Chapter 4

Elliptic Net Scalar Multiplication upon Koblitz and Twisted Edward Curves

Norliana Muslim & Mohamad Rushdan Md Said

Institute for Mathematical Research, Universiti Putra Malaysia

norliana_muslim@unisel.edu.my

ABSTRACT

Elliptic net scalar multiplication provides an alternative method to compute elliptic curve point multiplication. The elliptic net scalar multiplication was initiated with division polynomials in the Weierstrass curves. However, the usage of scalar multiplication via elliptic net for computing scalar multiplications in Koblitz and Twisted Edward curves have yet to be reported. Hence, this study entailed investigations into the generation of point multiplication upon supersingular and non-supersingular Koblitz and Twisted Edward curves. The objectives outlined in this study are to examine the relationships between division polynomials with Koblitz curves and division polynomials with Twisted Edward curves. In this study, the explicit formulae in x and y coordinates for each corresponding Koblitz and Twisted Edward curves were proposed. New analysis on the cost of arithmetic operations such as addition, multiplication, squaring and inversion in elliptic net scalar multiplication upon Weierstrass, Koblitz and Twisted Edward curves are compared and discussed. The proposed elliptic net scalar multiplications have the potential to be developed as smart cards or an Android device in the internet of things.

Key Words: elliptic, division polynomials, Koblitz, non-linear, Twisted Edward.

1. INTRODUCTION

Koblitz (1987) independently proposed the elliptic curve cryptosystem, which relies on the difficulty of discrete logarithmic problem in the group of rational points on an elliptic curve. Scalar multiplication is one of the major activities and difficulties in elliptic curve cryptosystems. Scalar multiplication speed plays an important role in the efficiency of the whole system. Elliptic curves can be represented in different ways. Different forms of elliptic curves have been extensively studied over the past two decades to obtain faster scalar multiplications. One significant family of elliptic curves includes Weierstrass (Silverman, 1986).

Meanwhile, the elliptic net of rank one was defined by Morgan Ward as an elliptic divisibility sequence (Ward, 1948). After studying the non-linear recurrence theory (Shipsey, 2000), Stange introduced a mapping from a finite rank Abelian group to an integral domain R, which was called an elliptic net (Stange, 2007). Since then, elliptic net upon Weierstrass

with its higher rank has been applied to compute Tate and r-Ate pairing (Ogura et al., 2011). In addition, the same theory of elliptic net has been employed to calculate scalar multiplication (Kanayama et al., 2014), which is the primary goal and interest in this paper. The first elliptic net scalar multiplication was applied to the Weierstrass curve using Weierstrass's division polynomials. Nevertheless, in the attempt to prove the possibility to construct scalar multiplication via elliptic net using new cryptographic curves, the Koblitz and Twisted Edward curves that related to Weierstrass, had been utilized.

The first objective of this study is to define the explicit formulas of the novel elliptic net scalar multiplications upon two groups of elliptic curves, namely as Koblitz and Twisted Edward curves. The second objective is to analyze the cost of arithmetic operations of the new schemes. The study outcomes are meant to verify the correlations between elliptic divisibility sequences, division polynomials, and Koblitz curves. These correlations, along with the coordinates of multiples of a point P = (x,y) on Koblitz and Twisted Edward curves, form non-linear recurrences that were used to construct new elliptic net scalar multiplication. Furthermore, the cost of arithmetic operations for the new elliptic net scalar multiplication will be evaluated and discussed.

In Section 2, this study introduces the preliminaries topics such as elliptic curve Weierstrass, elliptic net and its scalar multiplication. Section 3 presents the initial division polynomials and their relationships with Koblitz and Twisted Edward curves. After that, the novel elliptic net scalar multiplications are depicted in Section 4, along with its explicit formulas. Meanwhile, Section 5 discusses the computational cost of the novel elliptic net scalar multiplications. The final section concludes the study outcomes.

2. PRELIMINARIES

This section presents several significant concepts that had been applied throughout this study.

2.1 Elliptic Curve Weierstrass

Elliptic curves have been widely researched in algebraic geometry and number theory since the mid-nineteenth century. More lately, the elliptic curves have been used to devise efficient algorithms to factor big integers (Lenstra, 1987) or to prove primality (Atkin, A. O. L. & Morain, 1993). The elliptic curves also disclosed usefulness in the building of cryptosystems [18, 20]. In present, there are many models of cryptographic curves such as Weierstrass (Silverman, 1986), Koblitz (N Koblitz, 1991), Hessian (Hesse, 1844), Huff (Huff, 1948), Montgomery (Montgomery, 1987) and Twisted Edward (Bernstein et al., 2008). These models sometimes allow for more efficient computation on elliptic curves or provide other features of interest to cryptographers.

Division polynomials for Weierstrass curves are well known and play a key role in the theory of elliptic curves. They can be used to find a formula for the n-th multiple of the point (x, y) in terms of x and y. The following Weierstrass equation was introduced as the elliptic curve E for a set of algebraic solutions with $y^2 = x^3 + Ax + B$, whereby $y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$. Generally, the Weierstrass curve has division polynomials expression of $d_2 = b_1^2 + 4b_2$, $d_4 = 2b_4 + b_1b_3$, $d_6 = b_3^2 + 4b_6$, $d_8 = b_1^2b_6 + 4b_2b_6 - b_1b_3b_4 + b_2b_3^2 - b_4^2$ and $D = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$.

2.2 Elliptic Net

Stange (2008) came up with generalized forms of elliptic divisibility sequences in higher-order dimensions as well as specific fields and called it as an elliptic net. The elliptic net is a function of W: $A \rightarrow R$ from finite-rank free Abelian groups, A, to integral domains, R, which uphold the said feature.

$$W(p+q+s)W(p-q)W(r+s)W(r)+W(q+r+s)W(q-r)$$
$$W(p+s)W(p)+W(r+p+s)W(r-p)W(q+s)W(q)=0, \quad \forall p,q,r,s \in A.$$

2.3 Elliptic Net Scalar Multiplication upon Weierstrass

Consider the elliptic curve Weierstrass and $P=(x_P,y_P)$ is a point on the Weierstrass curve. An elliptic net scalar multiplication using Weierstrass's division polynomials (Kanayama et al., 2014) can be defined as finding $kP=(x_{kP},y_{kP})$ with the following:

$$x_{kP}=x_P-\frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}^2(k)}$$

$$y_{kP}=\frac{\hat{W}^2(k-1)\hat{W}(k+2)-\hat{W}^2(k+1)\hat{W}(k-2)}{4y_P\hat{W}^3(k)}$$

Among several cryptographic curves that have been presented in the literature, this study chooses Koblitz and Twisted Edward curves. The main criteria for the selection are the initial values of the division polynomials. This means that the first two initial value of division polynomials must be $\psi_0=0$ and $\psi_1=1$. In other words, for any cryptographic curve that does not hold these criteria, then the curve is not suitable to be utilized with the theory of elliptic net scalar multiplication.

3. METHODOLOGY

3.1 Koblitz curves

Koblitz (1991) introduced two common types of curves called non-super singular and super singular curve. These curves are denoted in the following:

$$y^2+b_1xy=x^3+b_2x^2+b_6 \quad (1)$$
$$y^2+b_3y=x^3+b_4x+b_6 \quad (2)$$

The non-super singular Koblitz curve, as portrayed in equation 1, has the usual quantities of $d_2=b_1^2+4b_2$, $d_4=0$, $d_6=4b_6$, $d_8=b_1^2b_6+4b_2b_6$, and $D=-d_2^2d_8-27d_6^2$. In equation 1, the division polynomials upon Koblitz curve was derived from Silverman (1986), as shown below:

$$\psi_0=0, \quad \psi_1=1, \quad \psi_2=2y+b_1x \quad (3)$$
$$\psi_3=3x^4+d_2x^3+3d_6x+d_8 \quad (4)$$
$$\psi_4=(2y+b_1x)(2x^6+d_2x^5+10d_6x^3+10d_8x^2+d_2d_8x-d_6^2) \quad (5)$$

The usual quantities for super singular curve Koblitz are $d_2 = 0$, $d_4 = 2b_4$, $d_6 = b_3^2 + 4b_6$, $d_8 = -b_4^2$, $D = -8d_4^3 - 27d_6^2$ and its division polynomials are presented in the following:

$$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y + b_3 \tag{6}$$

$$\psi_3 = 3x^4 + 3d_4x^2 + 3d_6x + d_8 \tag{7}$$

$$\psi_4 = \left(2y + b_3\right)\left(2x^6 + 5d_4x^4 + 10d_6x^3 + 10d_8x^2 - d_4d_6x + d_4d_8 - d_6^2\right) \tag{8}$$

3.2 Twisted Edward Curve

Initially, the Twisted Edward curve has been introduced to speed up the addition and doubling on elliptic curves (Bernstein & Lange, 2007). The general form of Twisted Edward curve is $ax^2 + y^2 = 1 + dx^2y^2$. The division polynomials of Twisted Edward curve were defined by Bernstein et. al (2008) as follow:

$$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = \frac{(a-d)(1+y)}{x\left(2(1-y)\right)} \tag{9}$$

$$\psi_3 = \frac{(a-d)^3\left(a + 2ay - 2dy^3 - dy^4\right)}{\left(2(1-y)\right)^4} \tag{10}$$

$$\psi_4 = \frac{2(a-d)^6\, y(1+y)\left(a - dy^4\right)}{x\left(2(1-y)\right)^7} \tag{11}$$

For both types of Koblitz curves and Twisted Edward curves with $m \geq 2$, the recurrence relations for ψ_m are:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \tag{12}$$

$$2y\psi_{2m} = \psi_m\left(\psi_{m+1}\psi_{n-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \tag{13}$$

4. FINDINGS

The discussion in this section focuses on the main objective of the present study which is to present the explicit formulae of the elliptic net scalar multiplication upon Koblitz and Twisted Edward curves. In addition, the comparison of the cost-ratios will be applied to evaluate the cost of arithmetic operations that will be discussed in Section 5.

4.1 Elliptic Net Scalar Multiplication upon Koblitz Curves

Let $P = (x_1, y_1)$ and the multiple points (N Koblitz, 1991) were implemented to arrive at the set of division polynomials φ_n, ψ_n, and ω_n upon non-super singular curve:

$$x_n = x_1 - \frac{\hat{W}(n-1)\hat{W}(n+1)}{\hat{W}^2(n)} \tag{14}$$

$$y_n = x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(n-1)\hat{W}(n+1)}{\hat{W}^2(n)}\right) + \frac{x_1\hat{W}^2(n+1)\hat{W}(n-2)}{\hat{W}^3(n)} \tag{15}$$

while for super singular curve Koblitz, the set of division polynomials is as given below:

$$x_n = x_1 - \frac{\hat{W}(n-1)\hat{W}(n+1)}{\hat{W}^2(n)} \tag{16}$$

$$y_n = y_1 + b_3 + \left(x_1^2 + b_4\right)\left(\frac{\hat{W}(n+1)\hat{W}(n-1)}{\hat{W}(2)\hat{W}^2(n)}\right) + \frac{\hat{W}^2(n+1)\hat{W}(n-2)}{\hat{W}(2)\hat{W}^3(n)} \tag{17}$$

Note that from the above, equation 14 and equation 16 are identical to x_k in the elliptic net scalar multiplication upon Weierstrass curve.

4.2 Elliptic Net Scalar Multiplication upon Twisted Edward Curves

Suppose that $P = (x_1, y_1)$ is a point on the Twisted Edward curve. The elliptic net scalar multiplication upon this curve, $[n]P = (x_n, y_n)$ can be derived as:

$$x_n = \frac{\hat{W}^2(n)}{\hat{W}(2n)}\left[\frac{(a-d)(1+y)\hat{W}^2(n)}{2(1-y)} - 2\hat{W}(n-1)\hat{W}(n+1)\right] \tag{18}$$

$$y_n = \frac{(a-d)y_1\hat{W}^2(n) - 2(1-y_1)\hat{W}(n-1)\hat{W}(n+1)}{(a-d)\hat{W}^2(n) - 2(1-y_1)\hat{W}(n-1)\hat{W}(n+1)} \tag{19}$$

4.3 Numerical example on Elliptic Net Scalar Multiplication upon Non-supersingular Koblitz

In this instance, the non-super singular Koblitz curve was selected for rapid implementation. Note that $b_1 = 1$, $b_2 = 0$, $b_6 = 1$ and $b_6 = 1$ are applied to equation 1. Let $y^2 + xy = x^3 + 1$ and point $P = (-1,0)$ with respect to the elliptic net. After that, 5*P* is calculated.

Solution:
First, the initial values of the elliptic net were obtained from the properties of elliptic net, such that

$$\hat{W}(0) = 0,\ \hat{W}(1) = 1,\ \text{and}\ \hat{W}(2) = 2y + b_1 x = 2(0) + 1(-1) = -1.$$

Next, the terms $\hat{W}(3)$ and $\hat{W}(4)$ were calculated as

$$\hat{W}(3) = 3(1) + 1(-1) + 3(4)(-1) + 1 = -9$$

$$\hat{W}(4) = (-1)\left[2(1) + 1(-1) + 10(4)(-1) + 10(1)(1) + (-1) - 16\right] = 46$$

To continue, the term of $\hat{W}(5)$ and $\hat{W}(6)$ were generated using equation 12 and equation 13 such that

$$\hat{W}(5) = \hat{W}(4)\hat{W}^3(2) - \hat{W}^3(3)\hat{W}(1) = 46(-1) - \left[(-9)^3(1)\right] = 683$$

$$\hat{W}(6) = \frac{\hat{W}(3)\left[\hat{W}(5)\hat{W}^2(2) - \hat{W}(1)\hat{W}^2(4)\right]}{\hat{W}(2)}$$
$$= \frac{(-9)\left[(683)(1) - 1(46^2)\right]}{-1} = -12897$$

Then,

$$x_5 = x_1 - \frac{\hat{W}(5-1)\hat{W}(5+1)}{\hat{W}^2(5)}$$
$$= x_1 - \frac{\hat{W}(4)\hat{W}(6)}{\hat{W}^2(5)}$$
$$= -1 - \frac{46(-12897)}{(683)^2} = \frac{126773}{683^2}$$

The *y*-coordinate was computed with equation 15, such that

$$y_5 = x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(5-1)\hat{W}(5+1)}{\hat{W}^2(5)}\right) + \frac{x_1\hat{W}^2(5+1)\hat{W}(5-2)}{\hat{W}^3(5)}$$
$$= x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(4)\hat{W}(6)}{\hat{W}^2(5)}\right) + \frac{x_1\hat{W}^2(6)\hat{W}(3)}{\hat{W}^3(5)}$$
$$= -1 + 0 + 0 + \frac{(-1)(-12897)^2(-9)}{(683)^3} = \frac{1178381494}{683^3}$$

Therefore, when $P = (-1,0)$, $5P = \left(\frac{126773}{683^2}, \frac{1178381494}{683^3}\right)$.

5. DISCUSSION

To evaluate the computational cost of arithmetic operations, this study implements the cost-ratios (Lopez and Dahab, 1998) as follow:

$$r_1 = \frac{\text{number of inversion}}{\text{number of multiplication}}$$
$$r_2 = \frac{\text{number of multiplication}}{\text{number of squaring}}$$
$$r_3 = \frac{\text{number of multiplication}}{\text{number of addition}}$$

Let A denotes the number of addition or subtraction, S as the number of squaring, M as the number of multiplication and I be the number of inversions. The experimental values for the cost-ratio in the new elliptic net scalar multiplications are given in Table 1.

Table 1: Comparison of the computational cost of arithmetic operations between ENSM Weierstrass, Koblitz and Twisted Edward Curves.

Curves	Number of arithmetic operation (without repetition)	r_1	r_2	r_3	2I to M
Weierstrass	2A + 3S + 4M + 2I	0.50	1.33	2.00	5M
Non-supersingular Koblitz	3A + 2S + 3M + 2I	0.67	1.50	1.00	4.34M
Supersingular Koblitz	4A + 3S + 4M + 2I	0.50	1.33	1.0	5M
Twisted Edward	2A + 1S + 4M + 2I	0.50	4.00	2.00	5M

As r_2 and r_3 are bigger than r_1, this means the cost of the addition, subtraction and squaring can be neglected. In other words, the main comparison for the computational cost of the new elliptic net scalar multiplications is depending on the cost of r_1. Since there are 2 inversions required for all types of the elliptic net scalar multiplications, then the cost of inversion can be converted to the cost of multiplication. From Table 1, we can conclude that the computational cost of multiplication in the elliptic net scalar multiplication upon non-supersingular Koblitz is 13.2 % faster than other methods.

6. CONCLUSION

The present study has managed to describe the form of non-supersingular Koblitz, super singular Koblitz and Twisted Edward curves and proposes their division polynomials, along with their properties. Based on the proposed division polynomials, the study was extended to define the explicit formulas for the novel elliptic net scalar multiplications. From the new elliptic net scalar multiplications, this study found that the proposed elliptic net scalar multiplications satisfied the non-linear recurrence properties. Furthermore, from the comparison of computational cost of arithmetic, the present study found that the cost of arithmetic operations in the non-supersingular Koblitz was 13.2% faster compared to other methods.

REFERENCES

Atkin, A. O. L. & Morain, F. (1993). Elliptic curves and primality proving. *Mathematics of Computation*, *61*((203)), 29–68.

Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards Curves. *Lecture Notes in Computer Science*, *5023*.

Bernstein, D. J., & Lange, T. (2007). Faster Addition and Doubling on Elliptic Curves. *Advances in Cryptology – ASIACRYPT 2007*, 29–50. https://doi.org/10.1007/978-3-540-76900-2_3

Hesse, O. (1844). Uber die Elimination der Variabeln aus drei algebraischen G ¨ leichun- gen vom zweiten Grade mit zwei Variabeln. *Journal F¨ur Die Reine Und Angewandte Mathematik*, 68–96.

Huff, G. B. (1948). Diophantine problems in geometry and elliptic ternary forms. *Duke Mathematical Journal*, *15*(2), 443–453.

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*, *E97-A*(1), 300–302.

Koblitz, N. (1991). 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, pp. 156–167). Springer, Berlin, Heidelberg.

Koblitz, Neal. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–203. https://doi.org/10.1090/S0025-5718-1987-0866109-5

Lenstra, H. W. (1987). Factoring integers with elliptic curves. *Annual Mathematics*, *126*(2), 649–673.

Montgomery, P. L. (1987). Speeding the Pollard and Elliptic Curve Methods of Factorization.

Mathematics of Computation, *48*(177), 243–264.

Ogura, N., Kanayama, N., Uchiyama, S., & Okamoto, E. (2011). Cryptographic pairings based on elliptic nets. In *Iwata T., Nishigaki M. (eds) Advances in Information and Computer Security. IWSEC 2011. Lecture Notes in Computer Science* (Vol. 7038). Springer, Berlin, Heidelberg.

Shipsey, R. (2000). *"Elliptic Divisibility Sequences."* PhD thesis, University of London.

Silverman, J. H. (1986). *The arithmetic of elliptic curve*. New York: Springer-Verlag.

Stange, K. E. (2007). Elliptic nets and points on elliptic curves. *Algorithmic Number Theory*, (1), 1–4. https://doi.org/10.2140/ant.2011.5.197

Stange, K. E. (2008). *Elliptic Net and Elliptic Curve*. PhD thesis, Brown University.

Ward, M. (1948). Memoir on Elliptic Divisibility Sequences. *American Journal of Mathematics*, *70*(1), 31–74.