International Journal of Engineering & Technology, 7 (4.34) (2018) 403-406

International Journal of Engineering & Technology

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

Research paper

Constructing Scalar Multiplication via Elliptic Net of Rank Two

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

[1]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[2]*Department of Mathematics, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
**Corresponding author E-mail:norliana_muslim@yahoo.com*

Abstract

Elliptic nets are a powerful method for computing cryptographic pairings. The theory of rank one nets relies on the sequences of elliptic divisibility, sets of division polynomials, arithmetic upon Weierstrass curves, as well as double and double-add properties. However, the usage of rank two elliptic nets for computing scalar multiplications in Koblitz curves have yet to be reported. Hence, this study entailed investigations into the generation of point additions and duplication of elliptic net scalar multiplications from two given points on the Koblitz curve. Evidently, the new net had restricted initial values and different arithmetic properties. As such, these findings were a starting point for the generation of higher-ranked elliptic net scalar multiplications with curve transformations. Furthermore, using three distinct points on the Koblitz curves, similar methods can be applied on these curves.

Keywords: *add; double; elliptic; non-linear; rank.*

1. Introduction

The term "elliptic net" and its concepts were the brainchild of [9]. Currently, such nets are being extensively utilized for pair-based cryptographical optimizations. With their origin from non-linear recurrence relations, first-ranked nets are also known as elliptic divisibility sequences [11] apart from having addition and duplication properties [7]. Stange described general elliptic nets as the mapping of finite-ranked abelian groups onto integral-related domains (i.e. R). During her talk at Microsoft Research on January 30, 2007, she has described the various applications of elliptic nets in cryptography [10].

Since then, the higher-ranked elliptic nets on Weierstrass curves have been applied in the computation of Tate and r − Ate pairings [6]. Years later, the same theory of elliptic nets which employed polynomials has been applied in the calculation of scalar multiplications [2, 5, 12]; this is the primary goal and interest in this current paper. In the attempt to prove the possibility of developing elliptic nets from a new cryptographic curve, Koblitz curve had been utilized. The latter has been extensively studied for its additional structure that allowed speed-ups in the computations of elliptic curve scalar multiplications by means of implementing sequence of addition and duplication of points.

This study was intended to verify the relationships between elliptic functions, net polynomials, and Koblitz curves. These associations, along with two points [$P = (x_1, y_1)$ and $Q = (x_2, y_2)$] on Koblitz curve, gave rise to net polynomials that were subsequently used to formulate new elliptic net scalar multiplications.

Initially, the Weierstrass and Koblitz curves as well as their arithmetic were revised. Next, the properties of the elliptic functions and their relationships with the Koblitz curves were elucidated. The novel rank-two elliptic net scalar multiplications of the Koblitz curves were then described along with the numerical instances. In the final section of this paper, the study outcomes were concluded.

2. Weierstrass and Koblitz Curve

The famous Weierstrass equation [8] known as an elliptic curve E of $y^2 + axy + by = x^3 + cx^2 + dx + e$ and E is the general solutions of $y^2 = x^3 + Ax + B$. The curve E also has important auxiliary polynomials like $\varphi_m = x(\Psi_m)^2 - \Psi_{m+1}\Psi_{m-1}$ and $4y\Omega_m = \Psi_{m+2}(\Psi_{m-1})^2 - \Psi_{m-2}(\Psi_{m+1})^2$. Meanwhile, φ_m, Ψ_m and Ω_m constitute the set of division polynomials of Weierstrass which are related to a rank-one elliptic net and depicted in the form of $[t]R = \left(\frac{\varphi_t(R)}{\gamma_t(R)^2}, \frac{\omega_t(R)}{\gamma_t(R)^3}\right)$. As for rank-two nets, a set of polynomials in the form of $[n]R_1 + [m]R_2 = \left(\frac{\varphi_{nm}(R_1,R_2)}{\gamma_{nm}(R_1,R_2)^2}, \frac{\omega_{nm}(R_1,R_2)}{\gamma_{nm}(R_1,R_2)^3}\right)$ are considered. However, this study employed a special curve of Weierstrass which is known as Koblitz curve [3]. The two Koblitz curves here were denoted by $y^2 + xy = x^3 + 1$ and $y^2 + xy = x^3 + x^2 + 1$, both of which constituted the sets of all solutions to the equation $y^2 + xy = x^3 + cx^2 + 1$.

Both Weierstrass and Koblitz curves have useful arithmetic properties that can be manipulated. In further detail, the latter possesses add and double properties. Let $E_c : y^2 + xy = x^3 + cx^2 + 1$, where $c \in \{0,1\}$, $P = (x_1, y_1) \in E_c$, $Q = (x_2, y_2) \in E_c$, and $P \neq \pm Q$. Subsequently, the addition $(P + Q)$ is generated by

$$x_3 = \lambda^2 + \lambda - c - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 - x_3, \text{ where } \lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

To double a Koblitz point, let $P = (x_1, y_1) \in E_c$, and $P = Q$. Next, $2P$ is calculated as follows:

$x_3 = \lambda^2 + \lambda - c - x_1 - x_2,$

$y_3 = \lambda(x_1 - x_3) - y_1 - x_3,$ where $\lambda = \dfrac{3x_1^2 + 2cx_1 - y_1}{2y_1 + x_1}.$

After analyzed the elliptic divisibility concept with *n*-dimensional arrays, in [9] came up with the following general definition of elliptic nets:

3. Important Definitions, Lemma and Theorems

Definition 1: *Consider A to be a free, finitely-generated abelian group, while R one of the integral domains. Elliptic nets constitute all maps of W: A → R where W (0) = 0 so in any value of s, t, u, v ∈A,*

$$W(s+t+v)\,W(s-t)\,W(u+v)\,W(u)+W(t+u+v)\,W(t-u)\,W(s+v)\,W(s)+W(u+s+v)\,W(u-s)\,W(t+v)\,W(t)=0 \quad (1)$$

The addition and duplication properties of equation (1) made use of the following elliptic function theorems which have been proposed by [4]:

Theorem 1 (Addition):

Let $z_1 \neq z_2$, while assuming $\rho(z_1)$ and $\rho(z_2)$ to be elliptic functions with $\rho'(z_1)$ and $\rho'(z_2)$ being the differential equations that are associated to $\rho(z_1)$ and $\rho(z_2)$. Hence, the addition of the elliptic functions is given by

$$\rho(z_1+z_2) = \frac{1}{4}\left(\frac{\rho'(z_1)-\rho'(z_2)}{\rho(z_1)+\rho(z_2)}\right)^2 - \rho(z_1) - \rho(z_2) \quad (2)$$

Theorem 2 (Duplication):

For an elliptic function $\rho(z)$ with $\rho'(z)$ and $\rho''(z)$ being the differential equations that are associated with $\rho(z)$, the following relationship holds:

$$\rho(2z) = -\rho(2z) + \frac{1}{4}\left(\frac{\rho''(z)}{\rho'(z)}\right)^2 \quad (3)$$

Additionally, in [9] defined a rank-two elliptic net upon Weierstrass as such:

Definition 2: *Consider* $(z_1, z_2) \in \mathrm{Z}^2$, *then there exists a function* Ω_{v_1,v_2} *in* $\mathbb{C}^2$ *such that*

$$\Omega_{v_1,v_2}(z_1,z_2) = \frac{\sigma(v_1z_1 + v_2z_2)}{\sigma(z_1)^{v_1^2}\,\sigma(z_2)^{v_2^2 - v_1v_2}\,\sigma(z_1+z_2)^{v_1v_2}} \quad (4)$$

Before addressing the properties of the Koblitz function, the following definition needs to be out forward:

Definition 3: *The Koblitz ρ -function can be written as*

$$\rho(z) = \frac{1}{z^2} + \sum_{\omega \in L}\left(\frac{1}{(z-\omega)^2} - \frac{1}{z^2}\right) \quad (5)$$

where L is a lattice in a complex plane such that $L = \{m_1\lambda_1 + m_2\lambda_2 : m_1, m_2 \in \mathbf{Z}\}$ *with* λ_1, λ_2 *being complex numbers.*

Since the Koblitz curve is one of the elliptic functions, then the curve satisfied Theorem 1, Theorem 2, and the following lemma:

Lemma 1:

If ρ is the Koblitz ρ-function, then there are functions of σ and Ω in Koblitz that satisfy the following equations:

$$\rho(z_1) - \rho(z_2) = -\frac{\sigma(z_1+z_2)\sigma(z_1-z_2)}{\sigma(z_1)^2\,\sigma(z_2)^2} \quad (6)$$

$$\rho(v\cdot z) - \rho(w\cdot z) = -\frac{\Omega_{v+w}(z)\Omega_{v-w}(z)\sigma(z_1-z_2)}{\Omega_v(z)^2\,\Omega_w(z)^2} \quad (7)$$

Evidence:
The proof for the above lemma is similar to that of [1], except that the Weierstrass function notation has been transformed into that of a Koblitz function.
Recently, modifications have been made on Stange's elliptic-net method for the calculation of elliptic curve scalar multiplications [2]. Subsequently, the following theorem was proposed:

Theorem 3:

Consider the Weierstrass curve for the finite field $E/F_q : y^2 = x^3 + cx + d$, and that $P = (x_1, y_1)$. A rank-one elliptic net scalar multiplication whose initial values are $W_0 = 0$, $W_1 = W_{-1} = 1$ are denoted by the terms of $kP = (x_{kP}, y_{kP})$ such that

$$x_{kP} = x_P - \frac{W_{k-1,0}\,W_{k+1,0}}{(W_{k,0})^2} \quad (8)$$

$$y_{kP} = \frac{(W_{k-1,0})^2\,W_{k+2,0} - (W_{k+1,0})^2\,W_{k-2,0}}{4y_P(W_{k,0})^3} \quad (9)$$

4. Novel Elliptic Net upon Koblitz

Previous studies have developed elliptic nets, or elliptic net scalar multiplications, upon Weierstrass. Theorem 4 proves the existence of new rank-two elliptic nets upon Koblitz.

Theorem 4:

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points on a Koblitz curve. Hence, the rank-two elliptic net scalar multiplication is generated by ten initial values such that

$$W_{0,0}(P,Q) = 0,$$

$$W_{1,0}(P,Q) = W_{0,1}(P,Q) = W_{1,1}(P,Q) = 1,$$

$$W_{1,-1}(P,Q) = x_2 - x_1 \quad (10)$$

$$W_{-1,1}(P,Q) = x_1 - x_2 \quad (11)$$

$$W_{2,1}(P,Q)=2x_1+x_2-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-\left(\frac{y_2-y_1}{x_2-x_1}\right) \quad (12)$$

$$W_{1,2}(P,Q)=x_1+2x_2-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-\left(\frac{y_2-y_1}{x_2-x_1}\right) \quad (13)$$

$$W_{0,2}(P,Q)=2y_2+x_2 \quad (14)$$

$$W_{2,0}(P,Q)=2y_1+x_1 \quad (15)$$

Evidence:
The elliptic net scalar multiplication upon Koblitz begins with $W_{0,0}(P,Q)=0,$ and $W_{1,0}(P,Q)=W_{0,1}(P,Q)=W_{1,1}(P,Q)=1,$ whose proof arises from Proposition 5.1.1 [9]. Note that these four initial values are identical to W_0, W_1 and W_{-1} in Theorem 3.
The proof for $W_{1,-1}(P,Q)$ and $W_{-1,1}(P,Q)$ can be derived from Lemma 1 such that

$$W_{1,-1}(P,Q)=\rho(Q)-\rho(P)=x_{2.}-x_1$$

$$W_{-1,1}(P,Q)=\rho(P)-\rho(Q)=x_{1.}-x_2$$

Meanwhile, the proof for $W_{2,1}(P,Q)$ can be derived from Lemma 1 and Theorem 1 such that

$$W_{2,1}(P,Q)=\rho(P)-\rho(P+Q)$$

$$=\rho(P)-\left(-\rho(P)-\rho(Q)+\frac{1}{4}\left(\frac{\rho'(P)-\rho'(Q)}{\rho(P)-\rho(Q)}\right)^2\right)$$

$$=2\rho(P)-\rho(Q)-\frac{1}{4}\left(\frac{\rho'(P)-\rho'(Q)}{\rho(P)-\rho(Q)}\right)^2$$

Plugging in $\rho(P)=x_1+\frac{1}{12},\ \rho'(P)=2y_1+x_1,\ \rho(Q)=x_2+\frac{1}{12},$ and $\rho'(Q)=2y_2+x_2$ into $W_{2,1}(P,Q),$ the following equation is obtained:

$$W_{2,1}(P,Q)=2x_1+\frac{1}{6}+x_2+\frac{1}{12}-\frac{1}{4}\left(\frac{2(y_2-y_1)+(x_2-x_1)}{x_2-x_1}\right)^2$$

$$=2x_1+\frac{1}{4}+x_2-\left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+\left(\frac{y_2-y_1}{x_2-x_1}\right)+\frac{1}{4}\right)$$

$$=2x_1+x_2-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-\left(\frac{y_2-y_1}{x_2-x_1}\right)$$

A similar method is used to prove $W_{1,2}(P,Q)$ such that

$$W_{1,2}(P,Q)=\rho(Q)-\rho(P+Q)$$

$$=\rho(Q)-\left(-\rho(P)-\rho(Q)+\frac{1}{4}\left(\frac{\rho'(P)-\rho'(Q)}{\rho(P)-\rho(Q)}\right)^2\right)$$

$$=2\rho(Q)-\rho(P)-\frac{1}{4}\left(\frac{\rho'(P)-\rho'(Q)}{\rho(P)-\rho(Q)}\right)^2$$

$$=2x_2+\frac{1}{4}+x_1-\left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+\left(\frac{y_2-y_1}{x_2-x_1}\right)+\frac{1}{4}\right)$$

$$=2x_2+x_1-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-\left(\frac{y_2-y_1}{x_2-x_1}\right)$$

The proof for equation (14) and (15) can be found in Theorem 3. This completes the proof. Note that the right-hand side of equation (10) until (15) are known as net polynomials.
To speed up the calculation of rank-two nets upon Koblitz with $k\geq 3,$ the following formula are required:

$$W_{2k-1,0}=W_{k+1,0}\left(W_{k-1,0}\right)^3-W_{k-2,0}\left(W_{k,0}\right)^3 \quad (16)$$

$$W_{2k,0}=\left(\frac{W_{k,0}W_{k+2,0}\left(W_{k-1,0}\right)^2-W_{k,0}W_{k-2,0}\left(W_{k+1,0}\right)^2}{W_{2,0}}\right) \quad (17)$$

$$W_{2k-1,1}=W_{k+1,1}W_{k-1,1}\left(W_{k-1,0}\right)^2-W_{k,0}W_{k-2,0}\left(W_{k,1}\right)^2 \quad (18)$$

$$W_{2k,1}=W_{k-1,1}W_{k+1,1}\left(W_{k,0}\right)^2-W_{k-1,0}W_{k+1,0}\left(W_{k,1}\right)^2 \quad (19)$$

$$W_{2k+1,1}=\left(\frac{W_{k-1,1}W_{k+1,1}\left(W_{k+1,0}\right)^2-W_{k,0}W_{k+2,0}\left(W_{k,1}\right)^2}{W_{-1,1}}\right) \quad (20)$$

$$W_{2k+2,1}=\left(\frac{W_{k+1,0}W_{k+3,0}\left(W_{k,1}\right)^2-W_{k-1,1}W_{k+1,1}\left(W_{k+2,0}\right)^2}{W_{2,-1}}\right) \quad (21)$$

Example 1:

Here, the Koblitz curve (in the form of $E_{1:}: y^2+xy=x^3+1$) was selected for rapid application. Let points $P=(0,1)$ and $Q=(1,1)$ with respect to elliptic net. After that, $2P-Q$ is computed.
Solution:
Note that $2P-Q=W_{2,-1}(P,Q),$ and that Lemma 1 can be used to derive $W_{2,-1}(P,Q)=\left(y_1+y_2\right)^2-\left(2x_1+x_2\right)\left(x_1-x_2\right)^2.$ Thus,

$$W_{2,-1}(P,Q)=(1+1)^2-(0+1)(0-1)^2=1.$$

5. Conclusion

This paper presents special curves connected to Weierstrass namely as Koblitz and proposes their net polynomials, along with their properties. Based on the proposed net polynomials arithmetic upon Koblitz curve, the study was extended to construct new elliptic net scalar multiplication of rank two. The presence of net polynomials upon Koblitz curve may yield other possible research. In precise, the addition between two points of Koblitz curve can be extended to three points of Koblitz curve and produce an elliptic net scalar multiplication of rank three.

Acknowledgement

Our heartfelt gratitude goes to Universiti Putra Malaysia in view of their funding of the presentation of this study during the 26th National Symposium on Mathematical Science 2018 (grant code: GP/2018/9595200).

References

[1] Chandrasekharan, K. (1985). Elliptic functions. Springer-Verlag.
[2] Kanayama, N., Liu, Y., Okamoto, E., Saito, K., Teruya, T., & Uchiyama, S. (2014). Implementation of an elliptic curve scalar multiplication method using division polynomials. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 97(1), 300–302.
[3] Koblitz, N. (1991). CM curves with good cryptographic properties. Proceedings of the Annual International Cryptology Conference, pp. 279-287.
[4] Lang, S. (1973). Elliptic functions. Addison-Wesley.
[5] Muslim, N., & Said, M. R. (2018). Elliptic net scalar multiplication using generalized equivalent elliptic divisibility sequence. Proceedings of the 6th International Cryptology and Information Security Conference, pp. 9–25.
[6] Ogura, N., Kanayama, N., Uchiyama, S., & Okamoto, E. (2011). Cryptographic pairings based on elliptic nets. Proceedings of the International Workshop on Security, pp. 65-78.
[7] Shipsey, R. (2000). Elliptic divisibility sequences. PhD thesis, University of London.
[8] Silverman, J. H. (1986). The arithmetic of elliptic curve. Springer-Verlag.
[9] Stange, K. E. (2008). Elliptic net and elliptic curve. PhD thesis, Brown University.
[10] Stange, K. E (2007). Elliptic nets with applications to cryptography. https://www.microsoft.com/en-us/research/video/elliptic-nets-with-applications-to-cryptography/.
[11] Ward, M. (1948). Memoir on elliptic divisibility sequences. American Journal of Mathematics, 70(1), 31–74.
[12] Muslim, N., & Said, M. R. M. (2017). Elliptic net and its cryptographic application. AIP Conference Proceedings, 1905(1), 030025.