International Journal of Cryptology Research 7(1): 1 - 15 (2017)

Scalar Decomposition Methods on Genus One Elliptic Curves

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

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

E-mail: sitinoorfarwina@yahoo.com
[*]*Corresponding author*

ABSTRACT

In this paper, we reviewed and revisited the extension scalar decomposition method of a well-known GLV method namely the GLS (Galbraith, Lin, and Scott) method, four-dimensional GLV (Gallant, Lambert and Vanstone) method and the ISD (Integer sub-decomposition) method which acted on genus one elliptic curves. We also discussed the comparison between the four-dimensional GLV method and the ISD method. Both methods used the lattice method and shortest vector problem to compute the decomposed scalars. Other than that, both method implement the Euclidean algorithm to obtain the required sequence to solve shortest vector problem. They also used the concept of efficiently computable endomorphism. However, in four-dimensional GLV method, two efficiently computable endomorphisms are being adopted, while ISD method adopted three fast endomorphisms. They also are defined over a different field where the four-dimensional GLV method being defined over quadratic extension field while ISD method defined over integer number field.

Keywords: Elliptic curve cryptography, Scalar Decomposition, Efficient computable endomorphisms, Frobenius endomorphism, Quadratic extension field.

1 INTRODUCTION

Supposed E be a genus one elliptic curve where

$$E : y^2 = x^3 + ax + b \ (\mathrm{mod}\, p), . \tag{1}$$

which is defined over prime field F_p and let $P, R \in E\left(F_p\right)$ .Two important operation in elliptic curve cryptography are point multiplication kP and point multiexponentiation $kP + lR$ (Sica et al., 2002). Supposed that point P form a subgroup in E with prime order n. And there exist a public key $Q = kP$ which is an elliptic point multiplication, where k is a secret key (scalar) chosen from the interval $[1, n-1]$. GLV method is an approach to speed up this elliptic curve point multiplication (Gallant et al., 2001). In GLV, the scalar k is decomposed into two scalars where the bit length of the decomposed scalars has reduced into half of its original length bits. Hence, this method able to accelerate the computation by 50%.

GLV proposed the decomposed scalar k_1 and k_2 to fall between $-\sqrt{n}$ and $\sqrt{n}$, however, they did not provide any proof. GLV method needs two GLV generator $\{v_1, v_2\}$ which contained in the kernel of the homomorphism T where $T : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n$. But since GLV is inefficient when dealing with a larger field, variants of approach being introduce to accelerate the computation on elliptic curve point multiplication (Hankerson et al., 2004) such as a GLS and four-dimensional GLV method. GLS method is an approach where they implement a different efficiently computable endomorphism, known as p-Frobenius endomorphism when dealing with a larger field of curves.

Later in 2012, Birkner et al. (2012) proposed a method which combined both GLV and GLS approach to solve the scalar multiplication where they decomposed the scalar k into four scalars. This approach is called as four-dimensional GLV method. This method has almost similar form with another method which has been proposed in 2014 to solve scalar multiplication when GLV condition is not fulfilled, which is when the decomposed values does not fall between $-\sqrt{n}$ and $\sqrt{n}$. This method is called as integer sub-decomposition (ISD) method. ISD helps to improve the successful computation of scalar multiplication on the elliptic curve. In this study, we compare four-dimensional GLV method and ISD method. Section 2 describes the GLV decomposition method. Section 3 describes the GLS method. Section

4 describes the four-dimensional GLV method. Section 5 describes the ISD method. Section 6 presents the comparison between four-dimensional GLV method and ISD method. And lastly, Section 7 provides the conclusions.

2 GLV METHOD

In GLV method, the scalar k is decomposed into two scalars k_1 and k_2 where $\max\{\,|k_1|\,,\ |k_2|\,\} \leq n$ where n denoted the order of the E. In order to find the decomposed scalar, first we need to find the generator vectors v_1 and v_2 using extended Euclidean Algorithm such that those vectors belong to the kernel T, in other words the transformation $T\,(v_1) = 0$ and $T\,(v_2) = 0$. The transformation T is defined as $T : (x_1, x_2) \mapsto x_1 + x_2\lambda\ (mod\, n)$. This GLV method used non-trivial endomorphism $\Phi : E \to E$ implying $\Phi(P) = \lambda P$ for some $\lambda \in [1, n-1]$ where λ is the root of the characteristic polynomial acting on Φ . The endomorphism is defined over quadratic extension field which makes the GLV method undergo complex multiplication. The characteristic polynomial for the endomorphism is given as $X^2 + rX + s$.

The extended Euclidean algorithm applied to n and λ produces a sequence of relations $s_i n + t_i \lambda = r_i$ and followed the Bezout's Identity where $\gcd\,(n, \lambda) = s_i n + t_i \lambda = 1$ since n, λ are relatively prime. From the algorithm, the shortest vector $v_1 = (r_{m+1}, -t_{m+1})$ is chosen where m is the largest integer for $r_m \geq \sqrt{n}$ and the second shortest vector v_2 is chosen between $(r_{m+2}, -t_{m+2})$ and $(r_m, -t_m)$ which ever has the smallest rectangle norm. Then, we need to find the vector $v = \mathbb{Z}v_1 + \mathbb{Z}v_2$ that is closed to $(k, 0) = \mathbb{Q}v_1 + \mathbb{Q}v_2$. And find the short vector u where $u = (k, 0) - v$ such that $T\,(u) = k$.

The general form for the decomposition of kP is given by

$$kP = k_1 P + k_2 \Phi\,(P) = k_1 P + k_2 \lambda P, \tag{2}$$

where $\max\left(|k_1|\,, |k_2|\right) \leq C\sqrt{n}$ for some explicit constant $C > 0$ .However,the original GLV fails to provide an explicit upper bound for k_1 and k_2. Later, some researchers were able to find the bounds on the decomposed scalars by relating it to the bound on v_1 and v_2 which can be obtained based on the characteristic polynomial of the endomorphism.

3 GLS METHOD

Since original GLV method only applicable on curves over F_p that has a small degree of endomorphism and limited applications on dimension two, Galbraith-Lin and Scott have proposed a method known as GLS method that can be applied on a larger class of curves. GLS method works on F_{p^2}, a larger class of curve instead of F_p since the point multiplication on F_{p^2} was faster than F_p . And instead of working with $E\left(F_{p^2}\right)$, GLS works with $E'\left(F_{p^2}\right)$, the quadratic twist of E. The degree of a twist depends on the automorphism acting on an elliptic curve. From the definition of automorphism, the only change of variable that preserving the equation of an elliptic curve with characteristic field $char\left(K\right) \neq 2, 3$ is given by $x = u_2 x', y = u^3 y'$ for some $u \in \bar{K}^*$, hence GLS obtained the quadratic twist as $E' : y^2 = x^3 + A'x + B'$ where $A' = Au^2$ and $B' = Bu^3$ such that u be a non-square in F_{p^2}.

GLS method implemented the endomorphism which arises from p-Frobenius map where their idea comes from Itjima et al. which has constructed an efficiently computable homomorphism on elliptic curve $E\left(F_{p^k}\right)$ arising from the Frobenius map on twist of E where

$$\Psi_d : E'\left(F_{p^k}\right) \xrightarrow{\psi_d} E\left(F_{p^{dk}}\right) \xrightarrow{\pi} E\left(F_{p^{dk}}\right) \xrightarrow{\psi_d^{-1}} E'\left(F_{p^k}\right)$$

where d denoted the degree of separable isogeny $\psi : E \to E'$ defined over F_{p^k} and π is the p-Frobenius map which maps E to itself. The following formulation gives the general formula of GLS method

$$kP = k_1 P + k_2 \Psi\left(P\right) = k_1 P + k_2 \mu P, \tag{3}$$

where $max\left\{\left|k_1\right|, \left|k_2\right|\right\} = O\left(\sqrt{n}\right)$ given $\Psi\left(P\right) = \mu\left(P\right)$.

Since GLS method works with Frobenius endomorphism which is defined over F_{p^2}, they have the following theorem.

Theorem 3.1. *Galbraith et al. (2009)*

Let $p > 3$ be a prime and let E be an ordinary elliptic curve with $p + 1 - t$ points. Let E' over F_{p^2} be the quadratic twist of $E\left(F_{p^2}\right)$ with $\#E'\left(F_{p^2}\right) = \left(p-1\right)^2 + t^2$. Let $\phi : E \to E'$ be the twisting isomorphism defined over

F_{p^4} and $\pi : E \rightarrow E$ be the p-power Frobenius map. Let $r | \# E' \left(F_{p^2} \right)$ be a prime such that $r > 2p$. Let $\psi = \phi \pi \phi^{-1}$. For $P \in E \left(F_{p^2} \right) [r]$, we have $\psi^2 (P) + P = \mathcal{O}_E$.

Proof. Ref.Galbraith et al. (2009) □

4 FOUR-DIMENSIONAL GLV METHOD

In this four-dimensional GLV method, GLV and GLS curves are combined to extend the GLV method into a higher dimension. This method exploiting the Frobenius endomorphism and GLV endomorphism to solve more curves over F_{p^2} (GLS curve). The general form of the four-dimensional GLV method is given by

$$kP = k_1 P + k_2 \Phi (P) + k_3 \Psi (P) + k_4 \Psi \Phi (P) \qquad (4)$$

where the $\Psi = Frob_p$, the p-Frobenius endomorphism of E/F_p such that $\Psi^m (P) = P$. Given that $\Psi = \psi Frob_p \psi^{-1}$ and $\Phi = \psi \phi \psi$ are defined over F_{p^2} where $\psi : E \mapsto E'$ an isomorphism defined over F_{p^4} and E' is a twist of degree d of E over F_{p^d}. Since they are working on F_{p^2}, they have the Frobenius endomorphism as $\Psi^2 + 1 = 0$ as given in Theorem 3.1. Meanwhile, the characteristic polynomial for Φ is given as $\Phi^2 + r\Phi + s = 0$. These endomorphisms are defined over quadratic extension field which involved complex multiplication. The complex multiplication are performed by λ and μ where $\Phi (P) = \lambda P$ and $\Psi (P) = \mu P$.

Since the four-dimensional GLV method involve lattice of dimension four, there are two methods in order to obtain the generator vectors which are Lenstra-Lenstra-Lovasz algorithm, (LLL algorithm) [1] and Cornacchia algorithm [2]. In LLL algorithm, they need to have the basis of kernel T which is given by $w_1 = (n, 0, 0, 0), w_2 = (-\lambda, 1, 0, 0), w_3 = (-\mu, 0, 1, 0)$ and $w_4 =$

[1] LLL algorithm used to obtain the shortest vector that is closed to orthogonal for lattice that has dimension greater than two. It transform a lattice into a nice lattice by implementing Gram-Schmidt method.

[2] Cornacchia algorithm was introduced in 1908 to solve non-linear Diophantine equation in form of $x^2 + dy^2 = p$ where $d > 0, p$ is prime.

$(\lambda\mu, -\mu, -\lambda, 1)$ where reduction map $T : \mathbb{Z}^4 \to \mathbb{Z}/n$ or $T : (x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\lambda + x_3\mu + x_4\lambda\mu$. In other words, they have $T(w_1) = T(w_2) = T(w_3) = T(w_4) \equiv 0 \ mod \ n$. Then, LLL algorithm is applied in order to obtain the reduced basis v_1, v_2, v_3, v_4 which are the generator vectors and later being used to find the short vector u such that $u = (k, 0, 0, 0) - v$ which corresponds to the decomposed scalar k_1, k_2, k_3, k_4 respectively.

The LLL-basis can be written in matrix form as $L = \begin{pmatrix} n & 0 & 0 & 0 \\ -\lambda & 1 & 0 & 0 \\ -\mu & 0 & 1 & 0 \\ \lambda\mu & -\mu & -\lambda & 1 \end{pmatrix}$ where $d(L) = n$ and by following the theorem below, they obtained the upper bound for the generator vector in four-dimensional GLV method. We provided proofs of the following theorems and lemmas obtained from Birkner et al. (2012) and Longa and Sica (2014). We have filled the gaps in these proofs for better understanding.

Theorem 4.1. *Cohen (1996)*

Let $v_1, \dots, v_n$ *be an LLL-reduced of a lattice L. Then,* $d(L) \le \prod_{i=1}^{n} |v_i| \le 2^{n(n-1)/4} d(L)$.

From the theorem above, we have $\prod_{i=1}^{n} |v_i| \le 2^3 d(L) = 8\left[\mathbb{Z}^4 : kerT\right] = 8n$ given the kernel T has index $\left[\mathbb{Z}^4 : kerT\right] = n$ inside $\mathbb{Z}^4$. To sharpen this bound, they have come out with a lemma, and a theorem correspond to the norm function of the four-dimensional GLV method.

Lemma 4.1. *Birkner et al. (2012), Longa and Sica (2014)*

Let $N : \mathbb{Z}^4 \to \mathbb{Z}$

$$(x_1, x_2, x_3, x_4) \mapsto \sum_{i_1, i_2, i_3, i_4} b_{i_1} b_{i_2} b_{i_3} b_{i_4} x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$$

be the norm of an element where b_i*'s lies in* $\mathbb{Z}$*. Then, for any non-zero* $v \in kerT$*, one has* $|v| \ge \frac{n^{1/4}}{\left(\sum_{i_1, i_2, i_3, i_4} |b_{i_1} b_{i_2} b_{i_3} b_{i_4}|\right)^{1/4}}$.

Proof. Ref.Birkner et al. (2012), Longa and Sica (2014)

Consider $v = x_1 + x_2\Phi + x_3\Psi + x_4\Phi\Psi$ with reduction map $T : v \mapsto x_1 + x_2\lambda + x_3\mu + x_4\lambda\mu$. The definition of norm in algebraic number field $Q\left[\Phi, \Psi\right]$ is given by $N\left(v\right) = v\bar{v}$. If $v \in kerT$, $T\left(v\right) = 0$ and since is a homomorphism $T\left(N\left(v\right)\right) = N\left(v\right) = T\left(v\right)T\left(v_1\right)T\left(v_2\right)T\left(v_3\right) \equiv 0 \; mod\; n$ where v_1, v_2, v_3 are the conjugates for v with being each of the form $v = x_1 + x_2\bar{\Phi} + x_3\bar{\Psi} + x_4\bar{\Phi}\bar{\Psi}$. $N\left(v\right) \equiv 0 \; mod\; n$ if and only if $v = 0$. If $v \neq 0$, then $N\left(v\right) \geq 0$ and this in turn implies if $|v| < \frac{n^{1/4}}{\left(\sum_{i_1,i_2,i_3,i_4}\left|b_{i_1}b_{i_2}b_{i_3}b_{i_4}\right|\right)^{1/4}}$ and hence $N\left(v\right) < n$. This is a contradiction. □

Theorem 4.2. *Birkner et al. (2012), Longa and Sica (2014)*

Let E/F_p be a GLV curve and E'/F_{p^2} a twist, together with the two efficient endomorphism Ψ and Φ . Supposed that the minimal polynomial of Φ is $\Phi^2 + r\Phi + s = 0$. Let $P \in E\left(F_{p^2}\right)$ a generator of the large subgroup of prime order n . And there exists an efficient algorithm, which for any $k \in [1, n-1]$, finds integers k_1, k_2, k_3, k_4 such that $kP = k_1P + k_2\Phi\left(P\right) + k_3\Psi\left(P\right) + k_4\Psi\Phi\left(P\right)$ with $\underset{i}{max}\left(|k_i|\right) \leq 16B^3n^{1/4}$ where
$B = \left(4 + 4s^2 + 8s + 8|r| + 8|r|s + 2\left(r^2 + 2s\right) + 2\left|r^2 - 2s\right|\right)^{1/4}$.

Proof. Ref.Birkner et al. (2012), Longa and Sica (2014)

From Theorem 2 and Lemma 1, we have $|v| \leq 8n^{1/4}B^3$. And since we have $\Psi^2 + 1 = 0$ and $\Phi^2 + r\Phi + s = 0$ where $\Psi \equiv \imath \; mod\; n$ with $\imath^2 = -1$ and $\Phi = \frac{-r+\sqrt{r^2-4s}}{2} \Rightarrow \frac{-r+\left|\sqrt{r^2-4s}\right|\imath}{2}$ since $D = r^2 - 4s < 0$. So for any $v \in kerT$, we have $v = x_1 + x_2\Phi + x_3\Psi + x_4\Phi\Psi$ and

$N\left(v\right) = v\bar{v} = \left(x_1 + x_2\Phi + x_3\Psi + x_4\Phi\Psi\right)\left(x_1 + x_2\Phi + x_3\bar{\Psi} + x_4\Phi\bar{\Psi}\right)$ $\left(x_1 + x_2\bar{\Phi} + x_3\Psi + x_4\bar{\Phi}\Psi\right)\left(x_1 + x_2\bar{\Phi} + x_3\bar{\Psi} + x_4\bar{\Phi}\bar{\Psi}\right)$

$= x_1^4 + 2x_1^2x_2^2 + 2x_1^3x_2\Phi + 2x_1x_2x_3^2\Phi + 2x_1^2x_3x_4\Phi + 2x_3^3x_4\Phi + x_1^2x_2^2\Phi^2 + x_2^2x_3^2\Phi^2 + x_1^2x_4^2\Phi^2 + x_3^2x_4^2\Phi^2 + 2x_1^3x_2\bar{\Phi} + 2x_1x_2x_3^2\bar{\Phi} + 2x_1^2x_3x_4\bar{\Phi} + 2x_3^3x_4\bar{\Phi} + 4x_1^2x_2^2\Phi\bar{\Phi} + 8x_1x_2x_3x_4\Phi\bar{\Phi} + 4x_3^2x_4^2\Phi\bar{\Phi} + 2x_1x_2^3\Phi^2\bar{\Phi} + 2x_2^2x_3x_4^2\Phi^2\bar{\Phi}$
$+ 2x_1x_2x_4^2\Phi^2\bar{\Phi} + 2x_3x_4^3\Phi^2\bar{\Phi} + x_1^2x_2^2\bar{\Phi}^2 + x_2^2x_3^2\bar{\Phi}^2 + x_1^2x_4^2\bar{\Phi}^2 + x_3^2x_4^2\bar{\Phi}^2 +$

$2x_1x_2^3\Phi\bar{\Phi}^2+2x_2^2x_3x_4^2\Phi\bar{\Phi}^2+2x_1x_2x_4^2\Phi\bar{\Phi}^2+2x_3x_4^3\Phi\bar{\Phi}^2+x_2^4\Phi^2\bar{\Phi}^2+2x_2^2x_4^2\Phi^2\bar{\Phi}^2$
$+\ x_4^4\Phi^2\bar{\Phi}^2$

Where the coefficient of terms in the norm function is represented as $\sum_{i_1,i_2,i_3,i_4}|b_{i_1}b_{i_2}b_{i_3}b_{i_4}|$ and we have

$$B = \left(\sum_{i_1,i_2,i_3,i_4}|b_{i_1}b_{i_2}b_{i_3}b_{i_4}|\right)^{1/4}$$
$$= \left(4+4s^2+8s+8|r|+8|r|s+2\left(r^2+2s\right)+2\left|r^2-2s\right|\right)^{1/4}. \qquad \square$$

But since LLL algorithm could not provide a sharper bound, they preferred to use Cornacchia algorithm which required Euclidean algorithm in it. In this four dimensional GLV method, they used Cornacchia algorithm twice where:

1. In order to obtain a Gaussian prime $\nu \in F_{p^2}$ where $\nu = a + b\imath$ dividing n and $\nu P = 0$ $(a \in \Re(\nu), b \in \Im(\nu), \imath^2 = -1)$. Cornacchia algorithm need to solve $\mu^2 \equiv -1 \ mod\ n$ where $n \equiv 1\ mod\ 4$ is a prime. The Euclidean algorithm in $\mathbb{Z}$ is being applied to n, μ to obtain ν from the sequence of the algorithm such that the initial data is given as $\begin{pmatrix} r_1 & s_1 & t_1 \\ r_0 & s_0 & t_0 \end{pmatrix} = \begin{pmatrix} \mu & 1 & 0 \\ n & 0 & 1 \end{pmatrix}$. The iteration stop at m where m is the largest integer for which $r_m \geq \sqrt{n}$ and $r_{m+1} < \sqrt{n}$. From property 6 given in Lemma 2 in (Birkner et al., 2012, Longa and Sica, 2014), we have $r_0s_j + r_1t_j = r_j$ which means $ns_{m+1} + \mu t_{m+1} = r_{m+1} \Rightarrow r_{m+1} - \mu t_{m+1} = ns_{m+1} \equiv 0\ mod\ n$. So we have $\left(r_{m+1} - \mu t_{m+1}\right)\left(r_{m+1} + \mu t_{m+1}\right) = r_{m+1}^2 + t_{m+1}^2 \equiv 0\ mod\ n$ but it does not necessary to be $r_{m+1}^2 + t_{m+1}^2 = n$. Since $0 \leq r_{m+1}, t_{m+1} < \sqrt{n}$, we have $0 \leq r_{m+1}^2 + t_{m+1}^2 < n + n = 2n$, this implies $r_{m+1}^2 + t_{m+1}^2 = n$ which has same concept for Gaussian prime $|\nu| = a^2 + b^2 = n$. Hence, we have the shortest vector as $(a, b) = (r_{m+1}, -t_{m+1}) \Rightarrow \nu = a + b\imath = r_{m+1} - \mu t_{m+1}$.(Algorithm 1 Ref. Birkner et al. (2012), Longa and Sica (2014)).

2. In order to obtain generator vectors in the compact form which contain real and imaginary parts of the vectors. The Euclidean algorithm in $\mathbb{Z}[\imath]$ is being applied the algorithm to such that the initial data is given as $\begin{pmatrix} r_1 & s_1 & t_1 \\ r_0 & s_0 & t_0 \end{pmatrix} = \begin{pmatrix} \nu & 1 & 0 \\ \lambda & 0 & 1 \end{pmatrix}$. where $\lambda^2 + r\lambda + s = 0$ to obtain two $\mathbb{Z}[\imath]$ -linearly inde-

pendent vectors v_1, v_2 .The iteration stop at m where m is the largest integer for which $r_m \geq\ n^{1/4}$ and $r_{m+1} <\ n^{1/4}$. From Lemma 2 in (Birkner et al., 2012, Longa and Sica, 2014), we have $r_0 s_j + r_1 t_j = r_j$ which means $\lambda s_{m+1} + \nu t_{m+1} = r_{m+1} \Rightarrow\ r_{m+1} - \lambda s_{m+1} = \nu t_{m+1} \equiv 0\ mod\ \nu$. Hence, we have shortest vectors as $v_0 = (r_m, -s_m), v_1 = (r_{m+1}, -s_{m+1})$ .While the other two generator vectors are $v_2 = \imath v_0, v_3 = \imath v_1$. (Algorithm 2,3 Ref. Birkner et al. (2012), Longa and Sica (2014))

This algorithm gives uniform improvement when switching from 2-dimension to 4-dimensional GLV and since it used Euclidean algorithm, it gives stronger upper bound for the decomposed scalars. Later, they came out with the following theorem:

Theorem 4.3. *Birkner et al. (2012), Longa and Sica (2014)*

When performing an optimal lattice reduction on kernel T, it is possible to decompose k into k_1, k_2, k_3, k_4 such that $kP = k_1 P + k_2 \Phi(P) + k_3 \Psi(P) + k_4 \Psi\Phi(P)$ with $\max_j(|k_j|) \leq 103\sqrt{1 + |r| + s}n^{1/4}$.

5 ISD METHOD

In ISD method (Ajeena and Kamarulhaili, 2013, 2014a,b,c), the condition for the decomposed scalar k_1 and k_2 is $\max\{|k_1|, |k_2|\} > \sqrt{n}$, a complement to GLV method where the condition of the decomposed scalar k_1 and k_2 is $\max\{|k_1|, |k_2|\} \leq \sqrt{n}$. Similar to GLV method, in ISD method we need to find the shortest vector v_1 and v_2 such that it belongs to the kernel T. Then those vectors are crucial in finding short vector u which correspond to value of decomposed scalar k_1 and k_2. If the value do not exceed $\sqrt{n}$, then GLV method is applicable. But if it exceed $\sqrt{n}$, then we need to sub-decompose the scalars, and this process is the fundamental of ISD approach. In the second stage, scalar k_1 and k_2 are sub-decomposed into the scalars k_{11}, k_{12}, and k_{21}, k_{22} respectively. As a consequence, ISD method needs six generator vectors. Considering the ISD method only involve with two-dimensional problem, the Extended Euclidean Algorithm can be used to obtain those generator vectors . Similar to the GLV method, lattice method and shortest vector problem are being applied to acquire the vector u, u', u'' which correspond to the decomposed scalar k_{11}, k_{12}, and k_{21}, k_{22}.

The general form of ISD method is given by

$$kP = k_{11}P + k_{12}\Phi_1(P) + k_{21}(P) + k_{22}\Phi_2(P). \tag{5}$$

ISD method used three GLV trivial endomorphism which are and $\Phi_2 \equiv \lambda_2$ $(mod\, n)$ where the minimal polynomial is given as $\Phi - \lambda = 0$ which in linear form. As a consequence, ISD method only works on integer number field instead of the quadratic extension field. The equation can also be written as

$$kP = k_{11}P + k_{12}\lambda_1(P) + k_{21}(P) + k_{22}\lambda_2(P). \tag{6}$$

The general bounds for the decomposed scalars are obtained in 2015 by Antony and Kamarulhaili (2015). However, the explicit bound for the ISD method has not yet been found. The following theorems describe the general bound of the decomposed scalars.

Theorem 5.1. *Ref.(Antony and Kamarulhaili, 2015)*

Let $kP = k_1P + k_2\lambda(P)$. Then, the upper bound for the sub-decomposed scalars is given by $|k_1| \leq |n - 1 - (A)|$ and $|k_2| \leq |\sqrt{n}D|$.

Theorem 5.2. *Ref.(Antony and Kamarulhaili, 2015)*

Let $|k_1| \leq |n - 1 - A| > \sqrt{n}$ and $k_1P = k_{11}P + k_{12}\lambda_1(P)$. Then, the upper bound for the sub-decomposed scalars is given by $|k_{11}| \leq |n - 1 - (A + A')|$ and $|k_{12}| \leq |\sqrt{n}D'|$.

Theorem 5.3. *Ref.(Antony and Kamarulhaili, 2015)*

Let $|k_2| \leq |\sqrt{n}D\lambda|$ and $k_2P = k_{21}P + k_{22}\lambda_1(P)$. Then, the upper bound for the sub-decomposed scalars is given by $|k_{21}| \leq |\sqrt{n}D\lambda - A''|$ and $|k_{22}| \leq |\sqrt{n}D''|$.

The values for A, A', A'', D, D', D'' varies depending on the shortest vectors that was chosen. The comparison studies has been carried out by Ajeena and Kamarulhaili (2014b) to compute the successful computation of ISD method. And it turns out that the ISD method gives more successful computation compared to the GLV method.

6 COMPARISON BETWEEN FOUR-DIMENSIONAL GLV METHOD AND ISD METHOD

The similarities between four-dimensional GLV method and ISD method is both approaches are the extension of the original GLV method which decomposed scalar k into four scalars which are given by

Four-dimensional GLV : $kP = k_1P + k_2\Phi\left(P\right) + k_3\Psi\left(P\right) + k_4\Psi\Phi\left(P\right)$

ISD : $kP = k_{11}P + k_{12}\Phi_1\left(P\right) + k_{21}\left(P\right) + k_{22}\Phi_2\left(P\right)$.

The concept being used in both methods mostly are the same where they used the lattice method and shortest vector problem. The lattice method being used to obtain the shortest vectors, and then the shortest vectors are being solved to obtain the decomposed scalars. However, the four-dimensional GLV method and ISD method vary in many aspects. One of the aspects is, they are defined over a different field. The four-dimensional GLV method is defined over F_{p^2}, while the ISD method is defined over F_p. Hence, the four-dimensional GLV method can be used to solve larger field of curves as compared to the ISD method. Other than being defined over a different field, the four-dimensional GLV method and ISD method needs different types of the endomorphism. The four-dimensional GLV method requires two types of fast endomorphism which are the p-Frobenius endomorphism and GLV endomorphism while ISD method requires three endomorphisms. The endomorphisms for the four-dimensional GLV method are given as $\Psi^2 + 1 = 0$, which can be obtained from Theorem 3.1, and $\Phi^2 + r\Phi + s = 0$. The Ψ is being defined over $\mathbb{Q}\left(\Psi\right)$, while the Φ is being defined over $\mathbb{Q}\left(\Phi\right)$ where $\Psi \equiv i\left(modn\right)$ and $\Phi \equiv \frac{-r+\sqrt{r^2-4(s)}}{2}\left(modn\right)$. Since the four-dimensional GLV method allows complex multiplication, we assume the discriminant $d = \sqrt{r^2 - 4s} < 0$. From the concept of Galois theory, if a field K is being defined over two different field which is $\mathbb{Q}\left(\Psi\right)$ and $\mathbb{Q}\left(\Phi\right)$, then the field must be defined over the product of that two different field. This explains much on why they take into consideration the product of the endomorphisms, $\Psi\Phi$ to solve the scalar decomposition problem since the four-dimensional GLV method being defined over $K = \mathbb{Q}(\Psi, \Phi)$. Meanwhile, the endomorphisms for ISD method only defined over integer field. Consequently, the ISD method only performs integer multiplication which has less application in cryptography area as compare to complex multiplication. The endomorphisms for ISD method being pick randomly from interval $[1, n-1]$. To improve the current ISD method, we can replace one of the endomorphism being used with p-Frobenius endomorphism acted on F_p, following the same concept as proposed by Galbraith et al. (2009). By using p-Frobenius endomorphism, we can reduce the cost of computing. The following lemma gives the p-Frobenius acting on F_p curves which can be one of the endomorphisms for ISD method.

Lemma 6.1. *Let $p > 3$ be a prime and let E be an ordinary elliptic curve with $p + 1 - t$ points. Let E' over F_p be the quadratic twist of $E(F_p)$ with $\#E'(F_p) = p + 1 + t$. Let $\phi : E \to E'$ be the twisting isomorphism defined over F_{p^2} and $\pi : E \to E$ be the p-power Frobenius map. Let $r|\#E'(F_p)$ be a prime such that $r > 2p$. Let $\psi = \phi\pi\phi^{-1}$. For $P \in E(F_p)[r]$, we have $\psi(P) + P = \mathcal{O}_E$.*

Proof. Let $E : y^2 = x^3 + Ax + B$ with $A, B \in F_p$ and $u \in F_p^*$ be a non-square in F_p. The isomorphism is given by $\psi(x, y) = \left(ux, u^{3/2}y\right)$ defined over F_{p^2}. By definition, we have

$$\Psi(x, y) = \left(\frac{ux^p}{u^p}, \frac{u^{3/2}y^p}{u^{3p/2}}\right). \tag{7}$$

Since $u \in F_p$, which means $u^p = u$ and $\sqrt{u}^p = -\sqrt{u}$, then for $P \in E'(F_p)$, we have $x^p = x, y^p = y$. Hence, we have the following formulation

$$\begin{aligned} \Psi(x, y) &= \left(ux^p/u^p, \sqrt{u}^3 y^p/\sqrt{u}^{3p}\right) \\ &= \left(1.x^p, (-1)^3 y^p\right) \\ &= (x, (-1)y) \\ &= -(x, y). \end{aligned}$$

Thus, we have a linear polynomial which is given as $\Psi(P) = -P \Rightarrow \Psi(P) + P = \mathcal{O}_E$ as the p-Frobenius acting on F_p curves. □

Even this p-Frobenius endomorphism over F_p is quite useless for curves which perform complex multiplication, but this endomorphism can be useful if the method being defined over integer number field. Moreover, this endomorphism can reduce the cost of computing since its mapping only involves one multiplication.

Since the four-dimensional GLV method and the ISD method used different endomorphism defined over a different field, they need different algorithm to solve the lattice problem in order to generate their generator vectors. The four-dimensional GLV method used either Cornacchia's algorithm or LLL algorithm, while ISD method used the Extended Euclidean algorithm (EEA). It is found out that the Cornacchia's algorithm able to give stronger bound as compared to LLL algorithm to solve lattice problem with dimension four. Even Cornacchia's algorithm and Extended Euclidean Algorithm are two different approaches, but they form the same shortest vector since they are required to use the Euclidean algorithm which makes them look much similar. In the four-dimensional GLV method, the Euclidean algorithm being applied in $\mathbb{Z}$ and $\mathbb{Z}\left[\imath\right]$, while the ISD method used the Euclidean algorithm in $\mathbb{Z}$ only. The four-dimensional GLV method managed to obtain the bound on its generator vectors using LLL algorithm as $|v_i| \leq 8B^3 n^{\frac{1}{4}}$. However, when using Cornacchia's algorithm to find the vectors, the algorithm gives a sharper bound which is given as $|v_i| \leq 51.5\left(\sqrt{1+|r|+s}\right)n^{1/4}$. Meanwhile in ISD method, the generator vectors are bounded by $|v_i| \leq \sqrt{n}$ as provided in GLV method. Since they used different approaches, they have the different upper bound for the decomposed scalars. In four-dimensional GLV method, the upper bound for the decomposed scalars is given by $\max_i(|k_i|) \leq 103\left(\sqrt{1+|r|+s}\right)n^{1/4}$, while the ISD method have the general upper bound as $\max_i(|k_i|) < C\sqrt{n}$ where the value for C varies depending on the generator vectors (Antony and Kamarulhaili, 2015) but the explicit upper has not yet been found.

Other than that, since the four-dimensional GLV method allow complex multiplication, the method can be applied on special types of curves that are defined over imaginary quadratic field. One of the special types of curves is curves with j-invariant 0. On the contrary, the ISD method is irrelevant on this special types of curves, since the ISD method does not perform complex multiplication. A modification needs to be made in order to allow the ISD method to perform complex multiplication and hence it can be implemented on special types of curves. Thus, the four-dimensional GLV method is applicable over GLV-GLS curves while the ISD method is only applicable for GLV curves over F_p without complex multiplication.

ACKNOWLEDGMENTS

The authors would like to express their gratitude to the Ministry of Higher Education and the Universiti Sains Malaysia for the Fundamental Research Grant Scheme (FRGS), account no. 203/PMATHS/6711320. And, the authors also would like to thank Francesco Sica for some explanation from previous works.

REFERENCES

Ajeena, R. and Kamarulhaili, H. (2013). Analysis on the elliptic scalar multiplication using integer sub decomposotion method. *International Journal of Pure and Applied Mathematics*, 87(1):95–114.

Ajeena, R. and Kamarulhaili, H. (2014a). Glv-isd method for scalar multiplication on elliptic curves. *Australian Journal of Basic and Applied Sciences*, 8(15):1–14.

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

Ajeena, R. and Kamarulhaili, H. (2014c). Two dimensional sub decomposition method for point multiplication on elliptic curves. *Journal of Mathematical Sciences: Advances and Applications*, 25:43–56.

Antony, S. and Kamarulhaili, H. (2015). On the upper bounds of the sub decomposition values of the scalar k for elliptic scalar multiplication. *Global Journal of Pure and Applied Mathematics*, 11(6):4035–4046.

Birkner, P., Longa, P., and Sica, F. (2012). Four dimensional gallant-lambert-vanstone scalar multiplication. *ASIACRYPT*.

Cohen, H. (1996). *A Course in Computational Algebraic Number Theory*.

Galbraith, S., Lin, X., and Scott, M. (2009). Endomorphisms for faster elliptic curve cryptography on a large class of curve. *EUROCRYPT*, pages 518–535.

Gallant, R., Lambert, R., and Vanstone, S. (2001). Faster point multiplication on elliptic curve with efficient endomorphism. *CRYPTO 2001,Advances in Cryptology*, pages 190–200.

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

Longa, P. and Sica, F. (2014). Four dimensional gallant-lambert-vanstone scalar multiplication. *ASIACRYPT,Journal of Cryptology*, 27(2):248–283.

Sica, R., Ciet, M., and Quisquater, J.-J. (2002). Analysis of the gallant-lambert-vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves. *SAC 2002,Selected Areas in Cryptography,9th Annual International Workshop*, 2595:21–36.