Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 6 (2015), pp. 4035-4046

http://www.ripublication.com

# On The Upper Bounds of the Sub Decomposition values of the Scalar $k$ for Elliptic Scalar Multiplication

**Siti Noor Farwina Mohamad Anwar Antony & Hailiza Kamarulhaili**

*School of Mathematical Sciences, Universiti Sains Malaysia, 11800, Penang, Malaysia*
sitinoorfarwina@yahoo.com & hailiza@usm.my

**Abstract**

In this paper, upper bounds of the decomposition values for the scalar $k$ in elliptic scalar multiplication are computed. Namely, the scalar $k$ of the scalar multiplication $kP$ of a point $P$ which has a large prime order $n$ lying on elliptic curve group $E(F_p)$ over a finite prime field $F_p$. Method used to compute the decomposition values of the scalar $k$ is called the shortest lattice method and implemented in the integer sub decomposition (ISD) approach. The conception of the ISD approach depends on the sub-decomposition of the scalar $k$ to compute the scalar multiplication $kP$ which uses efficiently computable endomorphisms $\psi_1, \psi_2$ and $\psi_3$ of elliptic curve $E$ over $F_p$. The ISD sub-decomposition can be defined by

$$kP = k_{11}P + k_{12}\psi_2(P) + k_{21}(P) + k_{22}\psi_3(P),$$

for $\max\{|k_1|, |k_2|\} \geq \sqrt{n}$ and $\max\{|k_{11}|, |k_{12}|, |k_{21}|, |k_{22}|\} \leq C\sqrt{n}$

for some explicit constant $C > 0$. The integers $k_1, k_2, k_{11}, k_{21}, k_{21}, k_{22}$ are the decomposition values of the scalar $k$.

**Keywords:** Elliptic curve cryptography; integer decomposition method; Efficient computable endomorphisms; Integer sub-decomposition (ISD) method.

## INTRODUCTION

Scalar multiplication plays an important role in elliptic curve cryptosystem and consumes most of the cryptographic operations and costs. Thus, many methods have been developed to reduce costs in computing scalar multiplication on elliptic curves.

One of the latest development is the method called the GLV(Gallant, Lambert & Vanstone)[2] which was introduced in 2001, and since then, several GLV extensions and alternative have been developed such as in [3,4,5] and the modification of GLV which is known as the Integer Sub Decomposition(ISD) method by Ruma & Kamarulhaili [5,6,7,8,9,10]. Ruma & Kamarulhaili had proposed slightly a different method of decomposition from the previous techniques as the decomposition of the scalar $k$ was performed separately. The initial decomposition is in two dimensions and if the decomposition scalars still exceeded certain limit of upper bounds, they are then further decomposed.

The decompositions of the scalar $k$ help to reduce the cost of computing point on elliptic curves on larger field which are represented by $kP$. The GLV and the ISD methods also help to accelerate the multiplication computations $kP$. Both the GLV and the ISD used efficient endomorphism to decompose the scalar $k$ in the scalar multiplication $kP$ on the elliptic curve into two scalar multiplications, where $P$ is a point on the curve. The bit length of the original scalar $k$ has also been divided into two which means the bit-length of the decomposed scalars is half of the original length bits. Hence, this method reduced the cost of computing into halved, and accelerated the computation by 50%.

The decomposed scalars, $k_1$ and $k_2$ are expected to fall between $-\sqrt{n}$ and $\sqrt{n}$ for a large prime $n$. The initial generator vectors $\{v_1, v_2\}$ are the kernel of the homomorphism $T$ where $T : \square \times \square \rightarrow \square / n$ [2,3,4]. In the ISD method, for the initial decomposition values, $k_1, k_2$ which does not fall within the required range, further sub decomposition process has to be done on these values [5,6]. It is very important to keep all the decomposed values fall within the required range as we wanted all the scalars to be short. Shorter length of scalars required less costs and gives effective and efficient multiplication operations. In this paper, we attempt to obtain the upper bounds of all the decomposed scalars in the ISD method. This paper is organized as follows: Section 2 gives some overview of decomposition method used both in GLV and ISD methods. Section 3 provides main results on the upper bounds of the decomposition of scalar $k$ in ISD method. The proofs are divided into two cases as we have to consider two vectors and choose the shorter one. Section 4 presents the conclusions.

## 2.0 DECOMPOSITION OF THE SCALAR $k$ IN ELLIPTIC POINT MULTIPLICATION

In this section we revisit the decomposition method introduced earlier by GLV [2] and also adopted in the ISD method [5,6,7]. Supposed $E$ be an elliptic curve where $E : y^2 = x^3 + ax + b \pmod{p}$ which is defined over prime field $F_p$ and let $P = (x, y)$ be a point lies on $E$. The order of $P$ is a prime number $n$. In elliptic curve cryptography, the public key $Q = kP$ is an elliptic point multiplication, where the scalar $k$ is a secret key chosen from the interval, $[1, n-1]$. The ISD method appears to be a complement of the GLV method as those decomposed scalars that does not fall within the required

range are then sub decomposed into smaller scalars so that they would fall within the range. At first, the scalar $k$ is decomposed into the scalar $k_1$ and $k_2$ such that $\max\{|k_1|, |k_2|\} < \sqrt{n}$. However, in most cases this condition is not being satisfied. As a complement to this, the ISD method is proposed, where further decomposition is performed on those scalars $k_1$ and $k_2$, into smaller values that stays within the range of $-\sqrt{n}$ and $\sqrt{n}$. The decompositions involved the shortest vector problem. That is to find the shortest vector $v_1$ and $v_2$ such that it belongs to the kernel $T$, in other words the transformation $T(v_1) = 0$ and $T(v_2) = 0$. To generate the component of generating vectors, the extended Euclidean algorithm [4] is used. The transformation, $T : (x, y) \to x + \lambda y$ maps the vector $(x, y)$ into an integer $(x + \lambda y) \bmod n$. The decomposition process applied the extended Euclidean Algorithm on the positive integers $n, \lambda$ to produce a sequence of relations $s_i n + t_i \lambda = r_i$ and it also follows the Bezout's Identity where the $\gcd(n, \lambda) = s_i n + t_i \lambda = 1$, since $n, \lambda$ are relatively prime. The short vector $v_1 = (r_{m+1}, -t_{m+1})$ is chosen, where $m$ is the largest integer for which $r_m > \sqrt{n}$. The vector $v_2$ is chosen between $(r_{m+2}, -t_{m+2})$ and $(r_m, -t_m)$, the vector which has the smaller norm. For further details about the decomposition method one can refer to [2,3,4].

## 3.0 MAIN RESULTS

Before we discuss the main results, we need Lemma 1 to start generating the sequence, $r_i, s_i, t_i$, which are needed to obtain the generator vectors for decomposition operations in both the GLV and the ISD method. The following lemma gives important properties of the generator vectors components and the sequence $r_i = s_i n + t_i \lambda_1$. The ISD method requires several decomposition processes. In the first stage, the scalar $k$ is decomposed into $k_1$ and $k_2$, which involved the first generation of the sequence $r_i = s_i n + t_i \lambda_1$. In the second stage, $k_1$ and $k_2$ are then sub decomposed into the scalars $k_{11}, k_{12}, k_{21}, k_{22}$. This process involved recalling of the extended algorithms for which it yields new variables which are the derivation from the sequence $r_i = s_i n + t_i \lambda_1$ where this time the extended algorithms are executed on the two pairs $(n, \lambda_2)$ and $(n, \lambda_3)$ for $\lambda_2, \lambda_3 \in [1, n-1]$ which produces the variables, $r', s', t'$ and $r'', s'', t''$ respectively.

**Lemma 1:** [Gallant et al, 2001]

Let $s_i, r_i, t_i$ be the sequence of variable generated from the extended Euclidean algorithm for two positive integers $n$ and $\lambda_1$ such that $\gcd(n, \lambda_1) = 1$ and $\lambda_1 < n$. Then the following properties are true.

i. $r_i > r_{i+1} > 0$ for all $i \geq 0$.

ii. $|s_i| < |s_{i+1}|$ for all $i \geq 1$.

iii. $|t_i| < |t_{i+1}|$ for all $i \geq 0$.

iv. $r_{i-1}|t_i| + r_i|t_{i-1}| = n$ for all $i \geq 1$.

**Remarks**: Take note that the important assumption in the decomposition operation is that, $m$ is the greatest index for which the following relations are satisfied.

i. $r_m \geq \sqrt{n}$

ii. $|t_{m+1}| < \sqrt{n}$

iii. $|r_{m+1}| < \sqrt{n}$

The following theorem described the upper bound of the decomposition of scalar $k$.

**Theorem 1:** Supposed $E$ be an elliptic curve where $E: y^2 = x^3 + ax + b \pmod p$ which is defined over prime field $F_p$ and let $P = (x, y)$ be a point lies on $E$. Assume that $\lambda_1$ is any random integer selected from $[1, n-1]$ such that $\gcd(n, \lambda_1) = 1$. Then for the decomposition of scalar $k$ into two integer scalar $k_1$ and $k_2$ such that $k \equiv (k_1 + k_2\lambda_1) \bmod n$, we have $|k_1| \leq |n - 1 - A|$ and $|k_2| \leq \sqrt{n}D$ where

$$A = \begin{cases} t_{m+2} - t_{m+1}; \text{ when } \sqrt{{r_{m+2}}^2 + (t_{m+2})^2} \leq \sqrt{{r_m}^2 + (t_m)^2} \\ t_m - t_{m+1}; \text{ when } \sqrt{{r_m}^2 + (t_m)^2} \leq \sqrt{{r_{m+2}}^2 + (t_{m+2})^2} \end{cases},$$

and

$$D = \begin{cases} 2|t_{m+2}|; \text{ when } \sqrt{{r_{m+2}}^2 + (t_{m+2})^2} \leq \sqrt{{r_m}^2 + (t_m)^2} \\ |t_m| + |-t_{m+1}|; \text{ when } \sqrt{{r_m}^2 + (t_m)^2} \leq \sqrt{{r_{m+2}}^2 + (t_{m+2})^2} \end{cases}.$$

**Proof:** Suppose $v_1$ and $v_2$ are vectors which are obtained from the extended Euclidean Algorithm where $v_1 = (r_{m+1}, -t_{m+1})$ and $v_2$ is the shortest vector between $(r_m, -t_m)$ and $(r_{m+2}, -t_{m+2})$. The extended Euclidean algorithm generates the following sequence of relations as follows.

$$s_i n + t_i \lambda_1 = r_i \text{ for } i = 0, 1, \ldots, m, m+1, \ldots, z-1 \text{ where } z > m$$

where $m$ is the greatest index such that $r_m \geq \sqrt{n}$. Let vector $v_1, v_2, v = \square v_1 + \square v_2$ be linearly independent vectors and $T: \square \times \square \to \square / n$, such that we have $(k, 0) = \beta_1 v_1 + \beta_2 v_2$ [2]. Since the vector $v_1$ and $v_2$ are chosen from shortest vector, we divide the problem into two cases:

**Case 1:** $\sqrt{{r_{m+2}}^2 + (t_{m+2})^2} \leq \sqrt{{r_m}^2 + (t_m)^2}$

Firstly, we need to compute the scalar $\beta_1$ and $\beta_2$ for the integer lattice generated by $v_1$ and $v_2$ which is closed to $(k, 0)$, written as $(k, 0) = \beta_1 v_1 + \beta_2 v_2$ [4] where $\beta_1 = \frac{t_{m+2}}{n} k$

and $\beta_2 = -\frac{t_{m+1}}{n}k$. Then, rounded off the value of $\beta_1$ and $\beta_2$ to nearest integer to get the value for $c_1$ and $c_2$ where $c_1 = \lfloor \beta_1 \rceil$ and $c_2 = \lfloor \beta_2 \rceil$ which being used in the integer lattice generated by $v_1$ and $v_2$ which is closed to $v$, written as $v = c_1 v_1 + c_2 v_2$ [4]. Lastly, we need to find the short vector $u$ where $u = (k,0) - v$ and $T(u) = k$ which the vector $u$ returns the value for decomposed scalar $k_1$ and $k_2$.

$$\begin{aligned} u &= (k,0) - v \\ &= (k,0) - (c_1 v_1 + c_2 v_2) \\ &= (k,0) - \left(c_1(r_{m+1}, -t_{m+1}) + c_2(r_{m+2}, -t_{m+2})\right) \\ &= (k - c_1 r_{m+1} - c_2 r_{m+2}, c_1 t_{m+1} + c_2 t_{m+2}) = (k_1, k_2) \end{aligned}$$

From the assumption $|r_{m+1}| < \sqrt{n}$ and from Lemma 1, $1 \le r_{m+2} < r_{m+1}$, we now compute the upper bound for $k_1$.

$$\begin{aligned} k_1 &= k - (c_1 r_{m+1} + c_2 r_{m+2}) \\ &\le n - 1 - r_{m+2}(c_1 + c_2) \le n - 1 - (c_1 + c_2). \end{aligned}$$

Since, $\beta_1 = \frac{t_{m+2}}{n}k$ and $\beta_2 = -\frac{t_{m+1}}{n}k$ and $k \in [1, n-1] \Rightarrow k \le n$, then we have

$$\lim_{k \to n} \beta_1 = \lim_{k \to n} \frac{t_{m+2}}{n} k = t_{m+2},$$

and,

$$\lim_{k \to n} \beta_2 = \lim_{k \to n} -\frac{t_{m+1}}{n} k = -t_{m+1}$$

Thus, the upper bound for $|k_1|$ is $|n - 1 - (t_{m+2} - t_{m+1})|$.

Next, we calculate the upper bound for $k_2$. Again, from the Lemma, it shows that $|t_{m+1}| < \sqrt{n}$, $|t_{m+1}| < |t_{m+2}|$, and thus we have the following.

$$\begin{aligned} |k_2| &= |c_1 t_{m+1} + c_2 t_{m+2}| \end{aligned}$$

And from Lemma 1, we have

$$\begin{aligned} |k_2| &\le |t_{m+2}||t_{m+1}| + |-t_{m+1}||t_{m+2}| \\ &\le \sqrt{n}(2|t_{m+2}|) \end{aligned}$$

Finally, the upper bound for $|k_2|$ in this case when we choose $v_2 = (r_{m+2}, -t_{m+2})$, is $\sqrt{n}(2|t_{m+2}|)$. ▪

**Case 2:** $\sqrt{r_m{}^2 + (-t_m)^2} \le \sqrt{r_{m+2}{}^2 + (-t_{m+2})^2}$

Now, we compute the scalar $\beta_1$ and $\beta_2$ where $\beta_1 = \frac{t_m}{n}k$ and $\beta_2 = -\frac{t_{m+1}}{n}k$. Then, we rounded off the value of $\beta_1$ and $\beta_2$ to get the value for $c_1$ and $c_2$ where $c_1 = \lfloor \beta_1 \rceil$ and $c_2 = \lfloor \beta_2 \rceil$ for the integer lattice generated by $v_1$ and $v_2$ which is closed to $v$, written

as $v = c_1 v_1 + c_2 v_2$ [4]. Lastly, we need to find the short vector $u$ where $u = (k,0) - v$ and $T(u) = k$ which the vector $u$ returns the value for decomposed scalar $k_1$ and $k_2$.

$$\begin{aligned} u &= (k,0) - v \\ &= (k,0) - (c_1 v_1 + c_2 v_2) \\ &= (k,0) - \left(c_1(r_{m+1}, -t_{m+1}) + c_2(r_m, -t_m)\right) \\ &= (k - c_1 r_{m+1} - c_2 r_m, c_1 t_{m+1} + c_2 t_m) = (k_1, k_2) \end{aligned}$$

From Lemma 1, we have $1 \geq r_m \geq \sqrt{n} \geq r_{m+1}$. This in turn gives the following.

$$\begin{aligned} k_1 &= k - (c_1 r_{m+1} + c_2 r_m) \\ &\leq n - 1 - r_{m+1}(c_1 + c_2). \\ |k_1| &\leq |n - 1 - (c_1 + c_2)| \end{aligned}$$

Since, $\beta_1 = \frac{t_m}{n} k$ and $\beta_2 = -\frac{t_{m+1}}{n} k$ and $k \in [1, n-1] \Rightarrow k \leq n$, we then have the following.

$$\lim_{k \to n} \beta_1 = \lim_{k \to n} \frac{t_m}{n} k = t_m,$$

and,

$$\lim_{k \to n} \beta_2 = \lim_{k \to n} -\frac{t_{m+1}}{n} k = -t_{m+1}.$$

Hence, for this case, we have the upper bound for $|k_1|$ as $|n - 1 - (t_m - t_{m+1})|$.

As for the upper bound for $k_2$, we now have the following arguments.

$$|k_2| = |c_1 t_{m+1} + c_2 t_m|.$$

From Lemma 1, $|t_{m+1}| < \sqrt{n}$ and since $|t_m| < |t_{m+1}|$, we have the following

$$\begin{aligned} |k_2| &\leq |c_1||t_{m+1}| + |c_2||t_m| \\ &\leq |t_{m+1}|(|c_1| + |c_2|) \\ &\leq \sqrt{n}(|t_m| + |-t_{m+1}|). \end{aligned}$$

So, we have the upper bound for $|k_2|$ when we choose $v_2 = (r_m, -t_m)$, as $\sqrt{n}(|t_m| + |-t_{m+1}|)$. ▪

**Theorem 2:** Supposed $E$ be an elliptic curve where $E : y^2 = x^3 + ax + b \pmod p$ which is defined over prime field $F_p$ and let $P = (x, y)$ be a point lies on $E$. Assume that $\lambda_2$ is any random integer selected from $[1, n-1]$ such that $\gcd(n, \lambda_2) = 1$. And, we have $k_1 \leq |n - 1 - A|$, where $A$ as defined in Theorem 1. Then for sub decomposition of scalar $k_1$ into $k_{11}, k_{12}$ such that $k_1 \equiv (k_{11} + k_{12}\lambda_2) \bmod n$, we have $|k_{11}| \leq \left|n - 1 - \left(A + A'\right)\right|$ and $|k_{12}| \leq \sqrt{n} D'$ where

$$A' = \begin{cases} t_{m+2}' - t_{m+1}' \text{ when } \sqrt{\left(r_{m+2}'\right)^2 + \left(-t_{m+2}'\right)^2} \le \sqrt{\left(r_m'\right)^2 + \left(-t_m'\right)^2} \\ t_m' - t_{m+1}' \text{ when } \sqrt{\left(r_m'\right)^2 + \left(t_m'\right)^2} \le \sqrt{\left(r_{m+2}'\right)^2 + \left(t_{m+2}'\right)^2} \end{cases}$$

And

$$D' = \begin{cases} 2\left|t_{m+2}'\right| \text{ when} \sqrt{\left(r_{m+2}'\right)^2 + \left(-t_{m+2}'\right)^2} \le \sqrt{\left(r_m'\right)^2 + \left(-t_m'\right)^2} \\ \left|t_m'\right| + \left|-t_{m+1}'\right| \text{ when } \sqrt{\left(r_m'\right)^2 + \left(t_m'\right)^2} \le \sqrt{\left(r_{m+2}'\right)^2 + \left(t_{m+2}'\right)^2} \end{cases}$$

**Proof:** Suppose $v_3$ and $v_4$ are vectors which are obtained by applying the extended Euclidean Algorithm on $n$ and $\lambda_2$, where $v_3 = \left(r_{m+1}', -t_{m+1}'\right)$ and $v_4$ is the shortest vector between $\left(r_m', -t_m'\right)$ and $\left(r_{m+2}', -t_{m+2}'\right)$. Again, the extended Euclidean algorithm is used to obtain the following sequence of equations, where now, we choose $\lambda_2$ such that $(n, \lambda_2) = 1$.

$$s_i' n + t_i' \lambda_2 = r_i' \text{ for } i = 0,1,\ldots,m,m+1,\ldots,z-1 \text{ where } z > m$$

where $m$ is the greatest index such that $r_m' \ge \sqrt{n}$. Let vector $v_3, v_4, v' = \square v_3 + \square v_4$ be linearly independent vectors and $T : \square \times \square \to \square / n$, then we have $(k_1, 0) = \beta_3 v_3 + \beta_4 v_4$. Since the vector $v_3$ and $v_4$ are chosen from shortest vector, we divide the problem into two cases:

**Case 1:** $\sqrt{\left(r_{m+2}'\right)^2 + \left(-t_{m+2}'\right)^2} \le \sqrt{\left(r_m'\right)^2 + \left(-t_m'\right)^2}$

Firstly, we need to compute the scalar $\beta_3$ and $\beta_4$ for the integer lattice generated by $v_3$ and $v_4$ which is closed to $(k_1, 0)$, written as $(k_1, 0) = \beta_3 v_3 + \beta_4 v_4$ [4] where $\beta_3 = \frac{t_{m+2}'}{n} k_1$ and $\beta_4 = -\frac{t_{m+1}'}{n} k_1$. Then, we rounded off the value of $\beta_3$ and $\beta_4$ to get the value for $c_3$ and $c_4$ where $c_3 = \lfloor \beta_3 \rceil$ and $c_4 = \lfloor \beta_4 \rceil$ for the integer lattice generated by $v_3$ and $v_4$ which is closed to $v'$, written as $v' = c_3 v_3 + c_4 v_4$ [4]. Lastly, we need to find the short vector $u'$ where $u' = (k_1, 0) - v'$ and $T(u') = k_1$ which the vector $u'$ returns the value for decomposed scalar $k_{11}$ and $k_{12}$.

$$\begin{aligned} u' &= (k_1, 0) - v' \\ &= (k_1, 0) - (c_3 v_3 + c_4 v_4) \\ &= (k_1, 0) - \left(c_3\left(r_{m+1}', -t_{m+1}'\right) + c_4\left(r_{m+2}', -t_{m+2}'\right)\right) \\ &= \left(k_1 - c_3 r_{m+1}' - c_4 r_{m+2}', c_3 t_{m+1}' + c_4 t_{m+2}'\right) = (k_{11}, k_{12}) \end{aligned}$$

$$\begin{aligned} k_{11} &= k_1 - \left(c_3 r_{m+1}{}' + c_4 r_{m+2}{}'\right) \\ &\leq (n-1-A) - r_{m+2}{}'(c_3 + c_4). \end{aligned}$$

Similar as the previous case for $k_1$, we have the following arguments.

Since, $\beta_3 = \frac{t_{m+2}{}'}{n} k_1$ and $\beta_4 = -\frac{t_{m+1}{}'}{n} k_1$ and $k_1 \in [1, n-1] \Rightarrow k_1 \leq n$, we have

$$\lim_{k_1 \to n} \beta_3 = \lim_{k_1 \to n} \frac{t_{m+2}{}'}{n} k_1 = t_{m+2}{}',$$

and

$$\lim_{k_1 \to n} \beta_4 = \lim_{k_1 \to n} -\frac{t_{m+1}{}'}{n} k_1 = -t_{m+1}{}'.$$

Finally, we have the upper bound for $|k_{11}|$ as $\left|n-1-A-\left(t_{m+2}{}' - t_{m+1}{}'\right)\right|$.

As for the upper bound for $k_{12}$, we have the following.

$$\begin{aligned} |k_{12}| &= \left|c_3 t_{m+1}{}' + c_4 t_{m+2}{}'\right| \\ &\leq \left|t_{m+2}{}'\right|\left|t_{m+1}{}'\right| + \left|-t_{m+1}{}'\right|\left|t_{m+2}{}'\right| \\ &= \left|t_{m+1}{}'\right|\left(\left|t_{m+2}{}'\right| + \left|t_{m+2}{}'\right|\right) \\ &\leq \sqrt{n}\left(2\left|t_{m+2}{}'\right|\right). \end{aligned}$$

Thus, the upper bound for $|k_{12}|$ in this case when we choose $v_4 = \left(r_{m+2}{}', -t_{m+2}{}'\right)$ is $\sqrt{n}\left(\left|-t_{m+1}{}'\right| + \left|t_{m+2}{}'\right|\right)$. ▪

**Case 2:** $\sqrt{\left(r_m{}'\right)^2 + \left(t_m{}'\right)^2} \leq \sqrt{\left(r_{m+2}{}'\right)^2 + \left(t_{m+2}{}'\right)^2}$

Compute the scalar $\beta_3$ and $\beta_4$ for the integer lattice generated by $v_3$ and $v_4$ which is closed to $(k_1, 0)$, written as $(k_1, 0) = \beta_3 v_3 + \beta_4 v_4$ [4] where $\beta_3 = \frac{t_m{}'}{n} k_1$ and $\beta_4 = -\frac{t_{m+1}{}'}{n} k_1$. Then, we rounded off the value of $\beta_3$ and $\beta_4$ to get the value for $c_3$ and $c_4$ where $c_3 = \lfloor \beta_3 \rceil$ and $c_4 = \lfloor \beta_4 \rceil$ for the integer lattice generated by $v_3$ and $v_4$ which is closed to $v'$, written as $v' = c_3 v_3 + c_4 v_4$ [4]. Lastly, we need to find the short vector $u'$ where $u' = (k_1, 0) - v'$ and $T(u') = k_1$ which the vector returns the value for decomposed scalar $k_{11}$ and $k_{12}$.

$$\begin{aligned} u' &= (k_1, 0) - v' \\ &= (k_1, 0) - (c_3 v_3 + c_4 v_4) \\ &= (k_1, 0) - \left(c_3\left(r_{m+1}{}', -t_{m+1}{}'\right) + c_4\left(r_m{}', -t_m{}'\right)\right) \end{aligned}$$

$$= \left(k_1 - c_3 r_{m+1}{}' - c_4 r_m{}', c_3 t_{m+1}{}' + c_4 t_m{}'\right) = (k_{11}, k_{12})$$

$$k_{11} = k_1 - \left(c_3 r_{m+1}{}' + c_4 r_m{}'\right)$$

$$\leq n - 1 - A - r_{m+1}{}'(c_3 + c_4).$$

Similarly as in the previous method, taking the limit of $c_3$ and $c_4$, we then obtain the upper bound for $|k_{11}|$ as $\left|n-1-A-\left(t_m{}' - t_{m+1}{}'\right)\right|$. Next, repeating the method in the proof of Theorem 1, we obtained the upper bound for $|k_{12}|$ in this case when we choose $v_4 = \left(r_m{}', -t_m{}'\right)$, as $\sqrt{n}\left(\left|t_m{}'\right| + \left|-t_{m+1}{}'\right|\right)$. ▪

**Theorem 3:** Supposed $E$ be an elliptic curve where $E: y^2 = x^3 + ax + b \pmod p$ which is defined over prime field $F_p$ and let $P = (x, y)$ be a point lies on $E$. Assume that $\lambda_3$ is any random integer selected from $[1, n-1]$ such that $\gcd(n, \lambda_3) = 1$. And, we have $k_2 \leq \sqrt{n}\lambda_1 D$, where $D$ is defined as in Theorem 1. Then the sub decomposition of scalar $k_2$ into the scalar $k_{21}$ and $k_{22}$ such that $k_2\lambda_1 \equiv (k_{21} + k_{22}\lambda_3) \bmod n$, we have $|k_{21}| \leq \sqrt{n}\left|D\lambda_1 - (A'')\right|$ and $|k_{22}| \leq \sqrt{n} D''$ where

$$A'' = \begin{cases} t_{m+2}{}'' - t_{m+1}{}'' \text{ when } \sqrt{\left(r_{m+2}{}''\right)^2 + \left(t_{m+2}{}''\right)^2} \leq \sqrt{\left(r_m{}''\right)^2 + \left(t_m{}''\right)^2} \\ t_m{}'' - t_{m+1}{}'' \text{ when } \sqrt{\left(r_m{}''\right)^2 + \left(t_m{}''\right)^2} \leq \sqrt{\left(r_{m+2}{}''\right)^2 + \left(t_{m+2}{}''\right)^2} \end{cases}$$

And

$$D'' = \begin{cases} 2\left|t_{m+2}{}''\right| \text{ when } \sqrt{\left(r_{m+2}{}''\right)^2 + \left(t_{m+2}{}''\right)^2} \leq \sqrt{\left(r_m{}''\right)^2 + \left(t_m{}''\right)^2} \\ \left|t_m{}''\right| + \left|-t_{m+1}{}''\right| \text{ when } \sqrt{\left(r_m{}''\right)^2 + \left(t_m{}''\right)^2} \leq \sqrt{\left(r_{m+2}{}''\right)^2 + \left(t_{m+2}{}''\right)^2} \end{cases}$$

**Proof:** Suppose $v_5$ and $v_6$ are vectors which are obtained from the execution of the extended Euclidean Algorithm on the two positive integers, $n$ and $\lambda_3$ where $v_5 = \left(r_{m+1}{}'', -t_{m+1}{}''\right)$ and $v_6$ is the shortest vector between $\left(r_m{}'', -t_m{}''\right)$ and $\left(r_{m+2}{}'', -t_{m+2}{}''\right)$. The extended Euclidean algorithm is used to help generate the following sequence of relations below.

$$s_i{}'' n + t_i{}'' \lambda_3 = r_i{}'' \text{ for } i = 0, 1, \ldots, m, m+1, \ldots, z-1 \text{ where } z > m$$

where $m$ is the greatest index such that $r_m{}'' \geq \sqrt{n}$. Let vector $v_5, v_6, v'' = \square v_5 + \square v_6$ be linearly independent vectors and $T: \square \times \square \to \square / n$, such that we have $(k_2, 0) = \beta_5 v_5 + \beta_6 v_6$ [2]. Since the vector $v_5$ and $v_6$ are chosen from shortest vector, we again divide the problem into two cases:

**Case 1:** $\sqrt{\left(r_{m+2}''\right)^2+\left(t_{m+2}''\right)^2} \le \sqrt{\left(r_m''\right)^2+\left(t_m''\right)^2}$

As what we have done earlier, we need to compute the scalar $\beta_5$ and $\beta_6$ for the integer lattice generated by $v_5$ and $v_6$ which is closed to $(k_2,0)$, written as $(k_2,0)=\beta_5 v_5+\beta_6 v_6$ [4] where $\beta_5=\frac{t_{m+2}''}{n}k_2$ and $\beta_6=-\frac{t_{m+1}''}{n}k_2$. Then, we rounded off the value of $\beta_5$ and $\beta_6$ to get the value for $c_5$ and $c_6$ where $c_5=\lfloor \beta_5 \rceil$ and $c_6=\lfloor \beta_6 \rceil$ for the integer lattice generated by $v_5$ and $v_6$ which is closed to $v''$, written as $v''=c_5v_5+c_6v_6$ [4]. Lastly, we need to find the short vector $u''$ where $u''=(k_2\lambda_1,0)-v''$ and $T(u'')=k_2\lambda_1$ which the vector $u''$ returns the value for decomposed scalar $k_{21}$ and $k_{22}$.

$$\begin{aligned} u'' &= (k_2\lambda_1,0)-v'' \\ &= (k_2\lambda_1,0)-(c_5v_5+c_6v_6) \\ &= (k_2\lambda_1,0)-\left(c_5\left(r_{m+1}'',-t_{m+1}''\right)+c_6\left(r_{m+2}'',-t_{m+2}''\right)\right) \\ &= \left(k_2\lambda_1-c_5r_{m+1}''-c_6r_{m+2}'',c_5t_{m+1}''+c_6t_{m+2}''\right)=(k_{21},k_{22}) \end{aligned}$$

Similar assumption use here where by $\left|r_{m+1}''\right|<\sqrt{n}$ and from Lemma1, $1\le r_{m+2}''<r_{m+1}''\Rightarrow r_{m+2}''<\sqrt{n}$. Now we compute the upper bound for $k_{21}$.

$$k_{21} = k_2\lambda_1-\left(c_5r_{m+1}''+c_6r_{m+2}''\right).$$

Following the similar method as in the proof of Theorem 2, we then have the following.

$$\left|k_{21}\right|\le\sqrt{n}\left|D\lambda_1-\left(t_{m+2}''+\left(-t_{m+1}''\right)\right)\right|,$$

$$\left|k_{22}\right|\le\sqrt{n}\left(2\left|t_{m+2}''\right|\right).\ \blacksquare$$

**Case 2:** $\sqrt{\left(r_m''\right)^2+\left(t_m''\right)^2} \le \sqrt{\left(r_{m+2}''\right)^2+\left(t_{m+2}''\right)^2}$

Firstly, we need to compute the scalar $\beta_5$ and $\beta_6$ for the integer lattice generated by $v_5$ and $v_6$ which is closed to $(k_2\lambda_1,0)$, written as $(k_2\lambda_1,0)=\beta_5 v_5+\beta_6 v_6$ [4] where $\beta_5=\frac{t_{m+2}''}{n}k_2\lambda_1$ and $\beta_6=-\frac{t_{m+1}''}{n}k_2\lambda_1$. Then, we rounded off the value of $\beta_5$ and $\beta_6$ to get the value for $c_5$ and $c_6$ where $c_5=\lfloor \beta_5 \rceil$ and $c_6=\lfloor \beta_6 \rceil$ for the integer lattice generated by $v_5$ and $v_6$ which is closed to $v''$, written as $v''=c_5v_5+c_6v_6$ [4]. Lastly, we need to find the short vector $u''$ where $u''=(k_2\lambda_1,0)-v''$ and $T(u'')=k_2\lambda_1$ which the vector $u''$ returns the value for decomposed scalar $k_{21}$ and $k_{22}$.

$$\begin{aligned} u'' &= (k_2\lambda_1, 0) - v'' \\ &= (k_2\lambda_1, 0) - (c_5 v_5 + c_6 v_6) \\ &= (k_2\lambda_1, 0) - \left( c_5 \left( r_{m+1}'', -t_{m+1}'' \right) + c_6 \left( r_m'', -t_m'' \right) \right) \\ &= \left( k_2\lambda_1 - c_5 r_{m+1}'' - c_6 r_m'', c_5 t_{m+1}'' + c_6 t_m'' \right) = (k_{21}, k_{22}) \end{aligned}$$

Now, using the similar argument as in Theorem 2, we obtained the upper bound for $k_{21}$ as follows.

$$\begin{aligned} k_{21} &= k_2\lambda_1 - \left( c_5 r_{m+1}'' + c_6 r_m'' \right) \\ &\le \sqrt{n} D\lambda_1 - 1(c_5 + c_6). \end{aligned}$$

Repeating the same process as in the proof of Theorem 2, we have $|k_{21}| \le \left| \sqrt{n} D\lambda_1 - \left( t_m'' + \left( -t_{m+1}'' \right) \right) \right|$ and $|k_{22}| \le \sqrt{n} \left( \left| t_m'' \right| + \left| -t_{m+1}'' \right| \right)$. ▪

## 4.0 CONCLUSIONS

Integer Sub Decomposition or ISD method helps to accelerate point multiplications $kP$ on elliptic curves, which complement the GLV method in a way that it helps to produce the decomposition scalars that stays within the required range. The main application of this method is in the ECC (Elliptic Curve Cryptography) where the major operations rely very much on point multiplications. In this work, we managed to compute the upper bounds for all the decomposition scalars. These upper bounds are important to ensure the size of the scalars stay within the required range, so that point multiplications could be computed less costly. The required range here ideally means, the scalars should fall in the interval $\left[ -\sqrt{n}, \sqrt{n} \right]$. However, most cases in the GLV method produce decomposition scalars that fall outside this interval. Therefore, further decompositions are needed as what has been proposed in the ISD method [6]. Technically for each category of decomposition shown in this paper, is divided into two cases depending on the generator vectors, whichever is the smaller to ensure the shortness in length of the decomposition scalars produced. From the observation, the upper bounds for the decomposed scalars $k_{11,}, k_{12}, k_{21}$ and $k_{22}$ differ depending on the shortest vector $v_i$ and $v_{i+1}$ for $i = 1,3,5$ and from both cases we have proved that $\max\left\{ |k_{11}|, |k_{12}|, |k_{21}|, |k_{22}| \right\} \le C\sqrt{n},$ where $C > 0$. The value of $k_{11}$ depends on the value of $k_1$ and it is expected not to exceed the required upper bound, $C\sqrt{n}$ and, it is also expected that the value $A + A'$ is big so that $k_{11}$ is very much smaller than the value of $k_1$. Though $k_{11}$ does not obviously appeared to be bounded by $C\sqrt{n}$. We believed that by the way it is formulated, the value of $|k_{11}|$ has very high possibility not to

exceed $C\sqrt{n}$. However, this will be part of our future investigations. We also will look into a more refined and sharper upper bound for individual scalar.

**ACKNOWLEDGEMENTS**

The authors would like to express their gratitude to the Academic Staff Training Scheme (ASTS) which was funded by the Ministry of Higher Education and the Universiti Sains Malaysia and the FRGS Grant 203/PMATHS/6711320.

**REFERENCES**

[1] Hankerson, D., Menezes, A. and Vanstone, S., 2004, Guide to Elliptic Curve Cryptosystem, Springer.

[2] Gallant, R., Lambert, R. and Vanstone, S., 2001, "Faster point multiplication on elliptic curves with efficient endomorphisms, " in Advances in Cryptology—CRYPTO 2001, pp. 190-200.

[3] Longa, P. and Sica, F., 2012, "Four Dimensional Gallant-Lambert-Vanstone Scalar Multiplication," ASIACRYPT.

[4] Longa, P. and Sica, F., 2014, "Four Dimensional Gallant-Lambert-Vanstone Scalar Multiplication," Journal of Cryptology, 27(2), pp.248-283.

[5] Park, Y.H., Jeong, S., Kim, C.H. and Lim, J., 2002, "An Alternative Decomposition of an Integer for Faster Point Multiplication on certain Elliptic Curves," PKC 2002,LNCS 2274, pp.323-334.

[6] Ajeena, R.K. and Kamarulhaili, H., 2013, "Analysis on the Elliptic Scalar Multiplication using Integer Sub Decomposotion Method," International Journal of Pure and Applied Mathematics, Vol 87, no.1, pp.95-114.

[7] Ajeena, R.K. and Kamarulhaili, H., 2014, "GLV-ISD Method for Scalar Multiplication on Elliptic Curves," Australian Journal of Basic and Applied Sciences, 8(15), pp 1-14.

[8] Ajeena, R.K. and Kamarulhaili, H., 2014, "Two Dimensional Sub Decomposition Method for Point Multiplication on Elliptic Curves," Journal of Mathematical Sciences: Advances and Applications, Vol.25, pp43-56.

[9] Ajeena, R.K. and Kamarulhaili, H., 2014, "Point Multiplication using Integer Sub Decomposition for Elliptic Curve Cryptography," Journal of Applied Mathematics and Information Sciences, **8**, no.2, pp 517-525.

[10] Ajeena, R.K. and Kamarulhaili, H., 2014, "The Computational Complexity of Elliptic Curve Integer Sub Decomposition(ISD) Method," American Institute of Physics(AIP) Conference Proceedings, 1605,557.