Malaysian Journal of Mathematical Sciences 14(3): 373–388 (2020)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Elliptic Net Scalar Multiplication upon Koblitz Curves

Muslim, N.[1,2,3], Yunos, F. *[1,2], Razali, Z.[4], and Said, M. R. M.[1,2]

[1] *Department of Mathematics, Universiti Putra Malaysia, Malaysia*
[2] *Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[3] *Department of Engineering, Universiti Selangor, Malaysia*
[4] *Faculty of Communication, Visual Art and Computing, Universiti Selangor, Malaysia*

E-mail: faridahy@upm.edu.my
* *Corresponding author*

Received: 30 March 2020
Accepted: 20 August 2020

ABSTRACT

Elliptic net scalar multiplication (ENSM) is a recent trend in cryptography. The first ENSM was constructed using short Weierstrass's division polynomials over a prime field. However, the ENSM over binary field is unknown. Hence, this study proposes a scalar multiplication via elliptic net upon Koblitz curves over binary field. The objectives outlined in this study are to investigate the relationships between division polynomials, elliptic divisibility sequences, and two types of Koblitz curve over binary field. Additionally, this study looked into the new relationship established between elliptic net and its scalar multiplication. The explicit formulae for ENSM are proposed and their computational costs of field operations are evaluated and discussed.

Keywords: Binary field, elliptic net, point, scalar multiplication, Weierstrass curve.

1. Introduction

Since year 1948, the relations between linear and non-linear recurrences have intrigued researchers. Some discrete logarithm-based cryptosystems can be transformed into an analogue cryptosystem by using a linear recurrence cipher for security reasons and break impasse. For instance, the ElGamal cryptosystem was improvised to LUCELG by Smith and Skinner (1994), while the Cramer-Shoup was upgraded to LUCCS by Muslim and Said (2009).

The elliptic net of rank one was defined by Ward (1948) as an elliptic divisibility sequence. After studying the non-linear recurrence theory by Shipsey (2000), Stange (2008) introduced a mapping from a finite rank Abelian group to an integral domain R, which was then called an elliptic net. Since then, elliptic net upon Weierstrass with its higher rank has been applied to compute Tate and r-Ate pairing, see Ogura et al. (2011). The literature depicts the ability of non-linear recurrence relations (also known as "elliptic divisibility sequence" in the elliptic net) to aid cryptographic pairing as a computation tool. Furthermore, the same elliptic net method has been used to compute multiple of points, see Kanayama et al. (2014) and Chen et al. (2017). Previous studies have also discussed elliptic net upon short Weierstrass curve and its application, including scalar multiplication in detail by Muslim and Said (2017, 2018a) and Muslim and Said (2018c).

The primary purpose of this paper is to study ENSM upon Koblitz curves. The study outcomes are meant to verify the correlations between elliptic net, division polynomials, and Koblitz curves. These correlations, along with the coordinates of multiple point $P = (x, y)$ on the two types of Koblitz curves, form an elliptic divisibility sequence that was used to construct ENSM.

Section 2 presents a review pertaining to the Weierstrass equation and its division polynomials, followed by a review on elliptic net via Weierstrass. Section 3 proposes the initial division polynomials and their relationships with the two Koblitz curve forms. Then, the novel scalar multiplication via elliptic net is depicted in Section 4, along with an analysis of the cost of field operations. 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 and Division Polynomials

The following Weierstrass equation Silverman (1986) was introduced as an elliptic curve E for a set of algebraic solutions with $y^2 = x^3 + ax + b$, such that

$$E : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6. \tag{1}$$

Generally, Equation (1) has the 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 discriminant $D = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$, with several auxiliary polynomials denoted by

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

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2. \tag{3}$$

Note that Equations (2) and (3) are works for $n \geq 2$. Meanwhile, the division polynomials of ψ_n with $n \geq 2$ will satisfy that

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \tag{4}$$

and for $n \geq 3$,

$$2y\psi_{2n} = \psi_n\left(\psi_{n+1}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right). \tag{5}$$

The set of division polynomials φ_n, ψ_n and ω_n for short Weierstrass can be written as coordinates pair as follows:

$$[n]\,P = (x_n, y_n) = \left(\frac{\varphi_n\,(P)}{\psi_n^2\,(P)}, \frac{\omega_n\,(P)}{\psi_n^3\,(P)}\right). \tag{6}$$

2.2 Elliptic Net upon Weierstrass

The following theorem represents a finitely-generated free Abelian group, see Zomorodian (2005).

Theorem 1. *Let A be a nonzero free Abelian group of finite rank n and K be a nonzero subgroup of G. Then K is a free Abelian of rank $s \leq n$ and there exists a basis $\{x_1, x_2, ..., x_n\}$ for A and $d_1, d_2, ..., d_s \in \mathrm{Z}^+$ where $d_i|d_{i+1}$ for $i = 1, 2, ..., s-1$ such that $d_1x_1, d_2x_2, ..., d_sx_s$ is a basis for K.*

The definition of elliptic divisibility sequence was generalized by Stange (2008) to the n-dimensional array, called elliptic net as follows:

Definition 1. *Consider A as a finitely-generated and free group of Abelians with D be an integral domain. Any map $\hat{W} : A \rightarrow D$ is an elliptic net where $\hat{W}(0,0) = 0$ and such that for all $j, k, t, u \in A$,*

$$\hat{W}(j+k+u)\hat{W}(j-k)\hat{W}(t+u)\hat{W}(t) + \hat{W}(k+t+u)\hat{W}(k-t)$$
$$\hat{W}(j+u)\hat{W}(j) + \hat{W}(t+j+u)\hat{W}(t-j)\hat{W}(k+u)\hat{W}(k) = 0.$$

2.2.1 Properties of Elliptic Net Weierstrass

Consider a point $P = (x_1, y_1)$ from a short Weierstrass in the form of $y^2 = x^3 + ax + b$ over a prime field F_p with initial values of $\hat{W}(0,0) = 0$ and $\hat{W}(1,0) = 1$, wherein several essential properties of rank-one elliptic net can be generated by

$$\hat{W}(2,0) = 2y_1 \tag{7}$$

$$\hat{W}(3,0) = 3x_1^4 + 6ax_1^2 + 12bx_1 - a^2 \tag{8}$$

$$\hat{W}(4,0) = 4y_1\left(x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2x_1^2 - 4abx_1 - 8b^2 - a^3\right). \tag{9}$$

From the above formula, Equations (7) – (9) are required to initialise the rank-one elliptic net. To calculate the next term of the elliptic net, i.e. $\hat{W}(5,0)$, we use Equation (4) with $n = z = 2$ to arrive at the following equation:

$$\hat{W}(5,0) = \hat{W}(4,0)\hat{W}^3(2,0) - \hat{W}^3(3,0)\hat{W}(1,0). \tag{10}$$

Similarly, Equation (5) is required to calculate $\hat{W}(6,0)$ such that $n = z = 3$ and the elliptic net is derived by

$$\hat{W}(6,0) = \frac{\hat{W}(3,0)\left(\hat{W}(5,0)\hat{W}^2(2,0) - \hat{W}(1,0)\hat{W}^2(4,0)\right)}{\hat{W}(2,0)}. \tag{11}$$

The methods applicable in Equations (10) and (11) are known as double and double-add.

3. Methodology

3.1 Koblitz Curves and Division Polynomials

From Equation (1), Koblitz (1991) introduced two common types of curves called non-supersingular and supersingular curves in F_{2^m}. These curves are denoted in the following equations:

$$E : y^2 + b_1xy = x^3 + b_2x^2 + b_6 \tag{12}$$

$$E : y^2 + b_3 y = x^3 + b_4 x + b_6. \tag{13}$$

The non-supersingular Koblitz curve, as portrayed in Equation (12) has the usual quantities of $d_2 = b_1^2 + 4b_2$, $d_4 = 0$, $d_6 = 4b_6$, $d_8 = b_1^2 b_6 + 4b_2 b_6$ and discriminant $D = -d_2^2 d_8 - 27d_6^2$, whereas, the division polynomials upon this curve was derived from Silverman (1986) as shown below:

$$\psi_1 = 1, \psi_2 = b_1 x \tag{14}$$

$$\psi_3 = x^4 + d_2 x^3 + b_6 \tag{15}$$

$$\psi_4 = b_1 x \left(d_2 x^5 + x b_6\right). \tag{16}$$

The usual quantities for Equation (13) are denoted by $d_2 = 0$, $d_4 = 2b_4$, $d_6 = b_3^2 + 4b_6$, $d_8 = -b_4^2$, and discriminant $D = -8d_4^3 - 27d_6^2$. Meanwhile, their division polynomials are as follow:

$$\psi_1 = 1, \psi_2 = b_3 \tag{17}$$

$$\psi_3 = x^4 + b_3^2 x + b_4^2 \tag{18}$$

$$\psi_4 = b_3^5. \tag{19}$$

Note that the division polynomials of non-supersingular in Equations (14) – (16) and the division polynomials of supersingular curve in Equations (17) – (19) satisfy the properties of Equations (4) and (5), hence, Equations (10) and (11), respectively. Next, multiple points by Koblitz (1991) were implemented to arrive at the set of division polynomials φ_n, ψ_n, and ω_n upon the non-supersingular curve as

$$\begin{aligned}[n]P = \Bigg(& x_1 + \frac{\psi_{n-1}(P)\,\psi_{n+1}(P)}{\psi_n^2(P)}, y_1 + x_1 + \left(\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\right) \\ & + \left(x_1^2 + y_1\right)\frac{\psi_{n-1}(P)\,\psi_{n+1}(P)}{\psi_2(P)\,\psi_n^2(P)} + \frac{\psi_{n+1}^2(P)\,\psi_{n-2}(P)}{\psi_2(P)\,\psi_n^3(P)}\Bigg)\end{aligned} \tag{20}$$

while for supersingular curve, the set of division polynomials φ_n, ψ_n and ω_n is as given below:

$$\begin{aligned}[n]P = \Bigg(& x_1 + \frac{\psi_{n-1}(P)\,\psi_{n+1}(P)}{\psi_n^2(P)}, y_1 + b_3 \\ & + \left(x_1^2 + b_4\right)\left(\frac{\psi_{n-1}(P)\,\psi_{n+1}(P)}{\psi_2(P)\,\psi_n^2(P)}\right) + \frac{\psi_{n+1}^2(P)\,\psi_{n-2}(P)}{\psi_2(P)\,\psi_n^3(P)}\Bigg).\end{aligned} \tag{21}$$

3.2 Polynomial Basis Representation in F_{2^m}

Consider $m = 3$ in F_{2^m} for both Equations (12) and (13). In Equation (12), F_{2^3} is constructed using an irreducible polynomial $f(x) = x^3 + x + 1$ and Equation (13), used an irreducible polynomial $f(x) = x^3 + x^2 + 1$ with a root of $g = 010$. The element $g \equiv x \, mod \left(x^3 + x + 1\right)$ is a generator for Equation (12) and the element $g \equiv x \, mod \left(x^3 + x^2 + 1\right)$ is a generator for Equation (13). Therefore, the number of elements in F_{2^3} is equal to 8. The powers of g are listed in Table 1 as follows:

Table 1: Powers of generator $g = 010$.

Irreducible polynomial	0	g^0	g^1	g^2	g^3	g^4	g^5	g^6
$x^3 + x + 1$	000	001	010	100	011	110	111	101
$x^3 + x^2 + 1$	000	001	010	100	101	111	011	110

The addition among elements of F_{2^3} based on the irreducible polynomials $x^3 + x + 1$ or $x^3 + x^2 + 1$ is shown in Table 2 as follows:

Table 2: Addition among elements of $F_{2 3}$ in irreducible polynomials $x^3 + x + 1$ or $x^3 + x^2 + 1$.

$+$	0	g^0	g^1	g^2	g^3	g^4	g^5	g^6
0	0	g^0	g^1	g^2	g^3	g^4	g^5	g^6
g^0	g^0	0	g^3	g^6	g^1	g^5	g^4	g^2
g^1	g^1	g^3	0	g^4	g^0	g^2	g^6	g^5
g^2	g^2	g^6	g^4	0	g^5	g^1	g^3	g^0
g^3	g^3	g^1	g^0	g^5	0	g^6	g^2	g^4
g^4	g^4	g^5	g^2	g^1	g^6	0	g^0	g^3
g^5	g^5	g^4	g^6	g^3	g^2	g^0	0	g^1
g^6	g^6	g^2	g^5	g^0	g^4	g^3	g^1	0

Table 3 represents the multiplication among elements of F_{2^3} based on the irreducible polynomiasl $x^3 + x + 1$ or $x^3 + x^2 + 1$.

Table 3: Multiplication among elements of F_{2^3} in irreducible polynomials x^3+x+1 or x^3+x^2+1.

x	0	g^0	g^1	g^2	g^3	g^4	g^5	g^6
0	0	0	0	0	0	0	0	0
g^0	0	g^0	g^1	g^2	g^3	g^4	g^5	g^6
g^1	0	g^1	g^2	g^3	g^4	g^5	g^6	g^0
g^2	0	g^2	g^3	g^4	g^5	g^6	g^0	g^1
g^3	0	g^3	g^4	g^5	g^6	g^0	g^1	g^2
g^4	0	g^4	g^5	g^6	g^0	g^1	g^2	g^3
g^5	0	g^5	g^6	g^0	g^1	g^2	g^3	g^4
g^6	0	g^6	g^0	g^1	g^2	g^3	g^4	g^5

Note that the multiplication among elements of F_{2^3} for both irreducible polynomials are conducted based on Table 1.

4. Results and Discussion

4.1 New Elliptic Net Scalar Multiplication

Previous studies used the equivalence of $\hat{W}(n,0) = c^{n^2-1}W(n,0)$ in elliptic net upon short Weierstrass, see Shipsey (2000). The following proposition represents the equivalent reconsidered for elliptic divisibility sequences, proposed by Muslim and Said (2018a) and Muslim and Said (2018b):

Proposition 4.1. *Let p, u and v as proper elliptic divisibility sequences and satisfy the nonlinear recurrence relations, $p_{m+n}p_{m-n}p_1^2 = p_{m+1}p_{m-1}p_n^2 - p_{n+1}p_{n-1}p_m^2$, $u_{m+n}u_{m-n}u_1^2 = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2$ and $v_{m+n}v_{m-n}v_1^2 = v_{m+1}v_{m-1}v_n^2 - v_{n+1}v_{n-1}v_m^2$. Let c_1, c_2 and c_3 be any constant integer and there are equivalent elliptic divisibility sequences $\{j_n\}, \{k_n\}, \{l_n\}$ such that $j_n = {c_1}^{n^2-1}p_n, k_n = {c_2}^{n^2}u_n$ and $l_n = {c_3}^{n}v_n$. Then, $j_{m+n}j_{m-n} = j_{m+1}j_{m-1}j_n^2 - j_{n+1}j_{n-1}j_m^2$, $k_{m+n}k_{m-n} = k_{m+1}k_{m-1}k_n^2 - k_{n+1}k_{n-1}k_m^2$ and $l_{m+n}l_{m-n} = l_{m+1}l_{m-1}l_n^2 - l_{n+1}l_{n-1}l_m^2$.*

From Proposition 4.1, we can use either $\hat{W}(n,0) = c^{n^2-1}W(n,0)$ or $\hat{W}(n,0) = c^nW(n,0)$ as the elliptic net sequences. However, $c^nW(n,0)$ is in the generalised form which later, will be used to proof the ENSM upon Koblitz curves.

In the next section, we consider $\psi_n(P) = W(n,0)$ for any integer n.

Lemma 4.1. *Let $\{W(n,0)\}$ be the proper elliptic divisibility sequences over finite field F_q with q elements with $W(2,0) \neq 0$. Then there exists an elliptic* *net $\hat{W}(n,0)$ over F_q which is equivalent to the sequence $\{W(n,0)\}$.*

Proof. Assume $\{W(n,0)\}$ is defined over F_q. We can find a square root c of $W(n,0)^{-1}$ that lies in F_q. This means $c^2 = W(2,0)^{-1}$. Let $\hat{W}(n,0) = c^n W(n,0)$ for any integer n. The sequence $\left\{\hat{W}(n,0)\right\}$ is an elliptic net defined over F_q since c and $W(n,0)$ belong to F_q. This completes the proof. $\square$

Theorem 4.1 represents the ENSM upon short Weierstrass based on $\hat{W}(n,0) = c^n W(n,0)$, see Muslim and Said (2018a) and Muslim and Said (2018b).

Theorem 4.1. *Let $\{W(n,0)\}$ defined from Lemma 4.1 and $\hat{W}(2,0) = 2c^2 y_1$. If there is a point $P = (x_1, y_1)$ on short Weierstrass for type $y^2 = x^3 + ax + b$ over F_p, then the rank-one ENSM, $[n]P = (x_n, y_n)$, can be generated as follows:*

$$x_n = x_1 - \frac{\hat{W}(n-1,0)\hat{W}(n+1,0)}{\hat{W}^2(n,0)} \tag{22}$$

$$y_n = \frac{\hat{W}^2(n-1,0)\hat{W}(n+2,0) - \hat{W}^2(n+1,0)\hat{W}(n-2,0)}{4y_1\hat{W}^3(n,0)}. \tag{23}$$

Example 1.

Let $P = (-3, \frac{1}{2})$ be a point on the short Weierstrass, $y^2 = x^3 + 6x + 5$ over F_7, then $3P$ is calculated.

Solution:

Note that, $a = -\frac{11}{4}$, $b = 19$, $\hat{W}(0,0) = 0$, $\hat{W}(1,0) = 1$, and $c = 1$. By using Equation (7), $\hat{W}(2,0) \equiv 2c^2 y_1 \equiv 2\left(\frac{1}{2}\right) \equiv 1 \, mod\, 7$.

Next, $\hat{W}(3,0)$ was computed using Equation (8) such that

$$\hat{W}(3,0) \equiv 243 - \frac{297}{2} - 684 + \frac{121}{16} \equiv -\frac{9553}{16} \, mod\, 7 \equiv 1 \, mod\, 7.$$

The fourth term in the net, $\hat{W}(4,0)$ was derived based on Equation (9) such that

$$\begin{aligned}\hat{W}(4,0) &\equiv 4\left(\frac{1}{2}\right)\left(729 - \frac{4455}{4} - 10260 - \frac{5445}{16} - 627 - 8(19)^2 - \left(-\frac{11}{4}\right)^3\right) \\ &\equiv -\frac{926673}{32} \equiv 2 \, mod\, 7.\end{aligned}$$

Then, x_3 was calculated using Equation (22) such that

$$\begin{aligned} x_3 &\equiv x_1 - \frac{\hat{W}(2,0)\,\hat{W}(4,0)}{\hat{W}^2(3,0)} \\ &\equiv -3 - \frac{1\,(2)}{1^2} \equiv -5 \equiv 2\,mod\,7. \end{aligned}$$

The point y_3 was computed with Equation (23) such that

$$\begin{aligned} y_3 &\equiv \frac{\hat{W}^2(2,0)\hat{W}(5,0) - \hat{W}^2(4,0)\hat{W}(1,0)}{4y_1\hat{W}^3(3,0)} \\ &\equiv \frac{1^2\,(1) - 2^2\,(1)}{4\left(\frac{1}{2}\right)(1^3)} \equiv -\frac{3}{2} \equiv 2\,mod\,7. \end{aligned}$$

Therefore, for $P = (-3, \frac{1}{2})$, then $3P = (2, 2)$. Note that the point $3P$ is on the short Weierstrass curve, and because $y^2 = x^3 - 3x + 4$ implies that $2^2(mod 7) = 2^3 + 6\,(2) + 5(mod\,7)$, so LHS = RHS.

The following theorem depicts the novel ENSM upon non-supersingular Koblitz curve:

Theorem 4.2. *Let $\{W(n,0)\}$ be defined from Lemma 4.1 and $\hat{W}(2,0) = c^2b_1x_1$. If there is a point $P = (x_1, y_1)$ on non-supersingular curve for type $y^2 + b_1xy = x^3 + b_2x^2 + b_6$ over F_{2^m}, then the rank-one ENSM, $[n]P = (x_n, y_n)$, can be derived as*

$$x_n = x_1 + \frac{\hat{W}(n-1,0)\hat{W}(n+1,0)}{\hat{W}^2(n,0)} \tag{24}$$

$$\begin{aligned} y_n = y_1 + x_1 + \left(b_1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(n+1,0)\,\hat{W}(n-1,0)}{b_1\hat{W}^2(n,0)}\right) \\ + \frac{c^2\hat{W}^2(n+1,0)\hat{W}(n-2,0)}{\hat{W}(2,0)\,\hat{W}^3(n,0)}. \end{aligned} \tag{25}$$

Proof. Since working in the binary field, then an additive inverse was applied to Equation (6), to arrive at the following:

$$\frac{\varphi_n(P)}{\psi_n^2(P)} = \frac{x\psi_n^2(P) + \psi_{n+1}(P)\,\psi_{n-1}(P)}{\psi_n^2(P)}.$$

Let $P = (x_1, y_1)$ and the recurrence $\psi_n(P)$ can be transformed to equivalent sequences of $W(n,0)$ by Proposition 4.1, which can be expressed as

$$\begin{aligned} x_n &= x_1 + \frac{\psi_{n-1}(P)\,\psi_{n+1}(P)}{\psi_n^2(P)} \\ &= x_1 + \frac{W(n+1,0)\,W(n-1,0)}{W^2(n,0)} \end{aligned}$$

and because $\hat{W}(n,0) = c^n W(n,0)$, then

$$\begin{aligned} x_n &= x_1 + \frac{c^{-(n+1)}\hat{W}(n+1,0)\,c^{-(n-1)}\hat{W}(n-1,0)}{\left[c^{-n}\hat{W}(n,0)\right]^2} \\ &= x_1 + \frac{c^{-(n+1)-(n-1)}\hat{W}(n+1,0)\,\hat{W}(n-1,0)}{c^{-2n}\hat{W}^2(n,0)} \\ &= x_1 + \frac{\hat{W}(n-1,0)\hat{W}(n+1,0)}{\hat{W}^2(n,0)}. \end{aligned}$$

Referring to y_n in Equation (20) with $\psi_n(P) = W(n,0)$ and $\hat{W}(n,0) = c^n W(n,0)$, then

$$\begin{aligned} y_n &= y_1 + x_1 + \left(\frac{W(n-1,0)\,W(n+1,0)}{W^2(n,0)}\right) + \left(x_1^2 + y_1\right)\left(\frac{W(n-1,0)W(n+1,0)}{(b_1x_1)\,W^2(n,0)}\right) \\ &\quad + \frac{W^2(n+1,0)\,W(n-2,0)}{(b_1x_1)\,W^3(n,0)} \\ &= y_1 + x_1 + \frac{W(n-1,0)W(n+1,0)\left(b_1 + x_1 + \frac{y_1}{x_1}\right)}{b_1W^2(n,0)} + \frac{W^2(n+1,0)\,W(n-2,0)}{W(2,0)\,W^3(n,0)} \\ &= y_1 + x_1 + \frac{c^{-(n-1)}\hat{W}(n-1,0)c^{-(n+1)}\hat{W}(n+1,0)\left(b_1 + x_1 + \frac{y_1}{x_1}\right)}{b_1c^{-2n}\hat{W}^2(n,0)} \\ &\quad + \frac{c^{-2(n+1)}\hat{W}^2(n+1,0)\,c^{-(n-2)}\hat{W}(n-2,0)}{c^{-2}\hat{W}(2,0)\,c^{-3n}\hat{W}^3(n,0)}. \end{aligned}$$

Finally, we can rearrange the above equation to the following:

$$\begin{aligned} y_n &= y_1 + x_1 + \left(b_1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(n+1,0)\,\hat{W}(n-1,0)}{b_1\hat{W}^2(n,0)}\right) \\ &\quad + \frac{c^2\hat{W}^2(n+1,0)\hat{W}(n-2,0)}{\hat{W}(2,0)\,\hat{W}^3(n,0)}. \end{aligned}$$

□

Example 2. In this instance, the non-supersingular Koblitz curve was selected for rapid implementation. If $P = (g^3, g^2)$ is a point on the elliptic curve, $y^2 + xy = x^3 + g^3x^2 + 1$ over F_{2^3}, then $2P$ can be calculated.

Solution:

Note that, $b_1 = 1$, $P = (x_1, y_1) = (g^3, g^2)$, and $\hat{W}(0,0) = 0$. First, the initial values of elliptic net were obtained from Equation (14) such that $\hat{W}(1,0) = 1$ and $\hat{W}(2,0) \equiv 1\left(g^3\right) \equiv g^3 \, mod\left(x^3 + x + 1\right)$.

From Equations (15) and (16), the terms $\hat{W}(3,0)$ and $\hat{W}(4,0)$ were calculated as

$$\hat{W}(3,0) \equiv g^{12} + g^9 + g^0 \equiv g \, mod\left(x^3 + x + 1\right).$$
$$\hat{W}(4,0) \equiv g^{18} + g^6 \equiv g^3 \, mod\left(x^3 + x + 1\right).$$

Then, x_2 was calculated using Equation (24) such that

$$\begin{aligned} x_2 &\equiv x_1 + \frac{\hat{W}(1,0)\,\hat{W}(3,0)}{\hat{W}^2(2,0)} \\ &\equiv g^3 + \frac{g^0 g}{g^6} \equiv \frac{g^3 g^5 + g^0}{g^5} \equiv \frac{g^8 + g^0}{g^5} \equiv g^5 \, mod\left(x^3 + x + 1\right) \equiv g^5. \end{aligned}$$

The point y_2 was computed with Equation (25) such that

$$\begin{aligned} y_2 &\equiv y_1 + x_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right)\left(\frac{\hat{W}(1,0)\hat{W}(3,0)}{\hat{W}^2(2,0)}\right) + \frac{\hat{W}^2(3,0)\,\hat{W}(0,0)}{\hat{W}(2,0)\hat{W}^3(2,0)} \\ &\equiv g^2 + g^3 + (1 + g^3 + \frac{g^2}{g^3})\left(\frac{g^0 g^1}{(g^3)^2}\right) + \frac{g^2(0)}{g^3 g^9} \\ &\equiv g^2 + g^3 + g^{-5} + g^{-2} + g^{-6} \\ &\equiv g^4 \, mod\left(x^3 + x + 1\right) \equiv g^4. \end{aligned}$$

Therefore, when $P = (g^3, g^2)$, then $2P = \left(g^5, g^4\right)$. To validate $2P$, we may substitute $\left(g^5, g^4\right)$ into $y^2 + xy = x^3 + g^3x^2 + 1$ and derive that LHS = RHS such that

$$\begin{aligned} \left(g^4\right)^2 + g^5 g^4 &= \left(g^5\right)^3 + g^3\left(g^5\right)^2 + 1 \\ g^8 + g^9 &= g^{15} + g^{13} + g^0 \\ g^1 + g^2 &= g^1 + g^6 + g^0 \\ g^4 &= g^4. \end{aligned}$$

The following theorem presents the novel ENSM upon supersingular Koblitz curve:

Theorem 4.3. *Suppose that $\{W(n,0)\}$ is defined from Lemma 4.1. If there exists a point $P=(x_1,y_1)$ on supersingular curve for type $y^2+b_3y=x^3+b_4x+b_6$ over F_{2^m}, then the rank-one ENSM, $[n]P=(x_n,y_n)$, can be derived as*

$$x_n = x_1 + \frac{\hat{W}(n-1,0)\hat{W}(n+1,0)}{\hat{W}^2(n,0)} \tag{26}$$

$$\begin{aligned} y_n = \quad & y_1 + b_3 + \left(x_1^2+b_4\right)\left(\frac{\hat{W}\left(n+1,0\right)\hat{W}\left(n-1,0\right)}{\hat{W}\left(2,0\right)\hat{W}^2\left(n,0\right)}\right) \\ & + \frac{\hat{W}^2\left(n+1,0\right)\hat{W}\left(n-2,0\right)}{\hat{W}\left(2,0\right)\hat{W}^3\left(n,0\right)}. \end{aligned} \tag{27}$$

Proof. Note that the point x_n in Equation (26) is identical to that found in Equation (24). In the attempt to determine y_n, again $\hat{W}(n,0)=c^nW(n,0)$ and we make use y_n in Equation (21) to arrive at the following:

$$\begin{aligned} y_n &= y_1 + b_3 + \left(x_1^2+b_4\right)\left(\frac{W\left(n+1,0\right)W\left(n-1,0\right)}{b_3W^2\left(n,0\right)}\right) + \frac{W^2\left(n+1,0\right)W\left(n-2,0\right)}{b_3W^3\left(n,0\right)} \\ &= y_1 + b_3 + \left(x_1^2+b_4\right)\left(\frac{c^{-(n+1)}\hat{W}\left(n+1,0\right)c^{-(n-1)}\hat{W}\left(n-1,0\right)}{\hat{W}\left(2,0\right)\left[c^{-n}\hat{W}\left(n,0\right)\right]^2}\right) + \\ &\quad \frac{\left[c^{-(n+1)}\hat{W}\left(n+1,0\right)\right]^2 c^{-(n-2)}\hat{W}\left(n-2,0\right)}{\hat{W}(2,0)\left[c^{-n}\hat{W}\left(n,0\right)\right]^3} \\ &= y_1 + b_3 + \left(x_1^2+b_4\right)\left(\frac{c^{-2n}\hat{W}\left(n+1,0\right)\hat{W}\left(n-1,0\right)}{\hat{W}\left(2,0\right)c^{-2n}\hat{W}^2\left(n,0\right)}\right) + \\ &\quad \frac{c^{-3n}\hat{W}^2\left(n+1,0\right)\hat{W}\left(n-2,0\right)}{\hat{W}(2,0)c^{-3n}\hat{W}^3\left(n,0\right)} \\ &= y_1 + b_3 + \left(x_1^2+b_4\right)\left(\frac{\hat{W}\left(n+1,0\right)\hat{W}\left(n-1,0\right)}{\hat{W}\left(2,0\right)\hat{W}^2\left(n,0\right)}\right) + \frac{\hat{W}^2\left(n+1,0\right)\hat{W}\left(n-2,0\right)}{\hat{W}\left(2,0\right)\hat{W}^3\left(n,0\right)}. \end{aligned}$$

□

Example 3.

Let $P = (g^5, g^0)$ be a point on the supersingular curve of the type $y^2 + y = x^3 + x + 1$ over F_{2^3}. Then, $3P$ is calculated.

Solution:

Note that $b_3 = b_4 = b_6 = 1$ are applied to Equation (13). First, set $\hat{W}\,(0,0) = 0$ and from Equation (17), we have $\hat{W}\,(1,0) \equiv \hat{W}\,(2,0) \equiv 1 \equiv g^0 mod\left(x^3 + x^2 + 1\right).$

The terms $\hat{W}\,(3,0)$ and $\hat{W}\,(4,0)$ were calculated by referring to Equations (18) and (19) as

$$\hat{W}\,(3,0) \equiv \left(g^5\right)^4 + g^5 + g^0 \equiv g^6 + g^5 + g^0 \equiv g^2\ mod\left(x^3 + x^2 + 1\right).$$
$$\hat{W}\,(4,0) \equiv 1 \equiv g^0\ mod\left(x^3 + x^2 + 1\right).$$

Next, x_3 was generated from Equation (26) such that

$$\begin{aligned} x_3 &\equiv x_1 + \frac{\hat{W}\,(2,0)\,\hat{W}\,(4,0)}{\hat{W}^2\,(3,0)} \\ &\equiv g^5 + \frac{g^0 g^0}{g^4} \equiv g^5 + g^{-4} \equiv g^6\ mod\left(x^3 + x^2 + 1\right) \equiv g^6. \end{aligned}$$

The point y_3 was computed with Equation (27) such that

$$\begin{aligned} y_3 &\equiv y_1 + b_3 + \left(x_1^2 + b_4\right)\left(\frac{\hat{W}(4,0)\hat{W}(2,0)}{\hat{W}(2,0)\hat{W}^2(3,0)}\right) + \frac{\hat{W}^2\,(4,0)\,\hat{W}\,(1,0)}{\hat{W}(2,0)\hat{W}^3\,(3,0)} \\ &\equiv g^0 + g^0 + \left(\left(g^5\right)^2 + g^0\right)\left(\frac{g^0 g^0}{g^0 g^4}\right) + \frac{g^0 g^0}{g^0 g^6} \equiv g^{-6} + g^6 + g^{-4} \\ &\equiv g^0\ mod\left(x^3 + x^2 + 1\right) \equiv g^0. \end{aligned}$$

Therefore, for $P = (g^5, g^0)$, the multiple $3P = \left(g^6, g^0\right)$. To verify the point of $3P$, plug in $\left(g^6, g^0\right)$ into $y^2 + y = x^3 + x + 1$ to show that LHS = RHS such that

$$\begin{aligned} \left(g^0\right)^2 + g^0 &= \left(g^6\right)^3 + g^6 + g^0 \\ g^0 + g^0 &= g^{18} + g^6 + g^0 \\ g^0 + g^0 &= g^4 + g^6 + g^0 \\ 000 &= 000. \end{aligned}$$

4.2 Complexity Analysis

This section evaluates the cost of field operations in the ENSM over F_p and F_{2^m}. On evaluating the field operations, the cost of addition field or subtraction field can be neglected since this cost of operation is small compared to squaring, multiplication, and inversion. Let S denotes the number of squaring, M as the number of multiplication and I be the number of inversion. The number of field operations without repetition in the ENSM via elliptic net are given in Table 5.

Table 4: Computational cost of field operations in ENSM upon different curves and fields.

Curve	Formula x_n	Formula y_n	Total
Short Weierstrass in Fp (refer to Equations (22) and (23))	$1S + 1M + 1I$	$2S + 4M + 1I$	$3S + 5M + 2I$
Non-supersingular Koblitz in F_{2^m} (refer to Equations (24) and (25))	$1S + 1M + 1I$	$1S + 5M + 2I$	$2S + 6M + 3I$
Supersingular Koblitz in F_{2^m} (refer to Equations (26) and (27))	$1S + 1M + 1I$	$2S + 5M + 2I$	$3S + 6M + 3I$

The experiments indicate that the x-coordinate for ENSM in F_p and F_{2^m} have equal cost of field operations. However, a slight difference was noted for the y-coordinate. In prime field, the squaring cost is 80% from the multiplication cost, thus indicating that $1S{=}0.8M$. This can be reduced by considering modulo to $1S{=}0.6M$. However, in binary field, the cost of squaring can be neglected, see Ciet et al. (2006). Therefore, the overall cost of ENSM for (a) short Weierstrass over prime field is $6.8M{+}2I$; (b) nonsupersingular Koblitz over binary field is $6M{+}3I$; and (c) supersingular Koblitz over binary field is $6M{+}3I$.

5. Conclusion

The ENSM upon short Weierstrass over prime field has been reviewed together with an experimental value. This paper presented Koblitz curves of the type non-supersingular and supersingular and discussed their division polynomials, along with their properties. Based on the Koblitz curves' division polynomials and non-linear recurrence properties, the study was extended to develop rank-one ENSM. The cost of field operations in ENSM was evaluated based on the prime and binary fields. The presence of ENSM using division polynomials may yield other possible applications. In other words, the theory of ENSM can be applied to other suitable cryptographic curves, including Twisted Edwards curve for type $ax^2 + y^2 = 1 + dx^2y^2$.

Acknowledgement

This research was financially supported by Universiti Putra Malaysia Grant under Putra Grant Number GP/2018/9595200.

References

Chen, B., Hu, C., and Zhao, C. (2017). A note on scalar multiplication using division polynomials. *IET Information Security*, 11:195–198.

Ciet, M., Joye, M., Lauter, K., and Montgomey, P. L. (2006). Trading inversions for multiplications in elliptic curve cryptography. *Designs, Codes, and Cryptography*, 39:189–206.

Kanayama, N., Liu, Y., Okamoto, E., Saito, K., Teruya, T., and 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:300–302.

Koblitz, N. (1991). *Constructing Elliptic Curve Cryptosystems in Characteristic 2*. Heidelberg Berlin: Springer.

Muslim, N. and Said, M. R. M. (2009). A new cryptosystem analogous to lucelg and cramer-shoup. *International Journal of Cryptology Research*, 1:191–204.

Muslim, N. and Said, M. R. M. (2017). Elliptic net and its cryptographic application. In *Proceedings of the 13th IMT-GT International Conference on Mathematics, Statistics and their Applications (ICMSA2017)*, volume 1905, Kedah, Malaysia.

Muslim, N. and Said, M. R. M. (2018a). Elliptic net scalar multiplication using generalized equivalent elliptic divisibility sequence. In *Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018*, pages 19–25.

Muslim, N. and Said, M. R. M. (2018b). Generalizing equivalent elliptic divisibility sequence for elliptic net scalar multiplication. *International Journal of Cryptology Research*, 1:11–23.

Muslim, N. and Said, M. R. M. (2018c). Scalar multiplication via elliptic nets with application to cryptography. *International Journal of Engineering and Technology*, 7:153–156.

Ogura, N., Kanayama, N., Uchiyama, S., and Okamoto, E. (2011). *Cryptographic pairings based on elliptic nets*. Heidelberg Berlin: Springer.

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

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

Smith, P. J. and Skinner, C. (1994). A public-key cryptosystem and a digital signature system based on the lucas function analogue to discrete logarithms. *In Preproceedings Asiacrypt'94*, pages 298–306.

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.*, 70:31–74.

Zomorodian, A. J. (2005). *Topology for Computing (Cambridge Monographs on Applied and Computational Mathematics)*. New York: Cambridge University Press.