International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Scalar Multiplication via Elliptic Net using Generalized Equivalent Sequences

Norliana Muslim, Mohamad Rushdan Md. Said

Abstract*: Chord and tangent is a classical method to calculate the elliptic curve scalar multiplication. Alternatively, the scalar multiplication can be calculated by dividing polynomials over certain finite fields and the first elliptic net scalar multiplication was implemented on a short Weierstrass curve. The net was originated from non-linear recurrence sequences, namely as elliptic divisibility sequence. It is well known that the linear recurrence sequences have been applied in the cryptosystem as a cipher in the encryption and decryption process. From the perspective of cryptographic application, the elliptic divisibility sequence is used generally for integer factorization, solving elliptic curve discrete logarithm problem and computation of pairing or scalar multiplication. But there is a lack of contribution of these non-linear recurrence sequences in scalar multiplication. Therefore, this paper aims to discuss a generalization of the equivalent sequence of elliptic divisibility for computing scalar multiplication. The experimental results of scalar multiplication via the net and its coding in computer programming are presented. The future direction of scalar multiplication via the elliptic net is also discussed.

***Keywords*: elliptic curve, division polynomials, scalar multiplication**

I. INTRODUCTION

Koblitz [1] and Miller [2] proposed elliptic curve cryptosystems and these play a key role in safe transmission via an insecure network. Due to short key sizes, in restricted environments such as smart cards, the elliptic curve cryptosystem may be a valid candidate. Since scalar multiplication is the most important and costly process in the elliptic curve cryptosystem, the speed of scalar multiplications is the topic that the researchers need to improve. Miller, on the other hand, stated that the multiple of point in elliptic curve can be calculated in polynomial time through division polynomials. However, he did not provide any proof concretely and explicitly [2]. Besides, polynomials of division are closely related to sequences of elliptic divisibility that Ward studied [3]. Shipsey [4] provided an explicit method for calculating an elliptic division of the *k*-th term. Subsequently, Stange [5] generalized the elliptic sequences of divisibility to a higher rank and described elliptic nets. In some way, the elliptic net can be considered a strong computing tool. For example, Shipsey used them to solve the elliptic curve discrete logarithm problem or as an integer factorization [4]. Meanwhile, Stange implemented her net algorithm to calculate pairings [6] and Stange's algorithm was adapted to calculate elliptic curve scalar multiplication by Kanayama et al. [7]. The earlier discussion of the elliptic net by Malaysian researchers can be seen in Muslim & Said [8]-[9].

This paper contains four sections and Section I begins with the introduction to the elliptic curve cryptography. Section II review the elliptic divisibility sequences and its generalization of equivalent sequences, elliptic curve, and elliptic nets. Meanwhile, Section III presents the experimental result of the improved elliptic net scalar multiplication and followed by discussion. Finally, the conclusion of this study with future research questions is presented in Section IV.

II. METHODOLOGY

A. Elliptic divisibility sequences

Elliptic divisibility sequences are a generalization of the group of mathematical sequences studied by Lucas [10]. The similar results also discovered by Lucas for his sequences inspired many of Ward's results. The indices [11], an apparition rank [12] and the equivalent of the sequence [4][11] are some important topics of elliptic divisibility sequence for cryptographers.

An elliptic sequence of divisibility defined as an integer sequence that meets a non-linear recurrence relationship such that

$$s_{a+b}s_{a-b}s_1^2 = s_{a+1}s_{a-1}s_t^2 - s_{b+1}s_{b-1}s_a^2 \tag{1}$$

and for all $a \geq b \geq 1$, there is *a* divides *b* whenever s_a divides s_b.

If the first two initial values of $s_0 = 0, s_1 = 1$ and $s_2 \times s_3 \neq 0$ with s_2 divides s_4, then the sequence is called as a proper elliptic divisibility sequences. For instance, {0, 1, 1, 2, 1, −7, −16, −57} is a proper sequence. For any sequences does not meet one or more of these conditions, then the sequence is an improper elliptic sequence of divisibility.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Norliana Muslim*, Department of Engineering, Faculty of Engineering and Life Sciences, Universiti Selangor, 45600 Bestari Jaya, Selangor, Malaysia. Email: norliana_muslim@unisel.edu.my
Mohamad Rushdan Md. Said, Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

B. Generalization of Equivalent Sequences

Let s_n and $\tilde{s}_n$ be two elliptic divisibility sequences. For all integer n, s_n is said equivalent to $\tilde{s}_n$ if there exists a constant i such that

$$s_n = i^{n^2-1}\tilde{s}_n \tag{2}$$

There is a different form of equation (2) proposed by Ward [3]. Kanayama [7] and Chen [14] use this equivalent in their scalar multiplication. However, the initial value $N(2)$ of the sequences was not identical. The second equivalent sequence was defined by Shipsey [4] as

$$\tilde{s}_n = i^{n^2} s_n \tag{3}$$

and the proof can be seen in her thesis. Now, we present a new equivalent of elliptic divisibility sequences and we define as follows:

$$\tilde{s}_n = i^n s_n \tag{4}$$

To proof, we must use equation (1) with $s_1 = 1$ and show that $\tilde{s}_{a+b}\tilde{s}_{a-b} = \tilde{s}_{a+1}\tilde{s}_{a-1}\tilde{s}_b^2 - \tilde{s}_{b+1}\tilde{s}_{b-1}\tilde{s}_a^2$.

We begin with,

$$\begin{aligned}
\tilde{s}_{a+b}\tilde{s}_{a-b} &= i^{a+b}s_{a+b}i^{a-b}s_{a-b} \\
&= i^{2a}s_{a+b}s_{a-b} \\
&= i^{2a}\left(s_{a+1}s_{a-1}s_b^2 - s_{b+1}s_{b-1}s_a^2\right) \\
&= i^{a+1}s_{a+1}i^{a-1}s_{a-1}\cdot s_b^2 - s_{b+1}s_{b-1}\left(i^a s_a\right)^2 \\
&= \tilde{s}_{a+1}\tilde{s}_{a-1}s_b^2 - \tilde{s}_{b+1}\tilde{s}_{b-1}\tilde{s}_a^2 .
\end{aligned}$$

We completed the proof. From the above relationship, we define the following statement.

Definition 1: Let s_n be the proper elliptic divisibility sequence. Then $N(k) = i^k N(k)$ is a sequence such that $i^2 = N^{-1}(k)$ whenever $N(2) = 1$.

Ward [3] also showed that these sequences occur as values of an elliptic curve's division polynomials. The following theorem shows us the elliptic divisibility sequence-elliptic curve relationships.

C. Relationship to Weierstrass

Theorem 1 [4][15]: Consider s_n as an elliptic divisibility sequence with $n \in \mathbb{Z}$, whose initial value of $\{0,1,s_2,s_3,s_4\}$. Then, there exists an elliptic curve Weierstrass of the form

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

with coefficients of $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, quantities of

$$b_2 = a_1^2 + 4a_2 \tag{6}$$

$$b_4 = 2a_4 + a_1a_3 \tag{7}$$

$$b_6 = a_3^2 + 4a_6 \tag{8}$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \tag{9}$$

$$D = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{10}$$

and a rational point $P = (x_0, y_0)$ from the elliptic curve Weierstrass with the division polynomials of $\psi_n(P) = s_n$.

The first four polynomials of division ψ_n with are denoted by

$$\psi_1 = 1, \qquad \psi_2 = 2y + a_1x + a_3, \tag{11}$$

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \tag{12}$$

$$\psi_4 = \psi_2\begin{pmatrix} 2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + \\ (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2 \end{pmatrix} \tag{13}$$

and can be group to set of polynomials with x and y coordinates of the form of

$$[n]P = \left(\frac{\varphi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3}\right) \tag{14}$$

and such that

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1} \tag{15}$$

$$\omega_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y} \tag{16}$$

D. Polynomials to Elliptic Net

Stange [16] demonstrated that the set of polynomials satisfy the relationship for a fixed tuple point P on the elliptic curve in the following generalization theorem:

Theorem 2: An elliptic net is a map from a free Abelian group with finite rank to an integral domain R. The net contains $N(0) = 0$ and must satisfy

$$\begin{aligned}
&N(p+q+s)N(p-q)N(r+s)N(r) + N(q+r+s) \\
&N(q-r)N(p+s)N(p) + N(r+p+s)N(r-p) \\
&N(q+s)N(q) = 0
\end{aligned} \tag{17}$$

Elliptic nets in this context are generalizations of elliptic sequences of divisibility, which can be interpreted as k-dimensional arrays. Note that the initial value in the elliptic net and elliptic net scalar multiplication require s_{-2} and s_{-1} not only $\{0,1,s_2,s_3,s_4\}$.

III. RESULTS AND DISCUSSION

A. Improved Elliptic Net Scalar Multiplication

The following theorem represents scalar multiplication upon short Weierstrass. It is an improved version using a generalized equivalent sequence of $\tilde{s}_n = i^n s_n$.

Theorem 3: Let s_n be a proper elliptic divisibility sequence and a point $P = (x_0, y_0)$ from the short Weierstrass of the form $y^2 = x^3 + a_4x + a_6$. Then, the explicit formulae of scalar multiplication via the elliptic net $kP = (x_k, y_k)$ is denoted by

$$x_k = x_0 - \frac{N(k-1)N(k+1)}{N(k)^2} \tag{18}$$

$$y_k = \frac{N^2(k-1)N(k+2) - N^2(k+1)N(k-2)}{4y_1N^3(k)} \tag{19}$$

The algorithm for calculating scalar multiplication using division polynomials, namely in the form of elliptic net is presented as shown below in Figure 1:

```
Input: a positive integer k and P = (x0, y0)
Set N(-2), N(-1), N(0)=0, N(1)=1, N(2)=1, N(3), N(4)
 for i=5 to k
        if i%2 = =0
           N(2k) = N(k)[N(k+1)N^2(k-1)-N(k-2)N^2(k+1)]/2y0
        end if
        else
          N(2k+1) = N(k+2)N^3(k)-N(k-1)N^3(k+1)
        end else
    end for
 Set   x[k] = x0 –[ N(k-1)N(k+1)/N^2(k)]
       y[k] = N^2(k-1)N(k+2)-(N^2(k+1)N(k-2)]/4 y0N^3(k)]
Output kP =( x[k], y[k] )
```

Fig. 1.Algorithm for computing elliptic net scalar multiplication using division polynomials

B. Comparison of the Initial Values

The following Table I compares the value of $N(2)$ for elliptic net scalar multiplication between Kanayama et al. [7], Chen [14] and our method.

Table- I: Value of elliptic net scalar multiplication

Method	Equivalent EDS	$N(2)$
Kanayama et al. [7]	$\tilde{s}_n = i^{n^2-1}s_n$	$N(2) \neq 1$
Chen [14]	$\tilde{s}_n = i^{n^2-1}s_n$	$N(2) = 1$
This method	$\tilde{s}_n = i^{n}s_n$	$N(2) = 1$

Meanwhile, Table II below shows the initial vector from the equivalent sequences. Note that $N(5)$ was calculated using the relationship in equation 1.

Table- II: Equivalent sequences as vector in the net

Net Term	Kanayama	Chen	Our method
$N(1)$	1	1	1
$N(2)$	$i^3N(2) = p$	$i^3N(2) = p = 1$	$i^2N(2) = p = 1$
$N(3)$	$i^8N(3) = \hat{q}$	$i^8N(3) = \hat{q}$	$i^3N(3) = \hat{q}$
$N(4)$	$i^{15}N(4) = \hat{r}$	$i^{15}N(4) = \hat{r}$	$i^4N(4) = \hat{r}$
$N(5)$	$p^3\hat{r} - \hat{q}^3$	$\hat{r} - \hat{q}^3$	$\hat{r} - \hat{q}^3$

From Table I and Table II, we can say that the equivalent sequence in our method is a generalization form and has the same performance as Chen's method.

C. Experimental results

To calculate the multiplication of scalar for x and y coordinates, we need value for the k-term as shown in Table III. Note that the values in Table III can be simplified to a certain value using modulo of a prime number. These can prevent from working with a long digit. We provide the following data in Table IV for the point multiplication via the net. The running environments for these experiments are Windows 10 64-bit, AMD Quad-Core A8-7410 APU, 2.2 GHz, and 4GB memory. The program was written in C Programming and based on Codeblocks as shown in the Appendix.

Table- III: Value for calculating scalar multiplication for $P = (1, 2)$

k	$N(k)$
0	0
1	1
2	4
3	44
4	-1728
5	-195776
6	-67302400

Table- IV: Scalar multiplication for $P = (1, 2)$

Point	*x*-coordinate	*y*-coordinate
P	1	2
2P	$-\frac{28}{16}$	$-\frac{1728}{512}$
3P	$\frac{8848}{1936}$	$-\frac{6118400}{681472}$
4P	$\frac{11600128}{2985984}$	$\frac{283610415104}{41278242816}$
5P	$-\frac{77970305024}{38328242176}$	$\frac{187472091476393980}{60029999521988608}$

We may verify values in Table IV by substituting x and y coordinates to the short Weierstrass stated in Theorem 3 and getting the left-hand side is equal to the right-hand side of the equation.

IV. CONCLUSION

The generalized equivalent elliptic divisibility sequence has been discussed for calculating scalar multiplication via the elliptic net. Then, the explicit formulae of the improved net were presented. In the improved scalar multiplication, the algorithm of the new net was presented with its experimental results. As for future research questions, the researcher may consider implementing the generalized equivalent elliptic divisibility sequence in other types of scalar multiplication but with a different kind of cryptographic curve. The computation chain for the elliptic net is another topic that the researcher may consider analyzing.

APPENDIX

The coding for calculating the k-term and its scalar multiplication is provided below:

```
#include <stdio.h>
#include <math.h>
//Weirstrass - Net p(1,2)
static double x,y;
static double a1,a2,a3,a4,a6,b2,b4,b6,b8;

int main()
{  x = 1.0;
   y = 2.0;
   a1 = 0.0;
   a2 = 0.0;
   a3 = 0.0;
   a4 = -5.0;
   a6 = 8.0;
   b2 = pow(a1,2) + (4*a2);
   b4 = (2*a4) + (a1*a3);
   b6 = pow(a3,2) + (4*a6);
   b8 =
(pow(a1,2)*a6)+(4*a2*a6)-(a1*a3*a4)+(a2*pow(a3,2))-(pow(a4,2));

   printf("x : %.0f     y : %.0f\n",x ,y);
   printf("a1 : %.0f     a3 : %.0f\n",a1 ,a3);
   printf("a4 : %.0f     a4 : %.0f     a6 : %.0f\n",a2 ,a4, a6);
   printf("\n");
   printf("b2 : %.0f     b4 : %.0f\n",b2 ,b4);
   printf("b6 : %.0f     b8 : %.0f\n",b6 ,b8);
   printf("\n");
   // value of array be plus two
   int scalar;
   printf("Input scalar: ");
   scanf("%d", &scalar);

static double W[] = {};
   for(int i=0; i<scalar+3; i++)
   {
     if (i == 0)
       W[i] = 0;
     if (i == 1)
       W[i] = 1;
     if (i == 2)
       W[i] = (2*y)+(a1*x)+a3;
    if (i == 3)
    W[i]                                                    =
(3*pow(x,4))+(b2*pow(x,3))+(3*b4*pow(x,2))+(3*b6*x)+b8;
    if (i == 4)
        W[i]=W[2]*((2*pow(x,6))+(b2*pow(x,5))+(5*b4*pow(x,4))+
       (10*b6*pow(x,3))+(10*b8*pow(x,2))+
       (((b2*b8)-(b4*b6))*x)+((b4*b8)-pow(b6,2)));
   if (i > 4)
    {
       if (i % 2 == 0) // even
       { int m1 = i;
         m1 = m1/2;
      W[i]= (W[m1]*((W[m1+2]*pow(W[m1-1],2))-(W[m1-2]*
      pow(W[m1+1],2))))/W[2];
      }
       else  // odd
       {      int m2 = i;
              m2 = (m2-1)/2;
         W[i]                                               =
(W[m2+2]*pow(W[m2],3))-(W[m2-1]*pow(W[m2+1],3));
       }
     }
    printf("W%d : %.0f\n",i,W[i]);
   }  printf("\n");

//scalar multiplication
int n = scalar;
double x1 = x-((W[n-1]*W[n+1])/pow(W[n],2));
double numerX, denoX;
numerX = (pow(W[n],2)*x) - (W[n-1]*W[n+1]);
denoX = pow(W[n],2);
printf("Value of x%d\n",n);
printf("   in decimal  :  %f\n",x1);
printf("   in fraction :  %.0f\n",numerX);
printf("                 ---------\n");
printf("                 %.0f\n",denoX);
double y1=((pow(W[n-1],2)*W[n+2]) - (pow(W[n+1],2)
*W[n-2]))/(4*y*pow(W[n],3));
double numerY, denoY;
numerY = (pow(W[n-1],2)*W[n+2]) - (pow(W[n+1],2)*W[n-2]);
denoY = 4*y*pow(W[n],3);
printf("Value of y%d\n",n);
printf("   in decimal  : %f\n",y1);
printf("   in fraction : %.0f\n",numerY);
printf("                 ---------\n");
printf("                 %.0f\n",denoY);
return 0;
}
```

ACKNOWLEDGMENT

The generalization of equivalent sequences was first presented orally during the 6th International Cryptology and Information Security Conference, for that the authors thank Universiti Selangor for the opportunity. Both authors also feel gratitude to Universiti Selangor for providing the first author with financial support and an excellent facility to conduct the study.

REFERENCES

1. N. Koblitz, "Constructing Elliptic Curve Cryptosystems in Characteristic 2," in *Menezes A.J., Vanstone S.A. (eds) Advances in Cryptology-CRYPT0' 90. CRYPTO 1990. Lecture Notes in Computer Science*, vol. 537, Springer, Berlin, Heidelberg, 1991, pp. 156–167.
2. V. S. Miller, "Use of Elliptic Curves in Cryptography," *Lect. Notes Comput. Sci.*, no. 218, pp. 417–426, 1986.
3. M. Ward, "Memoir on Elliptic Divisibility Sequences," *Am. J. Math.*, vol. 70, no. 1, pp. 31–74, 1948.
4. R. Shipsey, "'Elliptic Divisibility Sequences,'" PhD thesis, University of London, 2000.
5. K. E. Stange, "Elliptic nets and points on elliptic curves," *Algorithmic Number Theory*, no. 1, pp. 1–4, 2007.
6. K. E. Stange, "The Tate Pairing via Elliptic Nets," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4575 LNCS, no. 1, pp. 329–348, 2007.
7. N. Kanayama, Y. Liu, E. Okamoto, K. Saito, T. Teruya, and S. Uchiyama, "Implementation of an elliptic curve scalar multiplication method using division polynomials," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E97-A, no. 1, pp. 300–302, 2014.
8. N. Muslim and M. R. M. Said, "Elliptic net and its cryptographic application," in *AIP Conference Proceedings*, 2017, vol. 1905, no. December.
9. N. Muslim and M. R. M. Said, "Constructing Scalar Multiplication via Elliptic Net of Rank Two," *Int. J. Eng. Technol.*, vol. 7, no. 4.34, pp. 403–406, 2018.
10. E. Lucas, "Theories des fonctions numeriques simplement periodiques," *Am. J. Math.*, vol. 1, pp. 184–239, 1878.
11. J. H. Silverman and K. E. Stange, "Terms in elliptic divisibility sequences divisible by their indices," *Acta Arith.*, vol. 146, no. 4, pp. 355–378, 2011.
12. B. Gezer and O. Bizim, "Elliptic divisibility sequences in certain ranks over finite fields," *Hacettepe J. Math. Stat.*, vol. 38, no. 2, pp. 161–171, 2009.
13. O. Bizim, "On The Elliptic Divisibility Sequences over Finite," *World Acad. Sci. Eng. Technol.*, vol. 35, pp. 1011–1015, 2009.
14. B. Chen, C. Hu, and C. Zhao, "A Note on Scalar Multiplication Using Division Polynomials," *IET Inf. Secur.*, vol. 11, no. 4, pp. 195–198, 2017.
15. J. H. Silverman and N. Stephens, "The sign of an elliptic divisibility sequence," no. February, pp. 1–17, 2004.
16. K. E. Stange, "Elliptic Net and Elliptic Curve," PhD thesis, Brown University, 2008.

AUTHORS PROFILE

Norliana Muslim is a Mathematics lecturer from the Department of Engineering, Faculty of Engineering and Life Sciences, Universiti Selangor. She had teaching experience in various subjects such as statistics, engineering mathematics, discrete mathematics, calculus, advanced calculus, and computer programming. She graduated Master of Science (Pure Mathematics) from Universiti Putra Malaysia with a research topic focused on the Lucas sequences. She is a member of the International Association for Cryptologic Research (IACR) and the Institution of Engineering and Technology (IET). Her research interest includes the cryptosystem and the application of mathematical sequences in cryptography.

Mohamad Rushdan Md. Said is a retired Associate Professor from Universiti Putra Malaysia. He is currently an associate researcher at the Institute for Mathematical Research, Universiti Putra Malaysia. He had produced many Master and Ph.D. students in Malaysia. Previously, he successfully received many research grants from the Ministry of Education, Malaysia. His expertise includes number theory and cryptography, especially the use of non-linear recurrence sequence, namely as Lucas sequences and elliptic curve scalar multiplication.