanstone) method in 2001. This method has been applied to special classes of elliptic curves which possess efficiently computable endomorphisms, with characteristic polynomials to compute the multiple kP of a point P of order n lying on an elliptic curves E. Accordingly, researchers used the GLV method and initially failed to provide an upper bound on $\max\{|k_1|,|k_2|\}$. They only produced a guided estimation showing that the upper bound should be $O(\sqrt{n})$ without demonstrating any estimation of the concerned constant.

The first upper bound appeared in Ref. [3] with the use of a different method compared to GLV idea. In 2003, the research gap on the bound of kernel vectors of the reduction map T was studied by Ref. [1], where T is a group homomorphism defined from a lattice $Z \times Z$ into group Z/n by

$$(a,b) \to a + b\lambda \pmod{n} \quad (1)$$

for some $\lambda \in [1, n-1]$ with a prime number n. The GLV decomposition with explicit constant C was established with the use of the following expression

Corresponding author: Ruma Kareem K. Ajeena, Ph.D., research fields: elliptic curve cryptography, scalar multiplication, algebraic number theory, linear algebra. E-mail: ruma.usm@gmail.com.

$$kp = k_1 p + k_2 \psi(P), \quad with \quad max\{|k_1|, |k_2|\} \le \sqrt{1+|w|+z}\sqrt{n}, \tag{2}$$

where $\psi(P)$ is an endomorphism of E over a prime field F_p, whereas w and z are small fixed integer values (that are coefficients of characteristic polynomial $X^2 + wX + z (\text{mod } n)$).

This study analyzes the GLV method introduced in Ref. [2]. Two fast endomorphisms with minimal polynomials $X^2 + w_j X + z_j$ or $X - \lambda_j$ for $j = 1,2$ are used to obtain the mathematical proofs. These mathematical proofs are utilized to compute the upper bound of the ISD (integer sub-decomposition) scalar multiplication kP. The sub-decomposition from $k = k_1 + k_2 \pmod n$ with $max\{|k_1|, |k_2|\} > \sqrt{n}$ is clearly shown as follows:

$$k_1 = k_{11} + k_{12}\lambda_1 (\text{mod } n)$$

and

$$k_2 = k_{21} + k_{22}\lambda_2 (\text{mod } n)$$

Computation of the ISD scalar multiplication kP is given by $kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P)$, with $max\{|k_{11}|, |k_{12}|\} \le \sqrt{1+|\lambda_1|}\sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} \le \sqrt{1+|\lambda_2|}\sqrt{n}$ on an ordinary elliptic curve or $max\{|k_{11}|, |k_{12}|\} \le \sqrt{1+|w_1|+z_1}\sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} \le \sqrt{1+|w_2|+z_2}\sqrt{n}$ on special classes of elliptic curve.

The rest of this paper is organized as follows. Section two reviews the mathematical background related to this work. Section three gives an explanation of the procedure of scalar multiplication through ISD computation method and the theoretical concept involved. Section four discusses the procedure used to fill the logical gap. The mathematical proofs used in determining the value C in the upper bound of the kernel vectors on the reduction map T for the ISD method are presented in two cases. Finally, the conclusions are given in Section five.

2. Preliminaries: Mathematical Foundations

Theorem 2.1: (Hasse's Theorem) [4]. Suppose E is an elliptic curve over a prime field F_p. Then

$$\#E(F_p) = p + 1 - t_p, with \quad |t_p| \le 2\sqrt{p} \tag{3}$$

where t_p is a trace of Frobenius for E over F_p. In other words, t_p forms as the trace of a 2×2 matrix that works as a linear transformation on two-dimensional vector space formed on E over F_p.

Definition 2.2: (Rectangle Norm) [1]. The rectangle norm of any vector $v = (x, y) \ne (0,0)$ in kernel, $\ker T$, of the group homomorphism T can be defined by

$$|(x, y)| = \max(|x|, |y|) \tag{4}$$

Definition 2.3: (SVP (Shortest Vector Problem)) [5]. The SVP involves finding the shortest nonzero vector in lattice L. In other words, the nonzero vector $v \in L$, which minimizes the Euclidean norm $\|v\|$ must be found.

Lemma 2.4: [2]. The vector $u = (k, 0) - v$ has norm at most $\max(\|v_1\|, \|v_2\|)$ In other words,

$$\|u\| \le max(\|v_1\|, \|v_2\|) \tag{5}$$

Lemma 2.5: (Properties of the EEA (Extended Euclidean Algorithm)) [2]. Suppose tuples of variables s_i, t_i and r_i are defined by

$$s_i n + t_i \lambda = r_i, \tag{6}$$

for $i = 0,1,2,..., m, m+1, m+2,..., z-1$, with $z > m$. where, $s_0 = 1, t_0 = 0, r_0 = n, s_1 = 0, t_1 = 1, r_1 = \lambda$ and $r_i \ge 0$ for all i produced by applying EEA to positive integers n and λ. Then these variables satisfy

i. $r_i > r_{i+1} \ge 0, \forall i \ge 0$.
ii. $|s_i| < |s_{i+1}|, \forall i \ge 1$.
iii. $t_i | < | t_{i+1} |, \forall i \ge 0$.
iv. $r_{i-1}|t_i| + r_i|t_{i-1}| = n, \forall i \ge 1$.

Lemma 2.6: (Properties of the GEEA (Generalized Extended Euclidean Algorithm)) [6]. Suppose $\langle s_{0_j}, s_{1_j}, \cdots, s_{(z-1)_j} \rangle$, $\langle t_j \rangle = \langle t_{0_j}, t_{1_j}, \cdots, t_{(z-1)_j} \rangle$ and $\langle r_j \rangle = \langle r_{0_j}, r_{1_j}, ..., r_{(z-1)_j} \rangle$ are z-tuples of integers such that $s_{i_j} n + t_{i_j} \lambda_j = r_{i_j}$, for $j = 1,2$ and

$i = 0,1, 2, ..., m, m+1, m+2, ..., z-1$ with $z > m$ obtained by applying GEEA to positive integers n, λ_j. Then the elements in these z-tuples satisfy the following properties:

i. $r_{i_j} > r_{(i+1)_j} \geq 0, \quad \forall\ 0 \leq i \leq z-1$ and $j = 1,2.$

ii. $|s_{i_j}| \lhd |s_{(i+1)_j}|, \forall\ 1 \leq i \leq z-1$ and $j = 1,2.$

iii. $|t_{i_j}| \lhd |t_{(i+1)_j}|, \forall\ 0 \leq i \leq z-1$ and $j = 1,2.$

iv. $r_{i_j} t_{(i-1)_j} - r_{(i-1)_j} t_{i_j} = (-1)^{i-1} n.$

In other words,

$$r_{i_j} |t_{(i-1)_j}| + r_{(i-1)_j} |t_{i_j}| = n, \forall\ 1 \leq i \leq z-1$$

and $j = 1,2.$

3. Upper Bound of Sub-scalars in ISD Computation Method

The ISD computation method [6-8] is briefly interpreted in this section. Assuming that F_p is a prime field, point $P = (x, y)$ lies on an elliptic curve E defined over a field F_p which has prime order n, such that the cofactor $h = \#E(F_p)/n$ is small, (e.g., $h = 1$). Also, suppose that the $\psi_j(P)$, with $j = 1,2,$ are efficient computable endomorphisms of E and their characteristic polynomials $X - \lambda_j$ modulo n, where λ_j denote the integers in the $[1, n-1]$ interval and $\lambda_1 \neq \pm\lambda_2$. The case $\lambda_j = 0$ is excluded. However, there is only one copy of Z/n inside $E(F_p)$ and $\psi_j(P)$ are sets of points that form subsets of the subgroup $\langle P \rangle$ of the group $E(F_p)$. The ISD method can be applied to compute kP of a point P lying on special elliptic curve group $E(F_p)$ with specific value of p, (e.g., elliptic curve group formed from elliptic curve $E: y^2 = x^3 + ax$ or $E: y^2 = x^3 + b$ over prime fields with $p \equiv 1 (\text{mod } 4)$ or $p \equiv 1 (\text{mod } 3)$ respectively, which has large prime order. The group order $\#E(F_p)$ here is a large prime order since $h \leq 4$.

The characteristic polynomials of non-trivial endomorphisms ψ_j, for $j = 1,2,$ defined over F_p take the form $X^2 + w_j X + z_j$, where w_j and z_j are actually small fixed integers. The Hasse bound shown in the Hasse's Theorem (2.1) can determine the bound of the order $\#E(F_p)$ as shown in Eq. (3), which has a large prime n, such that $\psi_j(P) = \lambda_j P$ for some $\lambda_j \in [1, n-1]$ for $j = 1,2$ and P is a point that has prime order n. There is only one copy of Z/n inside $E(F_p)$ which has order dividing n. Furthermore, the parameters $\lambda_j, j = 1,2,$ are roots of $X^2 + w_j X + z_j$ modulo n. The case $\lambda_j = 0$ is excluded.

A fundamental role of the ISD method lies in the definition of the group homomorphism given by Eq. (1). Supposing that *kerT* is a kernel of homomorphism T, *kerT* is clearly a sub-lattice L_s of a lattice $L = Z \times Z$. Let $\{v_1, v_2\}, \{v_3, v_4\}$ and $\{v_5, v_6\}$ be the bases in *kerT*. Therefore, vectors v_1, v_2, v_3, v_4, v_5 and v_6 are linearly independent vectors and are represented as integer lattice points of *kerT* satisfying

$$\left.\begin{aligned} max\{|v_1|, |v_2|\} \leq \sqrt{n}, \\ max\{|v_3|, |v_4|\} \leq \sqrt{n}, \\ max\{|v_5|, |v_6|\} \leq \sqrt{n}. \end{aligned}\right\} \quad (7)$$

for some $\sqrt{n} > 0$, where, $|\cdot|$ denotes the rectangle norm defined in Eq. (4). The lattice points (that is the vectors v_2, v_4 and v_6) are computed by solving the shortest vector problem in a lattice as seen in Definition (2.3). The GLV generator $\{v_1, v_2\}$ and ISD generators $\{v_3, v_4\}$ and $\{v_5, v_6\}$ can be computed by applying the EEA, as presented in Lemma (2.5) and the GEEA, as presented in Lemma (2.6), respectively.

Every vector v_i for $i = 1,2,...,6$ in *kerT* is expressed as a linear combination of the vectors contained in a generating set. Hence, these vectors are written as

$$\left.\begin{aligned} (k,0) = \beta_1 v_1 + \beta_2 v_2, \text{from a generating set} \{v_1, v_2\}, \\ (k_1,0) = \beta_3 v_3 + \beta_4 v_4, \text{from a generating set} \{v_3, v_4\}, \\ (k_2,0) = \beta_5 v_5 + \beta_6 v_6, \text{from a generating set} \{v_5, v_6\}, \end{aligned}\right\}$$

where, $\beta_i \in Q, i = 0,1,2,3,4,5,6.$ Then the rounding off β_i to the nearest integer $c_i = \lceil \beta_i \rceil = \lfloor \beta_i + 1/2 \rfloor$. Let

$v = c_1 v_1 + c_2 v_2$, $v' = c_3 v_3 + c_4 v_4$ and $v'' = c_5 v_5 + c_6 v_6$, be vectors. These vectors in $kerT$. Also, let us define the following vectors

$$u_0 = (k,0) - v\,, u_1 = (k_1,0) - v' \text{ and } u_2 = (k_2,0) - v''.$$

u_0, u_1 and u_2 are short vectors as proved in Lemma (2.4), and Lemma (3.30) in Ref. [6]. Then,

$$\left.\begin{aligned} |u_0| &\le max\{|v_1|,|v_2|\} \le \sqrt{n}, \\ |u_1| &\le max\{|v_3|,|v_4|\} \le \sqrt{n}, \\ |u_2| &\le max\{|v_5|,|v_6|\} \le \sqrt{n}. \end{aligned}\right\} \quad (8)$$

The vector $u_0 = (k_1, \bar{k}_2)$ is proved in Eq. (3.99) in Ref. [6]. Then $k \equiv k_1 + (\bar{k}_2 \lambda) \pmod n$ from the definition of homomorphism given in Eq. (1), where k_1 and $\bar{k}_2$ are the integers resulting from the decomposition of multiplier k using the balanced length-two representation of a multiplier Algorithm (3.74) in Ref. [10]. Integer k is decomposed using formula

$$\begin{aligned} &k \equiv k_1 + k_2 (\bmod n), \\ &with\,|(k_1,k_2)| = max\{|k_1|,|k_2|\} > \sqrt{n}. \end{aligned} \quad (9)$$

The proof of this relation is introduced in Theorem (3.26) in Ref. [6]. The main idea of the ISD method is to sub-decompose values $|k_1|$ and $|k_2|$ when their maximum value is not bounded by $\sqrt{n}$. Accordingly, decomposing k_1 and k_2 again into integers k_{11}, k_{12} and k_{21}, k_{22} indicates the sub-decomposition of k using algorithm (2) in Ref. [6, 7] of the ISD sub-decomposition for a scalar,

$$k \equiv k_{11} + k_{12}\lambda_1 + k_{22}\lambda_2 (\bmod n),$$

with $-\sqrt{n} \le k_{11}, k_{12}, k_{21}, k_{22} \le \sqrt{n}$ from any ISD generators $\{v_3, v_4\}$ and $\{v_5, v_6\}$. Suppose

$$u_1 \equiv (k_{11}, k_{12}), \text{ and } u_2 \equiv (k_{21}, k_{22})$$

then

$$T(u_1) = k_1 \equiv k_{11} + k_{12}\lambda_1 (\bmod n),$$

and

$$T(u_2) = k_2 \equiv k_{21} + k_{22}\lambda_2 (\bmod n)$$

(that have been proved in Ref. [6]). These are equivalent to

$k_1 P = k_{11} p + k_{12}\psi_1(P)$ and $k_2 P = k_{21} p + k_{22}\psi_2(P)$.

In other words, the ISD elliptic scalar multiplication is

$$kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P), \quad (10)$$

with

$$|(k_{11}, k_{12})| \le \sqrt{n} \text{ and } |(k_{21}, k_{22})| \le \sqrt{n} \quad (11)$$

The performance of the scalar multiplication kP in Eq. (10) can be done using the computation of the interleavings which depends on the pre-computations of two endomorphisms $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$, where, $P \in E(F_p)$, $\lambda_1, \lambda_2 \in [1, n-1]$ and $\lambda_1 \ne \pm\lambda_2$. Based on ISD Algorithm (10) in Ref. [6], the ISD method produces a 50% success rate increase in the kP computation compared to the GLV method.

4. Determining the Value for C in the Upper Bound for ISD Method

This section discusses overcoming the indeterminacy of the upper bound of ISD method which focuses on the sub-decomposition of integer k when the decomposed values $|k_1|$ and $|k_2|$ are not bounded by $\sqrt{n}$ on the interval $[1, n-1]$. The ISD method [6-8] construction depends on the GLV method. Hence, a tuple of relations in Eq. (6) for a given n and λ is generated using the EEA given in Lemma (2.5).

The GLV algorithm used in the ISD method defines index m as the largest integer for which $r_m \ge \sqrt{n}$. The employment of the statement defined in case (iv) and given in Lemma (2.5) with $i = m+1$ indicates that $|t_{m+1}| < \sqrt{n}$. Therefore, vector $v_1 = (r_{m+1}, -t_{m+1})$ in $kerT$ has a rectangle norm bounded by $\sqrt{n}$. Vector v_2 in the GLV generator algorithm (1) in Ref. [9] is the shortest between $(r_m, -t_m)$ and $(r_{(m+2)}, -t_{(m+2)})$, such that

$$min(|(r_m, -t_m)|, |(r_{m+2}, -t_{m+2})|) \le C\sqrt{n}, \quad (12)$$

with an explicit value of $C = 1$ and $gcd(r_m, -t_m) = 1$ and $gcd(r_{m+2}, -t_{m+2}) = 1$. Determining the upper bound of these vectors depends on the manner of

finding the C value. The discussion that follows focuses on finding the C value. The application of ISD method that uses efficient computable endomorphisms $\psi(P)=\lambda_j P$ of E over a prime field F_p which has characteristic polynomials $X-\lambda_j$ for $j=1,2$ can be proven by the following results.

Theorem 4.1: Let s_i, t_i, r_i for $i=0,1,2,...,m$, $m+1, m+2, z-1$ with $z>m$ and s_{i_j}, t_{i_j} and r_{i_j} for

$$i=0,\ 1,\ 2,\ ...,\ m_j,\ (m+1)_j,\ (m+2)_j,...,\ (z-1)_j$$

with $z_j > m_j$ and $j=1,2$ be tuples of variables resulting from EEA applied to n, λ and GEEA applied to n, λ_j, respectively. Let m and m_j be indexes defined as the largest integers for which $r_m, r_{m_j} \geq \sqrt{n}$. The components $r_{(m+1)}, -t_{(m+1)}$ and $r_{(m+1)_j}, -t_{(m+1)_j}$ form the vectors v_1, v_3 and v_5 respectively. The vector,

$$v_1=(r_{(m+1)}, -t_{(m+1)}),$$
$$v_3=(r_{(m+1)_1}, -t_{(m+1)_1}),$$
$$v_5=(r_{(m+1)_2}, -t_{(m+1)_2}) \neq (0,0)$$

where, $v_1, v_3, v_5 \in kerT$.

Then

$$\left.\begin{aligned} &\left|\left(r_{m+1}, -t_{m+1}\right)\right| \geq \sqrt{n}\Big/\sqrt{1+|\lambda|}, \\ &\left|\left(r_{(m+1)_j}, -t_{(m+1)_j}\right)\right| \geq \sqrt{n}\Big/\sqrt{1+|\lambda_j|},\ j=1,2 \end{aligned}\right\} \quad (13)$$

where $\lambda, \lambda_j \in [1, n-1]$.

Proof:

The first part of Eq. (13) has been proven in Lemma (4.5) in Ref. [6]. The second part of Eq. (13) can be proven as follows. Recall the GEEA given in Theorem (3.8) in Refs. [6,11] and applied to n and λ_j for $j=1,2$. This generalization was used in ISD method to generate two tuples of variables $(s_{i_1}, t_{i_1}, r_{i_1})$ and $(s_{i_2}, t_{i_2}, r_{i_2})$ such that

$$s_{i_j} n + t_{i_j} \lambda_j = r_{i_j} \quad (14)$$

where,

$$\text{j}=1,2 \text{ and } i=0,1,2,...m_j,(m+1)_j,(m+2)_j,...,(z-1)_j,$$

with $z_j > m_j$, where $|s_{i_j}| < |s_{(i+1)_j}|$ for $i \geq 1$ and for all $j=1,2$, $|t_{i_j}| < |t_{(i+1)_j}|$, $r_{i_j} > r_{(i+1)_j} \geq 0$ for all $i \geq 0$ and $j=1,2$ in Lemma (2.6).

The index m_j, for $j=1,2$, of the ISD algorithm defines as the largest integer for which $r_{m_j} \geq \sqrt{n}$ with $j=1,2$. Then from Statement (iv) in Lemma (2.6) with $i=(m+1)_j$, it can be found that $\left|t_{(m+1)_j}\right| < \sqrt{n}$. As a result, the kernel vectors $v_3=(r_{(m+1)_1}, -t_{(m+1)_1})$ and $v_5=(r_{(m+1)_2}, -t_{(m+1)_2})$ have rectangle norms bounded by $\sqrt{n}$. In addition, the determination of the vectors v_4 and v_6 depending on the selection of the shortest vectors between $v_4=(r_{m_1}, -t_{m_1})$ and $v_4=(r_{(m+2)_1}, -t_{(m+2)_1})$ and $v_6=(r_{m_2}, -t_{m_2})$ and $v_6=(r_{(m+2)_2}, -t_{(m+2)_2})$ respectively. The vectors v_4 and v_6 must satisfy the following relation,

$$\left.\begin{aligned} &min\left\{\left|\left(r_{m_1}, -t_{m_1}\right)\right|, \left|\left(r_{(m+2)_1}, -t_{(m+2)_1}\right)\right|\right\} \leq C\sqrt{n} \\ &min\left\{\left|\left(r_{m_2}, -t_{m_2}\right)\right|, \left|\left(r_{(m+2)_2}, -t_{(m+2)_2}\right)\right|\right\} \leq C\sqrt{n} \end{aligned}\right\} \quad (15)$$

that corresponding to the shortness conditions given in Steps (4) and (9) in Algorithm (3) in Ref. [6], where

$$\left.\begin{aligned} &gcd\left(r_{m_1}, -t_{m_1}\right)=1 \\ &gcd\left(r_{(m+2)_1}, -t_{(m+2)_1}\right)=1 \\ &gcd\left(r_{m_2}, -t_{m_2}\right)=1 \\ &gcd\left(r_{(m+2)_2}, -t_{(m+2)_2}\right)=1 \end{aligned}\right\}$$

with an explicit value $C=1$.

In more general, it can be rewritten Eqs. (12) and (15) in one form as follows

$$\left.\begin{aligned} &min\left\{\left|\left(r_m, -t_m\right)\right|, \left|\left(r_{m+2}, -t_{m+2}\right)\right|\right\} \leq C\sqrt{n} \\ &min\left\{\left|\left(r_{m_j}, -t_{m_j}\right)\right|, \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right|\right\} \leq C\sqrt{n},\ j=1,2 \end{aligned}\right\} \quad (16)$$

with an explicit value $C=1$.

Now, the determination of the upper bound of these vectors depending on how to find the value of C. The following discussion focuses on finding such value of C.

Let $\lambda_j \in [1, n-1]$ be the root of $X-\lambda_j \pmod n$, $j=1,2$. For *any* $(x,y) \in ker\text{T} -\{(0,0)\}$, then, from definition of the group

homomorphism T that is given in Eq. (1), it can be seen

$$(x, y) \to x + \lambda_j y \pmod{n} \equiv 0$$

so,

$$0 \equiv (x + \lambda_j y) \equiv x - \lambda_j y \pmod{n}.$$

Since $X - \lambda_j$ is irreducible polynomial in Z[X], then

$$x - \lambda_j y \geq n, \text{ for } j = 1,2 \tag{17}$$

This certainly leads to

$$\begin{aligned} n \leq x - \lambda_j y, \text{ for } j = 1,2 &\leq x + |\lambda_j| y \\ &\leq max\ \{x^2 + |\lambda_j| x^2, y^2 + |\lambda_j| y^2\}, \\ &= max\ \{(1 + |\lambda_j|)x^2, (1 + |\lambda_j|)y^2\}, \\ &= (1 + |\lambda_j|) max\ \{x^2, y^2\}, \\ \frac{n}{(1 + |\lambda_j|)} &\leq max\ \{x^2, y^2\}, \end{aligned}$$

so, from rectangle norm given in Eq. (4), one then has the following relation for any vector in $kerT$ which differs from $(0,0)$,

$$\sqrt{\frac{n}{(1 + |\lambda_j|)}} \leq max\ \{|x|, |y|\} = |(x, y)|, \tag{18}$$

In particular, since $v_3 = (r_{(m+1)_1}, -t_{(m+1)_1})$ and $v_5 = (r_{(m+1)_2}, -t_{(m+1)_2}) \in kerT - \{(0,0)\}$, so

$$\left.\begin{aligned} \left|\left(r_{(m+1)_1}, -t_{(m+1)_1}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda_1|}, \\ \left|\left(r_{(m+1)_2}, -t_{(m+1)_2}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda_2|}. \end{aligned}\right\} \tag{19}$$

Based on Eq. (4.23) that is proven in Ref. [6] and the relation in Eq. (19), one then rewrite

$$\left.\begin{aligned} \left|\left(r_{m+1}, -t_{m+1}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda|}, \\ \left|\left(r_{(m+1)_j}, -t_{(m+1)_j}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda_j|}, j = 1,2. \end{aligned}\right\}$$

Corollary 4.2: Let s_i, t_i, r_i for $i = 0,1,2,...,m$, $m+1, m+2, z-1$ with $z > m$ and s_{i_j}, t_{i_j} and r_{i_j} for $i = 0,1,2,...,m_j, (m+1)_j, (m+2)_j, ..., (z-1)_j$ with $z_j > m_j$ and $j = 1,2$ be tuples of variables resulting from EEA applied to n, λ and GEEA applied to n, λ_j, respectively. Let m and m_j be indexes defined as the largest integers for which $r_m, r_{m_j} \geq \sqrt{n}$. The components $r_{(m+1)}, -t_{(m+1)}$ and $r_{(m+1)_j}, -t_{(m+1)_j}$ form the vectors v_1, v_3 and v_5 respectively. The vector $v_1 = (r_{(m+1)}, -t_{(m+1)})$, $v_3 = (r_{(m+1)_1}, -t_{(m+1)_1})$, $v_5 = (r_{(m+1)_2}, -t_{(m+1)_2}) \neq (0,0)$ and $v_1, v_3, v_5 \in kerT$. Then

$$\left.\begin{aligned} \left|\left(r_{m+1}, -t_{m+1}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |w| + z}, \\ \left|\left(r_{(m+1)_j}, -t_{(m+1)_j}\right)\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |w_j| + z_j}, j = 1,2. \end{aligned}\right\} \tag{20}$$

where $w, w_j, z \text{ and } z_j$ are small fixed integers.

Proof:

The proof takes the similar pattern as used to prove the general case in Theorem (4.1).

Theorem 4.3: Suppose that

$$\left.\begin{aligned} |t_{m+1}| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda|}, \\ \left|t_{(m+1)_j}\right| &\geq \sqrt{n} \Big/ \sqrt{1 + |\lambda_j|}, \text{ when } j = 1,2. \end{aligned}\right\} \tag{21}$$

Then

$$\left.\begin{aligned} r_m &< \sqrt{1 + |\lambda|}\sqrt{n}, \\ r_{m_j} &< \sqrt{1 + |\lambda_j|}\sqrt{n}, \text{ when } j = 1,2. \end{aligned}\right\} \tag{22}$$

Hence

$$\left.\begin{aligned} \left|\left(r_m, -t_m\right)\right| &< \sqrt{1 + |\lambda|}\sqrt{n}, \\ \left|\left(r_{m_j}, -t_{m_j}\right)\right| &< \sqrt{1 + |\lambda_j|}\sqrt{n}, \text{ where } j = 1,2. \end{aligned}\right\} \tag{23}$$

where $\lambda, \lambda_j \in [1, n-1]$.

Proof:.

The first part of Eq. (23) has been proved in Lemma (4.6) in Ref. [6]. From the generalized Statement (iv) of Lemma (2.6) defined by $r_{i_j} |t_{(i-1)_j}| + r_{(i-1)_j} |t_{i_j}| = n$ for all $i \geq 1$ with $i = m+1$ and $j = 1,2$, then $r_{m_j} \left|t_{(m+1)_j}\right| = n - r_{(m+1)_j} \left|t_{(m)_j}\right| < n$, since $r_{(m+1)_j}$ and $|t_{m_j}| \text{ for } j = 1,2$ are positive integers. Now, $r_{m_j} \left|t_{(m+1)_j}\right| < n$.

So

$$r_{m_j} < \frac{n}{\left|t_{(m+1)_j}\right|}, \text{ for } j = 1,2. \tag{24}$$

But $|t_{(m+1)_j}| \geq \sqrt{n} / \sqrt{1+|\lambda_j|}$, from the second part of Eq. (21). Therefore

$$\frac{1}{\left|t_{(m+1)_j}\right|} \leq \frac{\sqrt{1+\left|\lambda_j\right|}}{\sqrt{n}} \tag{25}$$

The substitution of the relation in Eq. (25) in Eq. (24) leads to

$$r_{m_j} < n\frac{\sqrt{1+\left|\lambda_j\right|}}{\sqrt{n}} = \sqrt{n}\sqrt{1+\left|\lambda_j\right|} \tag{26}$$

Now, since $r_{m_j} > \sqrt{n} > |t_{(m+1)_j}| > |t_{m_j}|$, from the generalized Statement (iii) of Lemma (2.6) then

$$r_{m_j} > \left|t_{m_j}\right|$$

and from the relation in Eq. (26), yields the following relation

$$|t_{m_j}| < r_{m_j} < \sqrt{n}\sqrt{1+|\lambda_j|}.$$

Thus

$$\begin{aligned} \left|\left(r_{m_j}, -t_{m_j}\right)\right| &= max\left\{\left|r_{m_j}\right|, \left|t_{m_j}\right|\right\}, \text{ for } j = 1,2. \\ &= max\left\{\left|r_{m_j}\right|, \left|t_{m_j}\right|\right\} \\ &= r_{m_j} \\ &< n\sqrt{1+\left|\lambda_j\right|}, \end{aligned} \tag{27}$$

Therefore, from Eq. (4.27) proven in Ref. [6] and Eq. (27), it can be written

$$\left.\begin{aligned} \left|\left(r_m, -t_m\right)\right| &< \sqrt{n}\sqrt{1+\left|\lambda\right|}, \\ \left|\left(r_{m_j}, -t_{m_j}\right)\right| &< \sqrt{n}\sqrt{1+\left|\lambda_j\right|}, \text{ where } j = 1,2. \end{aligned}\right\}$$

Corollary 4.4: Suppose that

$$\left.\begin{aligned} \left|t_{m+1}\right| &\geq \sqrt{n}\Big/\sqrt{1+|w|+z}\,, \\ \left|t_{(m+1)_j}\right| &\geq \sqrt{n}\Big/\sqrt{1+\left|w_j\right|+z_j}\,, j = 1,2. \end{aligned}\right\} \tag{28}$$

Then

$$\left.\begin{aligned} r_m &< \sqrt{1+|w|+z}\sqrt{n}, \\ r_{m_j} &< \sqrt{1+\left|w_j\right|+z_j}\sqrt{n}, j = 1,2. \end{aligned}\right\} \tag{29}$$

Then one has the following relations,

$$\left.\begin{aligned} |(r_m, -t_m)| &< \sqrt{1+|w\ |+z}\sqrt{n}, \\ |(r_{m_j}, -t_{m_j})| &< \sqrt{1+|w_j\ |+z_j}\sqrt{n}, j = 1,2, \end{aligned}\right\} \tag{30}$$

where, w, w_j, z and z_j are small fixed integers.

Proof:

The proof takes the similar way that is used to prove the general case in Theorem (4.3).

Theorem 4.5: Assume that

$$\left.\begin{aligned} r_{m+1} &\geq \sqrt{n}\Big/\sqrt{1+\left|\lambda\right|}\,, \\ r_{(m+1)_j} &\geq \sqrt{n}\Big/\sqrt{1+\left|\lambda_j\right|}\,, \text{ for } j = 1,2. \end{aligned}\right\} \tag{31}$$

Then

$$\left.\begin{aligned} \left|t_{m+2}\right| &< \sqrt{1+\left|\lambda\right|}\sqrt{n}, \\ \left|t_{(m+2)_j}\right| &< \sqrt{1+\left|\lambda_j\right|}\sqrt{n}, \text{ for } j = 1,2. \end{aligned}\right\} \tag{32}$$

hence,

$$\left.\begin{aligned} \left|\left(r_{m+2}, -t_{m+2}\right)\right| &< \sqrt{1+\left|\lambda\right|}\sqrt{n}, \\ \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right| &< \sqrt{1+\left|\lambda_j\right|}\sqrt{n}, j = 1,2. \end{aligned}\right\} \tag{33}$$

where, $\lambda, \lambda_j \in [1, n-1]$.

Proof:

The first part of Eq. (33) has been proved in Lemma (4.7) in Ref. [6].

To prove second part of Eq. (33), suppose $n = r_{i_j}|t_{(i-1)_j}| + r_{(i-1)_j}|t_{i_j}|$ for all $i \geq 1$ with $i = m+2$ and $j = 1,2,$ is the generalized statement given in (iv) of Lemma (2.6).

Then,

$r_{(m+1)_j}\left|t_{(m+2)_j}\right| = n - r_{(m+2)_j}\left|t_{(m+1)_j}\right| < n$, since $r_{(m+2)_j}$ and $|t_{(m+1)_j}|$ are positive integers.

Now, $r_{(m+1)_j}\left|t_{(m+2)_j}\right| < n$. So,

$$|t_{(m+2)_j}| < \frac{n}{r_{(m+1)_j}}. \tag{34}$$

But $r_{(m+1)_j} \geq \sqrt{n} / \sqrt{1+|\lambda_j|}$, from the second part of Eq. (31). Therefore

$$\frac{1}{r_{(m+1)_j}} \leq \frac{\sqrt{1+|\lambda_j|}}{\sqrt{n}}. \quad (35)$$

The substitution of the relation in Eq. (35) in Eq. (34) leads to

$$\left|t_{(m+2)_j}\right| < n \cdot \frac{\sqrt{1+\left|\lambda_j\right|}}{\sqrt{n}} = \sqrt{n}\sqrt{1+\left|\lambda_j\right|}. \quad (36)$$

Now, the relation,

$$\left|r_{(m+2)_j}, -t_{(m+2)_j}\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n} \quad \text{for } j = 1.2,$$

in the second part of the statement (33) can be proven as follows.

Let $r_{(m+1)_j} \geq \sqrt{n} / \sqrt{1+|\lambda_j|}$ and $\left|t_{(m+2)_j}\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n}$, as given in the second parts of the Eqs. (31) and (32) respectively. For all $i \geq 1 \; with \; i = m+2$ and $j = 1,2,$ then $r_{i_j} |t_{(i-1)_j}| + r_{(i-1)_j} |t_{i_j}| = n$.

Therefore,

$$r_{(m+2)_j} = \frac{1}{|t_{(m+1)_j}|}(n - r_{(m+1)_j} |t_{(m+2)_j}|). \quad (37)$$

Since $|t_{(m+1)_j}| \geq \sqrt{n} / \sqrt{1+|\lambda_j|}$ from the second part of Eq. (21) in Theorem (4.3), therefore,

$$\frac{1}{|t_{(m+1)_j}|} \leq \frac{\sqrt{1+|\lambda_j|}}{\sqrt{n}}. \quad (38)$$

Thus, it can be rewritten Eq. (37) to become

$$r_{(m+2)_j} \leq \frac{\sqrt{1+\left|\lambda_j\right|}}{\sqrt{n}}(n - r_{(m+1)_j}\left|t_{(m+2)_j}\right|).$$

Since $|t_{(m+2)_j}| < \sqrt{n}$, then $n - r_{(m+1)} |t_{(m+2)_j}| < n.$ Therefore,

$$r_{(m+2)_j} \leq \frac{\sqrt{1+\left|\lambda_j\right|}}{\sqrt{n}} \cdot (n) = \sqrt{1+\left|\lambda_j\right|}\sqrt{n}.$$

And, from the second part of Eq. (32), $\left|t_{(m+2)_j}\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n}$,

Hence,

$$\left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n}. \quad (39)$$

From the relations in Eqs. (4.32) in Ref. [6] and Eq. (32), it can be written as,

$$\left.\begin{aligned} &\left|t_{m+2}\right| < \sqrt{1+\left|\lambda\right|}\sqrt{n}, \\ &\left|t_{(m+2)_j}\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n}, \text{ for } j = 1,2. \end{aligned}\right\}$$

Hence, it is possible to find

$$\left.\begin{aligned} &\left|\left(r_{m+2}, -t_{m+2}\right)\right| < \sqrt{1+\left|\lambda\right|}\sqrt{n}, \\ &\left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right| < \sqrt{1+\left|\lambda_j\right|}\sqrt{n}, \text{ for } j = 1,2. \end{aligned}\right\}$$

Corollary 4.6: Assume that

$$\left.\begin{aligned} &r_{m+1} \geq \sqrt{n} \Big/ \sqrt{1+|w|+z}, \\ &r_{(m+1)_j} \geq \sqrt{n} \Big/ \sqrt{1+\left|w_j\right|+z_j}, \text{ for } j = 1,2. \end{aligned}\right\} \quad (40)$$

Then,

$$\left.\begin{aligned} &\left|t_{m+2}\right| < \sqrt{1+|w|+z}\sqrt{n}, \\ &\left|t_{(m+2)_j}\right| < \sqrt{1+\left|w_j\right|+z_j}\sqrt{n}, \text{ for } j = 1,2. \end{aligned}\right\} \quad (41)$$

Hence,

$$\left.\begin{aligned} &\left|\left(r_{m+2}, -t_{m+2}\right)\right| < \sqrt{1+|w|+z}\sqrt{n}, \\ &\left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right| < \sqrt{1+\left|w_j\right|+z_j}\sqrt{n}, \text{ for } j = 1,2. \end{aligned}\right\}$$

where, w, w_j, z and z_j are small fixed integers.

Proof:

In similar way, it can be proved that this corollary depends on the proof of general case which has been proved in Theorem (4.5).

The following result finds the value of C and determines the upper bound for computing any ISD scalar multiplication kP. Finding the value C depends on two cases, these have been proved in Theorems (4.3) and (4.5) and also depends on the relation proven in Theorem (4.1).

Theorem 4.7: Let v_2, v_4 and v_6 be linear independent vectors such that a vector v_2 is a shorter vector between $(r_m, -t_m)$ and $(r_{m+2}, -t_{m+2}), v_4$ is a shorter vector between $(r_{m_1}, -t_{m_1})$ and $(r_{(m+2)_1}, -t_{(m+2)_1})$ and v_6 is a shorter vector between $(r_{m_2}, -t_{m_2})$ and $\left(r_{(m+2)_2}, -t_{(m+2)_2}\right)$. If these vectors satisfy the following relations,

$$\left.\begin{array}{l} min\left\{\left|(r_m, -t_m)\right|, \left|(r_{m+2}, -t_{m+2})\right|\right\} \le C\sqrt{n}, \\ min\left\{\left|\left(r_{m_j}, -t_{m_j}\right)\right|, \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right|\right\} \le C\sqrt{n}, \; j = 1,2. \end{array}\right\}$$

Then, the admissible value for C is

$$C = \begin{cases} \sqrt{1+|\lambda|}, \text{for GLV decomposit ion}, \\ \sqrt{1+|\lambda_j|}, \text{with } j = 1,2, \text{for ISD sub - decomposit ion} \end{cases} \quad (42)$$

In particular, any multiple kP can be decomposed as in Eq. (10) with

$$\left.\begin{array}{l} max\left\{|k_1|, |k_2|\right\} \le \sqrt{1+|\lambda|}\sqrt{n}, \\ max\left\{|k_{11}|, |k_{12}|\right\} \le \sqrt{1+|\lambda_1|}\sqrt{n}, \\ max\left\{|k_{21}|, |k_{22}|\right\} \le \sqrt{1+|\lambda_2|}\sqrt{n}. \end{array}\right\} \quad (43)$$

where, $\lambda, \lambda_1, \lambda_2 \in [1, n-1]$.

Proof:

First, it requires to prove the values of C as defined in Eq. (42). The value of C for GLV decomposition given in the first part of Eq. (4.38) is proven in Theorem (4.8) in Ref. [6]. So, the value of C as defined in second part of Eq. (42) can be proven as follow. Theorem (4.3), yields the following relation,

$$\left.\begin{array}{l} \left|(r_m, -t_m)\right| < \sqrt{1+|\lambda|}\sqrt{n}, \\ \left|\left(r_{m_j}, -t_{m_j}\right)\right| < \sqrt{1+|\lambda_j|}\sqrt{n}, \text{where } j = 1,2. \end{array}\right\}$$

And from Theorem (4.5),

$$\left.\begin{array}{l} \left|(r_{m+2}, -t_{m+2})\right| < \sqrt{1+|\lambda|}\sqrt{n}, \\ \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right| < \sqrt{1+|\lambda_j|}\sqrt{n}, \; j = 1,2. \end{array}\right\}$$

Then the last two relations yields,

$$\left.\begin{array}{l} min\left\{\left|(r_m, -t_m)\right|, \left|(r_{m+2}, -t_{m+2})\right|\right\} < \sqrt{1+|\lambda|}\sqrt{n}, \\ min\left\{\left|\left(r_{m_j}, -t_{m_j}\right)\right|, \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right|\right\} < \sqrt{1+|\lambda_j|}\sqrt{n}, \; j = 1,2. \end{array}\right\} \quad (44)$$

The comparison between equations,

$$\left.\begin{array}{l} min\left\{\left|(r_m, -t_m)\right|, \left|(r_{m+2}, -t_{m+2})\right|\right\} \le C\sqrt{n}, \\ min\left\{\left|\left(r_{m_j}, -t_{m_j}\right)\right|, \left|\left(r_{(m+2)_j}, -t_{(m+2)_j}\right)\right|\right\} \le C\sqrt{n}. \end{array}\right\}$$

for $j = 1,2$, as defined in the hypothesis with the relation in Eq. (44) finds the value of C as given in Eq. (42).

Now, there is need to prove any multiple kP decomposed as ISD elliptic scalar multiplication defined in Eq. (10) with the conditions in Eq. (43).

Since,

$$\left.\begin{array}{l} X - \lambda, \\ X - \lambda_j, \text{ for } j = 1,2. \end{array}\right\} \quad (45)$$

are irreducible polynomials in $Z[X]$,

$$\left.\begin{array}{l} x - \lambda y \ge n, \\ x - \lambda_j y \ge n, \text{ for } j = 1,2. \end{array}\right\} \quad (46)$$

as shown in Eqs. (4.24) in Ref. [6] and Eq. (17) respectively.

The inequalities, in Eq. (46), satisfy the following relations,

$$\left.\begin{array}{l} max\left\{|x|, |y|\right\} \ge \sqrt{\dfrac{n}{1+|\lambda|}}, \\ max\left\{|x|, |y|\right\} \ge \sqrt{\dfrac{n}{1+|\lambda_j|}}, \text{ for } j = 1,2. \end{array}\right\} \quad (47)$$

depending on the relations given in Eq. (4.25) in Ref. [6] and Eq. (18) respectively. Obviously,

$$\left.\begin{array}{l} \left|(r_{m+1}, -t_{m+1})\right| \ge \sqrt{n}\Big/\sqrt{1+|\lambda|} \\ \left|\left(r_{(m+1)_j}, -t_{(m+1)_j}\right)\right| \ge \sqrt{n}\Big/\sqrt{1+|\lambda_j|}, \; j = 1,2. \end{array}\right\}$$

through the relation (13) as proven in Theorem (4.1), and $\left|(r_{m+1}, -t_{m+1})\right| = |v_1|$, $\left|\left(r_{(m+1)_1}, -t_{(m+1)_1}\right)\right| = |v_3|$ and $\left|\left(r_{(m+1)_2}, -t_{(m+1)_2}\right)\right| = |v_5|$.

Since $u_0 = (k_1, k_2)$ from Eq. (3.99) $u_1 = (k_{11}, k_{12})$ and $u_2 = (k_{21}, k_{22})$ from Eqs. (3.121) and (3.122) in

Ref. [6], then $k \equiv k_1 + k_2 (\text{mod } n)$. Because $k_1 \equiv k_{11} + k_{12}\lambda_1 (\text{mod } n)$ and $k_2 \equiv k_{21} + k_{22}\lambda_2 (\text{mod } n)$ as shown in Eq. (3.123) in Ref. [6]. Therefore, the scalar k can be rewritten as $k \equiv k_{11} + k_{12}\lambda_1 + k_{21} + k_{22}\lambda_2 (\text{mod } n)$ .The expressions of k_1 and k_2 are equivalent to $k_1 P = k_{11} P + k_{12}\psi_1(P)$ and $k_2 P = k_{21} P + k_{22}\psi_2(P)$. It is more clearer to see, from inequalities defined by

$$\left.\begin{aligned} |u_0| \le \left|\frac{v_1 + v_2}{2}\right| \le \sqrt{n} \\ |u_1| \le \left|\frac{v_3 + v_4}{2}\right| \le \sqrt{n} \\ |u_2| \le \left|\frac{v_5 + v_6}{2}\right| \le \sqrt{n} \end{aligned}\right\}$$

and from Eqs. (9) and (11). Then

$$\left.\begin{aligned} |(k_1, k_2)| > \sqrt{n}, \\ |(k_{11}, k_{12})| \le \sqrt{n}, \\ |(k_{21}, k_{22})| \le \sqrt{n}. \end{aligned}\right\}$$

Since $\sqrt{n} \le C\sqrt{n}$, then $|(k_{11}, k_{12})| \le \sqrt{n} \le C\sqrt{n}$ and $|(k_{21}, k_{22})| \le \sqrt{n} \le C\sqrt{n}$.

Now, from definition of rectangle norm given in Eq. (4), $|(k_{11}, k_{12})| = max(|k_{11}|, |k_{12}|) \le C\sqrt{n}$ and $|(k_{21}, k_{22})| = max(|k_{21}|, |k_{212}|) \le C\sqrt{n}$.

Finally, from Eq. (42) to compute C,

$$\left.\begin{aligned} max\{|k_1|, |k_2|\} \le \sqrt{1 + |\lambda|}\sqrt{n}, \\ max\{|k_{11}|, |k_{12}|\} \le \sqrt{1 + |\lambda_1|}\sqrt{n}, \\ max\{|k_{21}|, |k_{22}|\} \le \sqrt{1 + |\lambda_2|}\sqrt{n}. \end{aligned}\right\}$$

where $\lambda, \lambda_1, \lambda_2 \in [1, n-1]$.

Corollary 4.8: Let v_2, v_4 and v_6 be linear independent vectors such that vector v_2 is a shorter vector between $(r_m, -t_m)$ and $(r_{m+2}, -t_{m+2})$, v_4 is shorter vector between $(r_{m_1}, -t_{m_1})$ and $(r_{(m+2)_1}, -t_{(m+2)_1})$ and v_6 is shorter vector between $(r_{m_2}, -t_{m_2})$ and $(r_{(m+2)_2}, -t_{(m+2)_2})$. If these vectors satisfy the following relations,

$$\left.\begin{aligned} min\{|(r_m, -t_m)|, |(r_{m+2}, -t_{m+2})|\} \le C\sqrt{n}, \\ min\{|(r_{m_j}, -t_{m_j})|, |(r_{(m+2)_j}, -t_{(m+2)_j})|\} \le C\sqrt{n}. \end{aligned}\right\}$$

for $j = 1, 2,$ then, the admissible value for C is

$$C = \begin{cases} \sqrt{1 + |w| + z}, \text{ for GLV decomposit ion}, \\ \sqrt{1 + |w_j| + z_j}, \text{ for ISD sub - decomposit ion} \end{cases} \quad (48)$$

for $j = 1, 2.$ In particular, any multiple kP can be decomposed as in Eq. (10) with

$$\left.\begin{aligned} max\{|k_1|, |k_2|\} \le \sqrt{1 + |w| + z}\sqrt{n}, \\ max\{|k_{11}|, |k_{12}|\} \le \sqrt{1 + |w_1| + z_1}\sqrt{n}, \\ max\{|k_{21}|, |k_{22}|\} \le \sqrt{1 + |w_2| + z_2}\sqrt{n}. \end{aligned}\right\} \quad (49)$$

where, w, z, w_j *and* z_j *with* $j = 1, 2$ are small fixed integers.

Proof:

The proof is similar to that used to prove the general case in Theorem (4.7).

5. Conclusions

This paper introduces an accurate analysis of the ISD method that optimizes and proves upper bounds of the kernel vectors on the ISD reduction map. These bounds determine the values of C that are greater than 1 ($C = \sqrt{1 + |\lambda_j|}$ where $\lambda_j \in [1, n-1]$ that is for endomorphism rings $End(E)$ over Z or $C = \sqrt{1 + |w_j| + z_j}$ with w_j and z_j as small fixed integers for the endomorphism rings $End(E)$ over an imaginary quadratic field Q[$\sqrt{D}$]). Analytical results proved embedding $End(E)$ into Z and $End(E)$ into an imaginary quadratic field Q[$\sqrt{D}$], with D discriminant of a quadratic characteristic polynomial. The new improved value of $C = \sqrt{1 + |\lambda_j|}$ in upper bound of ISD computation method that uses endomorphism rings $End(E)$ over Z increases the percentage of successful computation kP within the interval $[1, n-1]$ compared to the value of $C = \sqrt{1 + |w_j| + z_j}$ in upper bound of ISD

computation method that uses endomorphism rings $End(E)$ over imaginary quadratic field Q[$\sqrt{D}$].

References

[1] Sica, F., Ciet, M., and Quisquater, J. J. 2003. "Analysis of the Gallant-Lambert-Vanstone Method Based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves." In *Proceedings of the Selected Areas in Cryptography*, 21-36.

[2] Gallant, R., Lambert, R., and Vanstone, L. 2001. "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms." In *Proceedings of the Advances in Cryptology*, 190-200.

[3] Park, Y. H., Jeong, S., Kim, C. H., and Lim, J. 2002. "An Alternate Decomposition of an Integer for Faster Point Multiplication on Certain Elliptic Curves." *Public Key Cryptography, Springer*, 323-34.

[4] Washington, L. C. 2008. *Elliptic Curves: Number Theory and Cryptography*. USA: Chapman & Hall/CRC.

[5] Hoffstein, J., Pipher, J., and Silverman, J. H. 2008. *An Introduction to Mathematical Cryptograph*. USA: Springer.

[6] Ajeena, R. K. K., 2015. "Integer Sub-decomposition Method for Elliptic Curve Scalar Multiplication." Ph.D. thesis, University Sains Malaysia, Malaysia.

[7] Ajeena, R. K. K., and Kamarulhaili, H. 2014. "Point Multiplication Using Integer Sub-decomposition for Elliptic Curve Cryptography." *Journal of Applied Mathematics & Information Sciences* 8 (2): 517-25.

[8] Ajeena, R. K. K., and Kamarulhaili, H. 2014. "Comparison Studies on Integer Decomposition Method for Elliptic Scalar Multiplication." *Journal of Advanced Science Letters* 20 (2): 526-30.

[9] Kim, D., and Lim, S. 2003. "Integer Decomposition for Fast Scalar Multiplication on Elliptic Curves." In *Proceedings of the Selected Areas in Cryptography,* 13-20.

[10] Hankerson, D., Menezes A. J., and Vanstone, S. 2004. *Guide to Elliptic Curve Cryptography*. USA: Verlag.

[11] Ajeena, R. K. K., and Kamarulhaili, H. 2014. "A new Elliptic Scalar Multiplication Method Using a Generalized Extended Euclidean Algorithm." In *Proceedings of the 3rd International Conference on Computer Engineering & Mathematical Sciences,* 203-14.