International Journal of Cryptology Research 5(2): 56-65 (2015)

Comparative Study on the Distribution of ISD and GLV Scalars

[1]**Ruma Kareem K. Ajeena and** [2]**Hailiza Kamarulhaili** [2]

[1,2] School of Mathematical Sciences, Universiti Sains Malaysia, 11800, Penang, Malaysia

Email: [1]ruma.usm@gmail.com, [2]hailiza@usm.my

ABSTRACT

We introduce the probability distribution of elliptic scalar multiplication through finding the probability distribution of the secret key, namely, the scalar k of the scalar multiplication kP of a point P which has a prime order n lying on an elliptic curve group $E(F_p)$ over a finite prime field F_p. In this work, we compare the probability distribution of k in the closed interval $[1, n]$ between the integer sub-decomposition (ISD) method and the original Gallant, Lambert and Vanstone (GLV) method. In the ISD approach, the distribution of the values of scalars k lie outside the range $\pm\sqrt{n}$ on the interval $[1, n-1]$. This distribution determines the successful rate to compute a scalar multiplication kP, in ISD approach, in comparison with the original GLV method. 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 ψ_1 and ψ_2 of elliptic curve E over F_p. The ISD sub-decomposition can be defined by

$$kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P), \text{ with max } \left|k_{11}\right|, \left|k_{12}\right| \text{ and}$$

$$\max \left|k_{21}\right|, \left|k_{22}\right| \leq C\sqrt{n},$$

for some explicit constant $C > 0$.

Keywords: Elliptic curve cryptography; Distribution of scalars k ; Efficient computable endomorphisms, Integer sub-decomposition (ISD).

INTRODUCTION

Elliptic curve cryptography (ECC) is derived from the mathematical hard problem of the discrete logarithm problem over the additive group of points on an Elliptic Curve (EC) over finite fields [3,4,5,6]. The main operation deployed in the ECC is the scalar multiplication, which in turn without a proper method yield costly computations.

Scalar multiplication, generally, represented by kP, is considered the central time-consuming operation in ECC. Scalar multiplication can be accelerated on several elliptic curves defined over fields whose large prime characteristic can be obtained through a generic procedure called, GLV method, which was proposed in [7]. This method computes the decomposition of arbitrary scalar multiplication operation kP for $k \in [1, n-1]$ and P on elliptic curve E over prime field F_p into two scalar multiplications. The bit-lengths of these new scalars are only approximately half the bit-length of the original scalar. The use of the extended elliptic Shamir trick for simultaneous point multiplication eliminates half the doublings in the computation. Although the GLV method can accelerate the computation up to 50% compared with the best general methods for point multiplication, GLV method still has certain disadvantages that remain to be addressed.

Hence, GLV method has been proposed in another model to find a GLV generator by [8] which poses a necessary condition for the existence of a GLV generator and a method of finding a GLV generator when a GLV generator exists. Gallant et al. proposed a mean to find a GLV generator; however, their proposition was without any proof. In reality, the existence of a GLV generator cannot be guaranteed. Successfully finding a GLV generator even if a GLV generator exists is also not guaranteed. The GLV method and its subsequent improvements rely on the decomposition values of k_1 and k_2 that fall within the range $-\sqrt{n} < k_1, k_2 < \sqrt{n}$. The GLV method only considers k_1 and k_2 values within this range. However, the decomposition of k also gives scalars k_1 and k_2 lie outside the range of $\pm\sqrt{n}$. To overcome this problem, new approach has been proposed, which is called integer sub- decomposition (ISD) method [9,10,11]. The ISD method allowed us to work with k_1 and k_2 that fall outside the given range. This method improved computational efficiency compared with the general method of computing scalar multiplication in elliptic curves over prime fields. Therefore, in this study, we introduce the probability distribution of the elliptic curve scalar multiplication through finding the probability distribution of the secret key, namely, the scalar k of the ISD scalar multiplication. The rest of this paper is organized as follows. Section 2 and 3 provide the procedure to compute the distribution for both the GLV and the ISD scalars in the interval $[1, n-1]$ through enumerating scalars to find the probability distribution of GLV scalars and ISD scalars. Section 4 presents the comparison results and finally section 5 is the concluding remarks.

COMPUTATION OF THE DISTRIBUTION OF GLV SCALARS

This section describes a process of the sieving of scalars k in $[1, n-1]$ which are satisfy GLV-decomposition,namely the scalars that are satisfy the condition $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$, to compute elliptic curve scalar multiplication kP over prime field F_p. To enumerate all scalars that lie in the interval $[1, n-1]$, the sieving process firstly begins by writing down all the numbers k that start from 1 reach to $n-1$. The next step includes the checking of all scalars k that can be divided into other new scalars k_1 and k_2 such that $k_1, k_2 < k$ and $k_1, k_2 \neq 0$ as well $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$. This means that, crossing off all the decompositions when the values of k_1 and k_2 are not satisfy these conditions.In the other words, the results of sieving process of the scalars k that lie in the interval $[1, n-1]$ are determined according to some cases on the values of new scalars k_1 and k_2 which are resulting from decomposing k. These cases are

i. The decomposition of k into k_1 and k_2 results $\min \left|k_1\right|, \left|k_2\right| = 0$, or $\max \left|k_1\right|, \left|k_2\right| = k$.

ii. The decomposition of k into k_1 and k_2 leads to $\max \left|k_1\right|, \left|k_2\right| > k$.

iii. The decomposition of k into k_1 and k_2 yields $\max \left|k_1\right|, \left|k_2\right| > \sqrt{n}$.

iv. The decomposition of k into k_1 and k_2 produces $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$.

Repeating this process with writing off all cases (i),(ii), and (iii) gives a list of the scalars up to $n-1$ which lie inside the range of $\pm\sqrt{n}$. The scalars k that have such this property represent GLV scalars which are considered as successful GLV elliptic scalar multiplication kP. Formally, the following algorithm (1) determines all scalars that satisfy the GLV decomposition in the interval $[1, n-1]$.

Algorithm 1: The Distribution of a Multiplier k in the GLV Scalar Multiplication kP over Prime Field

Input: The integer n, vectors $v_1 = r_{m+1}, -t_{m+1}$ and $v_2 = r_{m+2}, -t_{m+2}$.
Output: The list of the GLV correct values of multiplier k.

1. **For** $k = 1$ to $n-1$ **do**
2. Compute $c_1 = \lfloor -t_{m+2} k / n \rceil$.
3. Compute $c_2 = \lfloor - -t_{m+1} k / n \rceil$.
4. Compute $k_1 = k - c_1 r_{m+1} - c_2 r_{m+2}$.
5. Compute $k_2 = -c_1 -t_{m+1} - c_2 -t_{m+2}$.
6. **If** values of k_1 and k_2 are satisfy the relation $k \equiv k_1 + k_2 \lambda \pmod n$ **then**
7. **If** $\min \left|k_1\right|, \left|k_2\right| = 0$, or $\max \left|k_1\right|, \left|k_2\right| = k$ **then**
8. Stop and go to step 1 to choose new value of k.
9. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| > k$ **then**
10. Stop and go to step 1 to choose new value of k.
11. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| > \sqrt{n}$ **then**
12. Stop and go to step 1 to choose new value of k.
13. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$ **then**
14. Print GLV scalar k.
15. **Else**
16. $k \geq n$.
17. Stop and go to step 1 to choose new value of k.
18. **End If**
19. **Else**
20. Stop and go to step 1 to choose new value of k.
21. **End If**
22. **End For**
23. **Return** The list of the GLV correct values of multipliers k.

We have shown how to find the correct values for scalars k that satisfy the success of GLV elliptic scalar multiplication computation, kP. In order to obtain a sense of just how many scalars there are, then the set of all GLV scalars can be defined and some of numerical examples can be computed to give the answer to this question. The following discussion aims to put a precise way which measures the number of the scalars in the interval $[1, n-1]$ through the answering of the following question: How many positive integers $k \leq n-1$ are GLV scalars? And, the determination of the probability distribution of the successful computation of GLV scalar multiplication kP. The answer to this question can be found through the following definition that determines the number of GLV scalars k.

Definition 1.Let k be a positive integer, $k \in [1, n-1]$, where, n is a prime order of a point P which lies on the elliptic curve E defined over a prime field F_p that has endomorphism $\psi(P) = \lambda P$ where $\lambda \in [1, n-1]$. The number of the GLV scalars, $k \in [1, n-1]$ is defined by the following set:

$$k_{GLV}(n-1) = \#\ k \in \mathbb{Z}^+, k \le n-1,\ k \equiv k_1 + k_2\lambda (\bmod n)\ . \qquad (1)$$

where $\max\ |k_1|, |k_2| < \sqrt{n}$ such that $\max\ |k_1|, |k_2| < k$, and these scalars k_1, $k_2 \neq 0$.

The parameter $\lambda \pmod n$ is a root of characteristic polynomial $p(X) = X - \lambda$ of endomorphism ψ of E. Moreover, the determination of the number of correct values of GLV scalars in the interval $[1, n-1]$ can be used to compute the ratio of GLV scalars in the same interval $[1, n-1]$ through the following.

$$R_{GLV}(k) = \#Correct\ GLV\ \ scalars\ /\ (n-1). \qquad (2)$$

In other words, the probability of the distribution of the GLV scalars k in the interval $[1, n-1]$, is $\#Correct\ GLV\ \ scalars\ /\ (n-1)$. On the other hand, it helps to determine the percentage of successful computation of GLV elliptic scalar multiplication kP as follows.

$$Percentage_{GLV}(kP) = R_{GLV} \times 100. \qquad (3)$$

COMPUTATION OF THE DISTRIBUTION OF ISD SCALARS

Suppose E is an elliptic curve defined over prime field F_p by $E : y^2 = x^3 + ax + b \pmod p$ and let $P = (x, y)$ be a point lies on E. The order of P is a prime number n. Suppose k is a multiplier (scalar) in an elliptic point multiplication kP. The procedure of sieving the scalars k in $[1, n-1]$ which satisfy the ISD method to compute elliptic curve scalar multiplication kP over prime field F_p, can be explained in this section. The new decomposed scalars k_1 and k_2 of a ISD scalar k should satisfy the condition $\max\ |k_1|, |k_2| > \sqrt{n}$. To enumerate all ISD scalars k in the interval $[1, n-1]$ that have decomposition with this property, the sieving process firstly begins by writing down all the scalars k that start from 1 up to $n-1$. The next step includes the checking of all

scalars k_1 and k_2 such that $k_1, k_2 < k$ and $k_1, k_2 \neq 0$ as well $\max \left|k_1\right|, \left|k_2\right| > \sqrt{n}$. Therefore, we performed the crossing off on all scalars k that have decompositions not satisfying these conditions. In the other words, the results of sieving process of the scalars k that lie in the interval $[1, n-1]$ are determined according to some cases on the values of new scalars k_1 and k_2 which are resulting from decomposing k. These cases are

i. The decomposition of k into k_1 and k_2 results $\min \left|k_1\right|, \left|k_2\right| = 0$, or $\max \left|k_1\right|, \left|k_2\right| = k$.

ii. The decomposition of k into k_1 and k_2 leads to $\max \left|k_1\right|, \left|k_2\right| > k$.

iii. The decomposition of k into k_1 and k_2 yields $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$.

iv. The decomposition of k into k_1 and k_2 produces $\max \left|k_1\right|, \left|k_2\right| > \sqrt{n}$.

The recurrence of this process until $n-1$ times with write off all cases in (i),(ii), and (iii) gives a list of the ISD scalars which lie outside the range of $\pm\sqrt{n}$. The scalars k that have such this property are used as successful ISD elliptic scalar multiplication kP. The following Algorithm (2) has been developed to determine all scalars that satisfy the ISD decomposition in the interval $[1, n-1]$.

Algorithm 2: The Distribution of a Multiplier k in the ISD Scalar Multiplication kP over Prime Field

Input: The integer n, vectors $v_1 = r_{m+1}, -t_{m+1}$ and $v_2 = r_{m+2}, -t_{m+2}$.

Output: The list of the ISD correct values of multiplier k.

1. **For** $k = 1$ to $n-1$ **do**
2. Compute $c_1 = \lfloor -t_{m+2} k / n \rceil$.
3. Compute $c_2 = \lfloor - -t_{m+1} k / n \rceil$.
4. Compute $k_1 = k - c_1 r_{m+1} - c_2 r_{m+2}$.
5. Compute $k_2 = -c_1 - t_{m+1} - c_2 - t_{m+2}$.
6. **If** values of k_1 and k_2 are satisfy the relation $k \equiv k_1 + k_2 (\text{mod } n)$ **then**
7. **If** $\min \left|k_1\right|, \left|k_2\right| = 0$, or $\max \left|k_1\right|, \left|k_2\right| = k$ **then**
8. Stop and go to step 1 to choose new value of k.
9. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| > k$ **then**
10. Stop and go to step 1 to choose new value of k.
11. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| < \sqrt{n}$ **then**
12. Stop and go to step 1 to choose new value of k.
13. **ElseIf** $\max \left|k_1\right|, \left|k_2\right| > \sqrt{n}$ **then**

14. Print ISD scalar k.
15. **Else**
16. $k \geq n$.
17. Stop and go to step 1 to choose new value of k.
18. **EndIf**
19. **Else**
20. Stop and go to step 1 to choose new value of k.
21. **EndIf**
22. **EndFor**
23. **Return** The list of the ISD correct values of multipliers k.

Through the discussion presented earlier, we can determine the correct values, in an interval $[1, n-1]$, which satisfy the ISD elliptic scalar multiplication, kP [9,10,11]. So, at this point, the question that needs to be answered is; how many positive integers $k \leq n-1$ are ISD scalars? This question can be answered depending on putting an accurate way to measures the number of the scalars in the interval $[1, n-1]$ through the following definition.

Definition 2.Let k be a positive integer such that $k \in [1, n-1]$ where n be a prime order of a point P on elliptic curve E defined over prime field F_p. Let λ be any random element in $[1, n-1]$. The number of ISD scalars k is defined by the set

$$k_{ISD}(n-1) = \#\ k \in \mathbb{Z}^+, k \leq n-1,\ k \equiv k_1 + k_2 (\bmod n)\ . \quad (4)$$

Where, $\max\ |k_1|, |k_2| > \sqrt{n}$ such that $\max\ |k_1|, |k_2| < k$, these scalars $k_1, k_2 \neq 0$ and $k_2 = \bar{k}_2 \lambda$.

The determination of the number of correct values of ISD scalars in the interval $[1, n-1]$ is useful in computing the ratio of ISD scalars in the same interval.

$$R_{ISD}(k) = \#Correct\ ISD\ scalars\ /\ (n-1). \quad (5)$$

In other words, the distribution probability of the ISD scalars k in the interval $[1, n-1]$ is:

$$\#Correct\ ISD\ scalars\ /\ (n-1).$$

It helps to find the percentage of successful computation of ISD elliptic scalar multiplication kP which can be computed as follows.

$$Percentage_{ISD}(kP) = R_{ISD} \times 100. \quad (6)$$

COMPARISON RESULTS

The integer sub-decomposition (ISD) method has probability distribution, for computing a scalar multiplication kP with $k \in [1, n-1]$, greater than the probability distribution of the GLV method to compute kP on the same interval $[1, n-1]$. Several experiments were implemented on various samples of primes, with different values given in Table (1), Figures (1) and Figure (2). Furthermore, when the value of prime n increases, the number of distributed scalars of ISD increased, but the number of distributed scalars of GLV start to decrease. This indicates that the ISD method offers more successful computations of kP. Therefore, the ISD method has improved the number of successful computation of kP as compared the GLV method and subsequently increased the successful possibilities for computing kP in elliptic curve cryptography. However, there are still more to research for especially on those values of large n, and we are now still working on several curves with large prime order.

Table 1: Experimental Results of the Distribution of Successful Computation of kP in the GLV and the ISD Method on the interval $[1, n-1]$.

The prime order n	**The number of GLV scalars** $\#k_{GLV}$	**The number of ISD scalars** $\#k_{ISD}$
67	3	26
197	6	85
229	1	103
499	5	230
577	14	262
701	15	321
1093	20	506

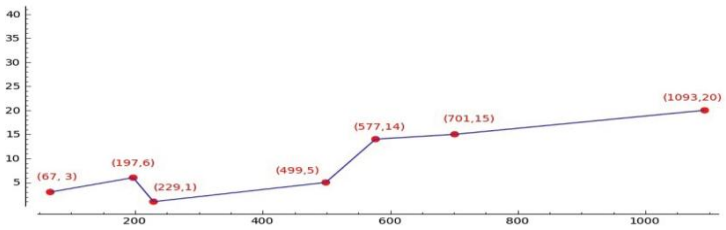

Figure 1. The distribution of the GLV scalars on the interval $[1, n-1]$.

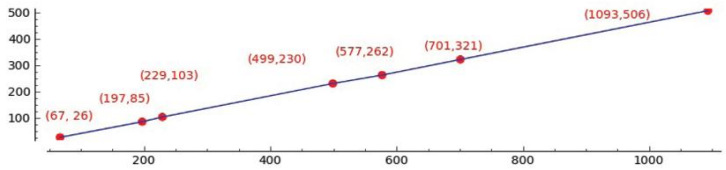

Figure 2. The distribution of the ISD scalars on the interval $[1, n-1]$.

CONCLUSION

Our main concern in this work was to investigate the successful computation rate of the scalar multiplication kP in the ISD setting and compare with the successful computation rate of the GLV method. The ISD method is rather considered as a complementary method to the existing GLV method. ISD method can help improve the percentage of successful computation of the point multiplication on an elliptic curve. As the ISD method contains two stages of decomposition, where in the first stage splits the scalar k into two smaller values and further decomposed them into much smaller values in the second stage. Thus the ISD method helps to increase the percentage of $k \in [1, n-1]$, to be computed as kP in a more efficient manner in terms of the bit size reduction. This in turn could promotes efficient cryptographic system. However, future investigation will involve much larger prime n, and to look further into the relation between those large prime n and the number of the successful computation of kP in the interval $[1, n-1]$.

ACKNOWLEDGMENTS

The authors would like to express their gratitude to the Fundamental Research Grant (FRGS), 203/PMATHS/6711320, funded by the Ministry of Higher Education and the School of Mathematical Sciences, Universiti Sains Malaysia.

REFERENCES

V. Miller, "Use of elliptic curves in cryptography", in Advances in Cryptology- CRYPTO'85 Proceedings, 1986, pp.417-426.

N. Koblitz, Mathematics of computation 48, 203-209 (1987).

Y. Hitchcock and P. Montague, Information Security and Privacy, 214-225 (2002).

Y. Hao, S. Ma, G. Chen, X. Zhang, H. Chen, and W. Zeng, Advanced Intelligent Computing Theories and Applications, 904- 911 (2008).

P. Longa and A. Miri, (Patents), 2011.

R. R. Farashahi, H. Wu, and C.-A. Zhao, Selected Areas in Cryptography, 135-148 (2013).

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

D. Kim and S. Lim, Selected Areas in Cryptography, 13-20 (2003).

R. Ajeena and H. Kamarulhaili, International Journal of Pure and Applied Mathematics 87, 95-114 (2013).

R. Ajeena and H. Kamarulhaili,Journal of Advanced Science Letters, 20(2): 526-530 (2014).

R. Ajeena and H. Kamarulhaili, Journal of Applied Mathematics & Information Sciences, 8(2): 517-525(2014).