International Journal of Engineering & Technology, 7 (3.28) (2018) 153-156

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Scalar Multiplication via Elliptic Nets with Application to Cryptography

Norliana Muslim[1]*, Mohamad Rushdan Md Said[2]

[1]*Faculty of Engineering and Life Sciences, Universiti Selangor, 45600 Bestari Jaya, Selangor, Malaysia*
[2]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
**Corresponding Author E-mail: norliana_muslim@yahoo.com*

Abstract

The net theory based on elliptic sequences is widely used as a computational tool in cryptographic pairing. The theory of this net is originated from non-linear recurrence relations which also known as elliptic divisibility sequences. In this study, at first we review the history of elliptic net such as recurrence sequences and elliptic divisibility sequences with the important properties. Next, we address scalar multiplication in elliptic curve cryptography. We further with division polynomials used in the elliptic net and followed by an elliptic net scalar multiplication. Finally, this study stated the future research directions of elliptic net and its scalar multiplication. The findings from this study will help other researchers to explore and to expand recent topics of applied mathematical sequences in cryptography.

Keywords: *divisibility; elliptic; polynomial; rank; scalar.*

1. Introduction

Elliptic nets introduced by [1] is an alternative method to compute cryptographic pairing. A single-round Tripartite Diffie-Hellman key exchange method was created by a cryptographer, Joux [20]. Tate pairing was the first pairing computation which employed elliptic nets [1] This was followed by Weil-, Ate-, as well as optimal-pairing [10]. Nevertheless, Tate pairing via elliptic net provides faster computation since Tate pairing calculation will be decreased by terms of an elliptic net formulation. Other than pairing, the same theory of the elliptic net has been applied to calculate elliptic curve scalar multiplication [14].

The famous principle stated by [2] (i.e. it is possible to reduce an elliptic curve's discrete log to a finite field), bring many researchers with new exploration of constructing cryptosystem using linear recurrence sequence or applying scalar multiplication and pairing in cryptography using non-linear recurrence sequence. Interestingly, the capability of the computation has become a main issue for elliptic curve cryptosystems, scalar multiplication and pairing.

In this paper, we introduce a special group of sequences namely as the recurrence sequences and an elliptic divisibility sequence. Next, we state through elliptic nets, elliptic curves are related with elliptic divisibility sequences, pairings and scalar multiplication. Finally, a presumptive study on elliptic nets (in terms of the ranks, periodic nature, as well as cryptographic applications of elliptic nets) was postulated.

2. Group of Recurrences

Mainly, the group of mathematical recurrences can be divided to two sequences of linear and nonlinear equations. The Lucas sequence [3] which denoted by U_r and V_r - is a second-order linear-recurrence relation. It is extensively studied in cryptosystem and was first applied in LUC [4]. Meanwhile an analogous of LUCELG and Cramer-Shoup cryptosystem has been designed by [5]. The formulated equations of linear-recurrence include the equations of $U_r = GU_{r-1} - HU_{r-2}$ and $V_r = GV_{r-1} - HV_{r-2}$ with G and H being the quadratic equations' values.

The Somos sequences [6] and elliptic divisibility sequences [5, 8], appear as nonlinear recurrence relation that have divisibility properties. In [7] has explored Lucas sequences and their features. Subsequently, he came up with a generalized form of the aforementioned relation as follows:

$$h_{r+t}\, h_{r-t}(h_1)^2 = h_{r+1}h_{r-1}\,(h_t)^2 - h_{t+1}h_{t-1}(h_r)^2 \quad (1)$$

In (1) has been transformed to a new notation of elliptic net rank one by the form of,

$$W(r+t)W(r-t)\,W(1)^2 = W(r+1)W(r-1)W(t)2 - W(t+1)W(t-1)W(r)^2 \quad (2)$$

Using $t = 2$ and $h_1^2 = 1$, an elliptic divisibility sequence (which also gave explicit formulae for Weierstrass equation coefficient) was formed in (1) by [5].

If we swap r and t to m and n, then the above-mentioned sequence $h_0, h_1, \ldots, h_n, \ldots$ contains integers which are adequate solutions in (1) with $m \geq n \geq 1$ and satisfy the divisibility property such that h_n divides h_m. If we proceed substituting the condition for m and n with $h_0 = 0$, then we can derive two properties of proper elliptic divisibility sequences denoted by

$$h_{2n}h_2 = h_{n+2}h_n h_{n-1}^2 - h_n h_{n-2}h_{n+1}^2 \quad (3)$$

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3 \quad (4)$$

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In (3), 2*n* denotes an even-numbered term, while the 2*n*+1 in (4) illustrates an odd-numbered term. Using $h_0 \neq 0$, in [8] generated the following feature of an improper elliptic divisibility sequence:

$$h_{2n+1} = \begin{cases} h_{n-1}h_{n+1}^3 & \text{for even number n} \\ h_{n+2}h_n^3 & \text{for odd number n} \end{cases}$$

For instances, the integer sequences of {0, 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, …} and {1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043,…} constitute the proper and improper forms of the said sequences that meet the condition such that for $n|m$ then $h_n|h_m$. Evidently, proper sequences are initialized by $h_0 = 0, h_1 = 1$ and have a condition of $h_2h_3 \neq 0$ (otherwise the sequence will be improper).

3. Elliptic Curve

Normally, algebraic interpretations have solution sets which comprise elliptic curves that are expressed as $y^2 = x^3 + ax + b$ (with *a* as well as *b* being real numbers). Meanwhile, elliptic curves [9] can be generalized by a Weierstrass equation:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6}$$

with all values of *a* being integers and the remaining unknowns being rational numbers. The above equation consists the succeeding equations of

$$b_2 = a_1^2 + 4a_2 \tag{7}$$

$$b_4 = 2a_4 + a_1a_3 \tag{8}$$

$$b_6 = a_3^2 + 4a_6 \tag{9}$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \tag{10}$$

$$D = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{11}$$

In (7) until (10) display the typical values of elliptic curves, while *D* in (11) represent the discriminant. The auxiliary polynomials, i.e. ϕ_n, ω_n, can be formed and utilized by

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1} \tag{12}$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2 \tag{13}$$

For the polynomials $\phi_n(P), \psi_n, \omega_n$ that connected to the elliptic curve by a scalar *n* then the *x* and *y* coordinates can be depicted as,

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

The polynomials in (6) are comparable to the division polynomials ψ_n in *x*, *y*. The following equations denote the initial 4 polynomials:

$$\psi_1 = 1, \qquad \psi_2 = 2y + a_1x + a_3, \tag{15}$$

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \tag{16}$$

$$\psi_4 = (2y + a_1x + a_3)(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2) \tag{17}$$

For $n \geq 2$, the division polynomial, ψ_n, contains the following recurrence relations:

$$2y\psi_{2n} = \psi_n(\psi_{n+1}h_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{18}$$

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \tag{19}$$

3.1 Elliptic Curve Scalar Multiplication

The rise of the elliptic curve scalar multiplication begins after the implementation of elliptic curve cryptography protocols like Elliptic-Curve Diffie-Hellman [19]. For a given point *P* that belongs to the elliptic curve with an integer *k*, then the elliptic curve scalar multiplication is used to calculate a new point *Q* such that *Q* = *kP* for *k* times.

Example 1:
Let a point *P* = (1,2) on a nonsingular elliptic curve *E* over rational numbers that satisfies $y^2 = x^3 - 5x + 8$, then find *Q* = 2*P* = *P* +*P*. From [15],

$$m = \frac{3x_1 + a}{2y_1} = \frac{3(1^2) + (-5)}{2(2)} = -\frac{1}{2}$$

$$x_3 = m^2 - x_1 - x_2 = \left(-\frac{1}{2}\right)^2 - 1 - 1 = -\frac{7}{4}$$

$$y_3 = m(x_1 - x_3) - y_1 = -\frac{1}{2}\left(1 + \frac{7}{4}\right) - 2 = -\frac{27}{8}$$

Therefore, $Q = \left(-\frac{7}{4}, -\frac{27}{8}\right) = \left(-\frac{7}{2^2}, -\frac{27}{2^3}\right)$.

3.2. Elliptic Net

In (14)-(17) – represent elliptic net rank 1 and use the same type of elliptic curve. In [10] came up with generalized forms of elliptic divisibility sequences in higher-order dimensions as well as specific fields. In the second rank, elliptic nets are functions of W: *A* → *R* from finite-rank free Abelian groups, *A*, to integral domains, *R*, which uphold the said feature.

$$W(a+b+d)W(a-b)W(c+d)W(c)+W(b+c+d)W(b-c)W(a+d)W(a)+W(a+c+d)W(c-a)W(b+d)W(b)=0, \text{ for all } a,b,c,d \in A \tag{20}$$

In (20), the starting values constitute $W(0,0) = W(1,0) = W(0,1) = W(1,1) = 0$ and with $W(1,2)$ and $W(0,2)$. Owing to the fact that there are associations between elliptic nets and curves, it is possible to generate the net polynomials $\Psi_v \in E^n(K)$ by generalizing the division polynomials, with the condition that $v \in Z^n$. With reference in (14), when $P, Q \in E(\mathrm{Q})$ and the construction of formal linear for point *P* as well as *Q* are taken into consideration, the following transformation can be constructed: $[f]P + [g]Q \longleftrightarrow W_{f,g}$

We propose the following lemma related to elliptic net.

Lemma 1: *The number of the proper sequences in the elliptic net of rank two over* F_p *is* $(p-1)^2$ *p.*

Proof: If $W(n,0)$ is a proper sequences in the elliptic net of rank two with $W(0,0)=0$, then $W(2,0)\neq 0$ and $W(3,0)\neq 0$. In this situation, there are $p-1$ case for selecting $W(2,0)=0$ and $W(3,0)$ or $W(3,0)=0$ and $W(2,0)$. So, there are $(p-1)^2$ sequences. For another situation such that $W(4,0)$ is divisible by $W(2,0)$, there are p case for selecting $W(4,0)$. Therefore, the number of the proper sequences in the elliptic net of rank two over F_p is $(p-1)^2$ p.

3.2.1. Properties of Elliptic Net

For a given $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ from an elliptic curve of the form $y^2=x^3+Ax+B$ with initial values of $W(0,0), W(1,0), W(0,1)$ and $W(1,1)$ is equal to one, then some important properties of elliptic net rank two were derived by [10] as follow:

$$W(2,0)=2y_1 \tag{21}$$

$$W(3,0)=3x_1^4+6Ax_1^2+12Bx_1-A^2 \tag{22}$$

$$W(4,0)=4y_1\left(x_1^6+5Ax_1^4+20Bx_1^3-5A^2x_1^2-4ABx_1-8B^2-A^3\right) \tag{23}$$

$$W(2,1)=2x_1+x_2-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 \tag{24}$$

$$W(-1,1)=x_1-x_2 \tag{25}$$

3.2.2. Alternative for Cryptographic Pairing

In [1] implemented her method in the Tate pairing, a method which resembled Miller's algorithm [11] in terms of the double-add. Additionally, the former was employed in Ate-, R-Ate-, as well as optimal-pairings [12]. Subsequently, in [13] improved the said method with the incorporation of double-add and -subtract. A few years ago, a novel study which employed elliptic nets to compute scalar multiplications has been published [14].

4. Elliptic Curve Scalar Multiplication via Elliptic Net

As mentioned by [14], some advantages of elliptic net scalar multiplication are no inverse operations will be needed for loop iteration, equivalent costing between double step and double add step and easy adjustment for different finite fields. This elliptic net scalar multiplication concept has been proposed by [13] six years after theory of elliptic net using arithmetic of elliptic curve [15] and with implementation of elliptic net.

Consider the elliptic curve over finite field $E/F_q: y^2=x^3+ax+b, \text{and } P=(x_1,y_1)\in E.$ An elliptic net scalar multiplication of rank one using division polynomials can be defined as finding $kP=(x_{kP},y_{kP})$ with the following:

$$x_{kP}=x_P-\frac{W(k-1,0)W(k+1,0)}{W(k,0)^2} \tag{26}$$

$$y_{kP}=\frac{W(k-1,0)^2W(k+2,0)-W(k+1,0)^2W(k-2,0)}{4y_PW(k,0)^3} \tag{27}$$

Note that the block for a scalar k can be constructed as shown in Figure 1. Both rows in in the block are eight consecutive term of elliptic net sequence with $W(i,0)$ having its center on $W(k,0)$ as well as $W(k+1,0)$.

		(k, 0)				
(k-3,0)	(k-2,0)	(k-1,0)	(k+1,0)	(k+2,0)	(k+3,0)	(k+4,0)

Fig. 1: Block on k

For a k-centered block vector, V, in [10] presented 2 algorithms namely Double (V) and DoubleAdd (V) that constructed blocks whose centers were $2k$ as well as $2k+1$ respectively.

We provide the following calculation as an example for elliptic net scalar multiplication.

Example 2:

Let $E: y^2=x^3-5x+8$ and a point $P=(6,3)\in E$ with respect to elliptic net, then calculate $2P$. The initial values of elliptic net $W(i,0)$ and $W(i,1)$ for $-2\le i\le 2$ with $k=2$ can be obtained from

$$\begin{aligned}&W(-1,0)=-1,\\ &W(1,0)=W(1,1)=W(0,1)=1,\ W(0,0)=0\\ &W(-2,0)=-2y_1=-2(3)=-6,\\ &W(2,0)=2y_1=2(3)=6.\end{aligned}$$

Next, we continue to calculate $W(3,0)$ and $W(4,0)$ such that

$$\begin{aligned}W(3,0)&=3x_1^3+6Ax_1^2+12Bx_1-A^2\\ &=3\left(6^3\right)+6(-5)(6^2)+12(8)(6)-(-5)^2=119\\ W(4,0)&=4y_1\left(x_1^6+5Ax_1^4+20Bx_1^3-5A^2x_1^2-4ABx_1\right.\\ &\quad\left.-8B^2-A^3\right)\\ &=4(3)\left(6^6+5(-5)\left(6^4\right)+20(8)\left(6^3\right)-5(-5)\left(6^2\right)\right.\\ &\quad\left.-4(-5)(8)(6)-8\left(8^2\right)-(-5)^3=512628\right.\end{aligned}$$

Then,

$$x_{2P}=x_P-\frac{W(1,0)W(3,0)}{W(2,0)^2}=6-\frac{1(119)}{6^2}=\frac{97}{36}$$

$$\begin{aligned}y_{2P}&=\frac{W(1,0)^2W(4,0)-W(3,0)^2W(0,0)}{4y_PW(2,0)^3}\\ &=\frac{1(512628)-\left(119^2\right)(0)}{4(3)\left(6^3\right)}=\frac{42719}{216}\end{aligned}$$

Therefore, for $P=(6,3)$ then

$$2P=\left(\frac{97}{36},\frac{42719}{216}\right)=\left(\frac{97}{6^2},\frac{42719}{6^3}\right).$$

Ward proposed Elliptic Net (1) while Stange Elliptic Net (2). The existence of net polynomials in rank two are applicable in third-rank nets and thus produce a new order of the net. In specific notation, if $[f]P$ implies W_f and $[g]Q$ implies W_g, thus the extension of a third-rank elliptic net whereby,

$[f]P+[g]Q+[h]R<\!\!\longrightarrow W_{f,g,h}$

With reference to the nets, a contrast method for locating integer points like periodicity relations is usable in second-order ranks or higher. In [16] recently researched on intra-sequence periodicity relations. With the intention of expanding this topic and referring to [17], the elliptic net rank one holds that

$$W_{E,P}(sr+k) = W_{E,P}(k)a^{sk}b^{s^2},$$

$$a = \frac{W_{E,P}(r+2)}{W_{E,P}(r+1)W_{E,P}(2)} \text{ and } b = \frac{W_{E,P}(r+1)^2 W_{E,P}(2)}{W_{E,P}(r+2)}.$$

For future cryptographic applications, the basic Tate pairing calculation via elliptic nets should be modified through the selection of hyper-elliptic curves. Evidently, elliptic nets are relevant in supersingular curves [18].

5. Conclusion

It is possible to generalize elliptic nets in terms of first- and second-ranks, apart from different individual non-linear recurrence relations. To transform division polynomials into net polynomials, a variety of features are needed. These produce cryptographic pairing and scalar multiplication computational problem. Besides pairing and scalar multiplication, the prospective researches which were recommended by this article have the potential to have other elliptic net-related applications.

Acknowledgement

The authors would like to express gratitude to the Institut Penyelidikan Matematik (INSPEM), Universiti Putra Malaysia and Universiti Selangor (UNISEL) for supporting this study.

References

[1] K. Stange, “The Tate pairing via elliptic nets,” *Lect. Notes Comput. Sci.*, 4575, 329–348, 2007.
[2] A. J. Menezes, T. Okamoto, and S. A. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” *IEEE Trans. Inf. Theory*, 39(5), 1639–1646, 1993.
[3] E. Lucas, “Theories des fonctions numeriques simplement periodiques,” *Am. J. Math.*, 1(3), 197–240, 1878.
[4] M. Smith, P., and Lennon, “LUC: A new public key system,” *Proceedings of the Ninth International Conference on Information Security*, pp. 103-117, 1993.
[5] N. Muslim and M. R. Md. Said, “A New Cryptosystem Analogous to LUCELG and Cramer-Shoup,” *Int. J. Cryptol. Res.*, 1(20, 191–204, 2009.
[6] M. Somos, “Problem 1470,” 1989., 1948.
[7] M. Ward, “Memoir on elliptic divisibility sequences,” *Am. J. Math.*, 70(1), 31–74.
[8] R. Shipsey, “Elliptic divisibility sequences,” PhD thesis, University of London, 2000.
[9] O. Bizim, “On the elliptic divisibility sequences over finite,” *World Acad. Sci. Eng. Technol.*, 35, 1011–1015, 2009.
[10] K. E. Stange, “Elliptic nets and elliptic curves,” *Algebr. Number Theory*, 2, 197–229, 2011.
[11] V. S. Miller, “Short programs for functions on curves,” 1986, http://pages.cs.wisc.edu/~cs812-1/miller86.pdf.
[12] N. Ogura and N. Kanayama, “Cryptographic pairings based on elliptic nets,” *Adv. Inf. Comput. Secur.*, 7038, 1–16, 2011.
[13] B. Chen and C. Zhao, “An improvement of the elliptic net algorithm,” *IEEE Trans. Comput.*, 65(9), 2903–2909, 2015.
[14] B. Chen, C. Hu, and C. Zhao, “A note on scalar multiplication using division polynomials,” *IET Inf. Secur.*, 11(4), 195–198, 2017.
[15] J. H. Silverman, *The arithmetic of elliptic curves*. Springer Science and Business Media, 2009.
[16] M. Ayad, “Periodicite (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques,” *Ann. Ins. Fourier*, 3(43), 585–618, 1993.
[17] K. E. Lauter and K. E. Stange, “The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences,” *Proceedings of the International Workshop on Selected Areas in Cryptography*, 2008, pp. 309–327.
[18] S. D. Galbraith, F. Hess, and F. Vercauteren, “Hyperelliptic pairings,” *Proceedings of the International Conference on Pairing-Based Cryptography*, 108–131, 2007.
[19] D. Hankerson, V. Scott and A. Menezes, "*Guide to elliptic curve cryptograph"*. Springer, 2004.
[20] A. Joux, “A one round protocol for Tripartite Diffie-Hellman”, *Journal of Cryptology*, *17*(4), 263-276, 2004.