International Journal of Cryptology Research 8(2): 11 - 23 (2018)

Generalizing Equivalent Elliptic Divisibility Sequence for Elliptic Net Scalar Multiplication

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

[1]*Institute for Mathematical Research, Universiti Putra Malaysia*
[2]*Faculty of Engineering and Life Sciences, Universiti Selangor*

E-mail: norliana_muslim@unisel.edu.my
[*]*Corresponding author*

ABSTRACT

Elliptic Net is a powerful method to compute cryptographic pairings or scalar multiplication. The elliptic net rank one originated from the nonlinear recurrence relations, also known as the elliptic divisibility sequence. In this paper, a generalization of equivalent sequences is defined. Combining the new generalization with a few restrictions on the initial value, the paper further proposes and discusses an elliptic net scalar multiplication of rank one for Weistrass equation and non-singular elliptic curve.

Keywords: Equivalence, Net, Divisible, Polynomials

1 INTRODUCTION

Elliptic net scalar multiplication was first introduced by Japanese cryptographer (Kanayama et al., 2014). His method adapts Stanges net theory (Stange, 2007b) and some research directions of elliptic net can be seen in previous year (Muslim and Said, 2017). The rich structure of elliptic net and its scalar multiplication resulted in cryptography field, in which it is used to solve elliptic curve discrete logarithm problem (Lauter and Stange, 2008), compute Ate pairing (Matsuda et al., 2009), and optimize pairing (Tang et al., 2014). Continuous contributions in cryptosystem and net developments are achieved since the discrete log problem on elliptic curve was successfully reduced to a finite field.

In this paper, we begin by reviewing elliptic divisibility sequence with its equivalent properties and division polynomials of the elliptic curve. Next, we propose the elliptic net scalar multiplication of rank one by using new properties. Finally, we discuss the simplification of elliptic net initial values.

2 ELLIPTIC DIVISIBILITY SEQUENCE

Morgan Ward introduced an elliptic divisibility sequence in the form of $h_{m+n} h_{m-n}h_1^2 = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ as a special sequence with the initial value of $h_0 = 0$, $h_1 = 1$, $h_2 \neq 0$ and $h_3 \neq 0$ (Ward, 1948). Meanwhile, the first cryptographic applications of these sequences have been discussed by Shipsey (2000) while the applications were extended by Stange (2007a) and Kanayama et al. (2014). By considering $n = 2$ and $h_1^2 = 1$, two frequently used equations are $h_{2n}h_2 = h_{n+2}h_nh_{n-1}^2 - h_nh_{n-2}h_{n+1}^2$ and $h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3$. Some important topics of elliptic divisibility sequence for cryptographers are the indices (Silverman and Stange, 2011), rank of apparition Gezer and Bizim (2009) and equivalence (Bizim, 2009, Shipsey, 2000). The equivalence theory will be discussed in the next section.

2.1 Proper and improper sequences

The divisibility sequence can be categorized to proper and improper. A proper elliptic divisibility sequence satisfies the conditions that $h_0 = 0, h_1 = 1$ and $h_2h_3 \neq 0$.

For sequences which do not satisfy one or more of these conditions and are therefore known as improper elliptic divisibility sequences. For examples, the integer sequences of $\{0, 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, \cdots\}$ and $\{1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043, \cdots\}$ constitute the proper and improper forms of the said sequences that meet the condition such that for $n|m$ then $h_n|h_m$.

2.2 Equivalent elliptic divisibility sequences

The term of equivalent sequences only can be used for proper sequences, in which the $h_0 = 0,\ h_1 = 1,\ h_2 \cdot h_3 \neq 0$ and h_4 divides h_2. Now, we will show how the equivalent sequences satisfy the nonlinear recurrence relations.

Proposition 2.1. *Consider 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 integers 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 $l_{m+n}l_{m-n} = l_{m+1}l_{m-1}l_n^2 - l_{n+1}l_{n-1}l_m^2$.*

Proof. Proof for $j_n = c_1^{n^2-1}p_n$ with $j_{m+n}j_{m-n} = j_{m+1}j_{m-1}j_n^2 - j_{n+1}j_{n-1}j_m^2$ is similar to Shipsey (2000). We will continue to prove for k_n and l_n. Since p, u and v are proper elliptic divisibility sequences, i.e $p_1 = u_1 = v_1 = 1$ then the nonlinear recurrence relations can be simplified to $p_{m+n}p_{m-n} = p_{m+1}p_{m-1}p_n^2 - p_{n+1}p_{n-1}p_m^2$, $u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2$ and $v_{m+n}v_{m-n} = v_{m+1}v_{m-1}v_n^2 - v_{n+1}v_{n-1}v_m^2$.

For

$$
\begin{aligned}
k_{m+n}k_{m-n} &= c_2^{(m+n)^2}u_{m+n}c_2^{(m-n)^2}u_{m-n} && (1)\\
&= c_2^{2(m^2+n^2)}\left(u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2\right) && (2)\\
&= c_2^{m^2}u_{m+1}c_2^{m^2}u_{m-1}c_2^{2n^2}u_n^2 - c_2^{n^2}u_{n+1}c_2^{n^2}u_{n-1}c_2^{2m^2}u_m^2 && (3)\\
&= c_2^{(m+1)^2}u_{m+1}c_2^{(m-1)^2}u_{m-1}\left(c_2^{n^2}u_n\right)^2 - c_2^{(n+1)^2}u_{n+1}c_2^{(n-1)^2}\\
&\quad u_{n-1}\left(c_2^{m^2}u_m\right)^2 && (4)\\
&= k_{m+1}k_{m-1}k_n^2 - k_{n+1}k_{n-1}k_m^2 && (5)
\end{aligned}
$$

and for

$$
\begin{aligned}
l_{m+n}l_{m-n} &= c_3^{m+n}v_{m+n}c_3^{m-n}v_{m-n} && (6)\\
&= c_3^{2m}v_{m+n}v_{m-n} && (7)\\
&= c_3^{2m}\left(v_{m+1}v_{m-1}v_n^2 - v_{n+1}v_{n-1}v_m^2\right) && (8)\\
&= c_3^{m+1}v_{m+1}c_3^{m-1}v_{m-1}\cdot v_n^2 - v_{n+1}v_{n-1}(c_3^m v_m)^2 && (9)\\
&= l_{m+1}l_{m-1}l_n^2 - l_{n+1}l_{n-1}l_m^2 && (10)
\end{aligned}
$$

■

The above steps complete the proof. From Proposition 2.1, we can say that any elliptic divisibility sequences are equivalent if there exist integers c_1, c_2 and c_3 such that for all n, $c_1^{n^2-1}p_n = c_2^{n^2}u_n = c_3^n v_n$. The sequence of $c_3^n v_n$ is a generalization form that will be further used to construct elliptic net scalar multiplication.

3 ELLIPTIC CURVE

The general Weierstrass equation (Silverman, 1986) can be defined as E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where an elliptic curve E is the set of algebraic solutions of $y^2 = x^3 + ax + b$ whereby a and b are real numbers with the following expression:

$$b_2 = a_1^2 + 4a_2 \tag{11}$$
$$b_4 = 2a_4 + a_1 a_3 \tag{12}$$
$$b_6 = a_3^2 + 4a_6 \tag{13}$$
$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \tag{14}$$
$$D = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \tag{15}$$

The auxiliary polynomials denoted by ϕ_n, ω_n are as follow:

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1} \tag{16}$$
$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2 \tag{17}$$

Then, for the curve E of the polynomials $\phi_n(P), \psi_n, \omega_n$ can be written as,

$$[n]\,P = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3}\right) \tag{18}$$

The division polynomials ψ_n in x, y and the first four division polynomials are

$$\psi_1 = 1, \qquad \psi_2 = 2y + a_1 x + a_3, \tag{19}$$
$$\psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8, \tag{20}$$
$$\psi_4 = (2y + a_1 x + a_3)(2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + b_4 b_8 - b_6^2) \tag{21}$$

Therefore, the nonlinear recurrence relations for division polynomial ψ_n when $n \geq 2$ are

$$2y\psi_{2n} = \psi_n(\psi_{n+1}h_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{22}$$
$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \tag{23}$$

4 ELLIPTIC NET SCALAR MULTIPLICATION OF RANK ONE

The first theory on elliptic net scalar multiplication was proposed by Kanayama et al. (2014) and followed by Chen et al. (2017), with both methods depend on

$\hat{W}(i) = \theta^{i^2-1}W(i)$ in their net. It is important to clarify that not all equivalences of proper elliptic divisibility sequences can be used to construct the rank one elliptic net. In our method, the equivalence theory in elliptic net lies on $\hat{W}(2) = 1$ and θ^j. We propose the following definition and lemmas for elliptic net scalar multiplication of rank one using the generalized equivalent elliptic divisibility sequence.

Definition 4.1. *Let $\{W(j)\}$ be the proper elliptic divisibility sequence over a finite field K and $gcd(2m+1,3) = 1$. Then $\hat{W}(j) = \theta^j W(j)$ is a sequence defined over K and $\hat{W}(2) = 1$ with $\theta^2 = W(2)^{-1}$.*

Lemma 4.1. *Consider $\{W(j)\}$ from Definition 4.1, and point $P = (x_1, y_1)$ on elliptic curve of the type $y^2 = Ax + B$ with $Char(K) \geq 5$. The elliptic net scalar multiplication of rank one $[k]P = (x_k, y_k)$ can be derived as,*

$$x_k = x_1 - \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} \tag{24}$$

$$y_k = \frac{\hat{W}(k-1)^2\hat{W}(k+2) - \hat{W}(k+1)^2\hat{W}(k-2)}{4y_1\hat{W}(k)^3} \tag{25}$$

Proof. Since $\hat{W}(j) = \theta^j W(j)$, this implies that $\hat{W}(j) = \theta^{-j}W(j)$. Then,

$$x_k = x_1 - \frac{W(k-1)W(k+1)}{W(k)^2} \tag{26}$$

$$= x_1 - \frac{\theta^{-(k-1)}\hat{W}(k-1)\theta^{-(k+1)}\hat{W}(k+1)}{[\theta^{-k}\hat{W}(k)]^2} \tag{27}$$

$$= x_1 - \frac{\theta^{-(k-1)-(k+1)}\hat{W}(k-1)\hat{W}(k+1)}{\theta^{-2k}\hat{W}(k)^2} \tag{28}$$

$$x_k = x_1 - \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} \tag{29}$$

and for

$$y_k = \frac{W(k-1)^2W(k+2) - W(k+1)^2W(k-2)}{4y_1W(k)^3} \tag{30}$$

$$= \frac{\left(\theta^{-(k-1)}\hat{W}(k-1)\right)^2\theta^{-(k+2)}\hat{W}(k+2) - \left(\theta^{-(k+1)}\hat{W}(k+1)\right)^2\theta^{-(k-2)}\hat{W}(k-2)}{4y_1\left(\theta^{-k}\hat{W}(k)\right)^3} \tag{31}$$

$$= \frac{\theta^{-2(k-1)}\hat{W}(k-1)^2\theta^{-(k+2)}\hat{W}(k+2) - \theta^{-2(k+1)}\hat{W}(k+1)^2\theta^{-(k-2)}\hat{W}(k-2)}{4y_1\left(\theta^{-k}\hat{W}(k)\right)^3} \tag{32}$$

$$= \frac{\theta^{-2k+2-k-2}\hat{W}(k-1)^2\hat{W}(k+2) - \theta^{-2k-2-k+2}\hat{W}(k+1)^2\hat{W}(k-2)}{4y_1\left(\theta^{-3k}\hat{W}(k)^3\right)} \tag{33}$$

$$y_k = \frac{\hat{W}(k-1)^2\hat{W}(k+2) - \hat{W}(k+1)^2\hat{W}(k-2)}{4y_1\hat{W}(k)^3} \tag{34}$$

■

Lemma 4.2. *Consider $\{W(j)\}$ from Definition 4.1, and point $P = (x_1, y_1)$ on a non-super singular elliptic curve of type $y^2 + xy = x^3 + a_2x^2 + a_6$ with $Char(K) = 2$. The elliptic net scalar multiplication of rank one $[k]P = (x_k, y_k)$ can be derived as,*

$$x_k = x_1 + \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} \tag{35}$$

$$y_k = x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right)\frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} + \frac{x_1\hat{W}(k+1)^2\hat{W}(k-2)}{\hat{W}(k)^3} \tag{36}$$

Proof. The derivation for x_k is similar to Lemma 4.1. We will proceed to prove for y_k as follows,

$$y_k = x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right) \frac{W(k-1)W(k+1)}{W(k)^2} + \frac{x_1 W(k+1)^2 W(k-2)}{W(k)^3} \tag{37}$$

$$= x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right) \frac{\theta^{-(k-1)}\hat{W}(k-1)\theta^{-(k+1)}\hat{W}(k+1)}{\left(\theta^{-k}\hat{W}(k)\right)^2} + \frac{x_1\left(\theta^{-(k+1)}\hat{W}(k+1)\right)^2 \theta^{-(k-2)}\hat{W}(k-2)}{\left(\theta^{-k}\hat{W}(k)\right)^3} \tag{38}$$

$$= x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right) \frac{\theta^{-2k}\hat{W}(k-1)\hat{W}(k+1)}{\theta^{-2k}\hat{W}(k)^2} + \frac{x_1\theta^{-2(k+1)}\hat{W}(k+1)^2\theta^{-(k-2)}\hat{W}(k-2)}{\theta^{-3k}\hat{W}(k)^3} \tag{39}$$

$$y_k = x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right) \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} + \frac{x_1\hat{W}(k+1)^2\hat{W}(k-2)}{\hat{W}(k)^3} \tag{40}$$

■

Significantly, the factor of θ^{-k} is in the simplest form by using the generalized sequence.

4.1 Discussion

The initial values in the elliptic net scalar multiplication of rank one are as follow:

$$\begin{aligned}
&\hat{W}(0) = 0, \quad \hat{W}(1) = 1, \quad \hat{W}(2) = 1, \quad \hat{W}(3) = \hat{p}, \quad \hat{W}(4) = \hat{q}, \\
&\hat{W}(5) = \hat{W}(3+2)\hat{W}(3-2) \\
&\qquad = \hat{W}(4)\hat{W}(2)[\hat{W}(2)]^2 - \hat{W}(3)\hat{W}(1)[\hat{W}(2)]^2 \\
&\qquad = \hat{q} - \hat{p}^3
\end{aligned} \tag{41}$$

Meanwhile, the required initial values for Stange method are

$$\begin{aligned}
&\hat{W}(0) = 0, \quad \hat{W}(1) = 1, \quad \hat{W}(2) = \hat{p}, \quad \hat{W}(3) = \hat{q}, \quad \hat{W}(4) = \hat{r}, \\
&\hat{W}(5) = \hat{W}(3+2)\hat{W}(3-2) \\
&\qquad = \hat{W}(4)\hat{W}(2)[\hat{W}(2)]^2 - \hat{W}(3)\hat{W}(1)[\hat{W}(2)]^2 \\
&\qquad = \hat{r}\hat{p}^3 - \hat{q}\hat{p}^2
\end{aligned} \tag{42}$$

$\hat{W}(5)$ is the last initial value required in the net. The next term for $\hat{W}(6)$ can be calculated using nonlinear recurrence relation of

$$\hat{W}(m+n)\hat{W}(m-n) = \hat{W}(m+1)\hat{W}(m-1)[\hat{W}(n)]^2 - \hat{W}(n+1)\hat{W}(n-1)[\hat{W}(m)]^2 \tag{43}$$

such that

$$\hat{W}(6) = \hat{W}(5)\hat{W}(3)[\hat{W}(2)]^2 - \hat{W}(3)\hat{W}(1)[\hat{W}(4)]^2 = \hat{p}[(\hat{q} - \hat{p}^3) - \hat{q}^2] \tag{44}$$

and in Stange method,

$$\hat{W}(6) = \hat{W}(5)\hat{W}(3)[\hat{W}(2)]^2 - \hat{W}(3)\hat{W}(1)[\hat{W}(4)]^2 = \hat{q}(\hat{r}\hat{p}^5 - \hat{q}\hat{p}^4) - \hat{r}^2 \tag{45}$$

Therefore, the elliptic net scalar multiplication (Chen et al., 2017) and our restriction are shown to provide better simplification.

We equip the following numerical instance for calculating elliptic net scalar multiplication:

Example 4.1. *Consider an elliptic curve* $E : y^2 + xy = x^3 + 1$ *and point* $P = (1, 0) \in E$*. After that,* $5P$ *is computed.*

Solution:

First, the initial values of elliptic net were obtained from division polynomials of equation 19 until equation 21. For $\psi_n = \hat{W}(n)$ then $\psi_0 = \hat{W}(0) = 0, \psi_1 = \hat{W}(1) = 1, \psi_2 = \hat{W}(2) = 1, \psi_3 = \hat{W}(3) = 18, \psi_4 = \hat{W}(4) = 27$.

From equation 35,

$$\begin{aligned} x_k &= x_1 + \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} \\ x_5 &= x_1 + \frac{\hat{W}(4)\hat{W}(6)}{\hat{W}(5)^2} \\ &= 1 + \frac{27(-12960)}{9^2} \\ &= -\frac{349839}{9^2} \end{aligned}$$

The y-coordinate was computed with equation 36, such that

$$\begin{aligned} y_k &= x_1 + y_1 + \left(1 + x_1 + \frac{y_1}{x_1}\right) \frac{\hat{W}(k-1)\hat{W}(k+1)}{\hat{W}(k)^2} + \frac{x_1 \hat{W}(k+1)^2 \hat{W}(k-2)}{\hat{W}(k)^3} \\ y_5 &= 1 + 0 + (1+1+0) \frac{\hat{W}(4)\hat{W}(6)}{\hat{W}(5)^2} + \frac{(1)\hat{W}(6)^2 \hat{W}(3)}{\hat{W}(5)^3} \\ &= 1 + (2)\frac{(27)(-12960)}{9^2} + \frac{(-12960)^2(18)}{9^3} \\ &= \frac{3017010969}{9^3} \end{aligned}$$

Therefore, when $P = (1,0), 5P = \left(-\frac{349839}{9^2}, \frac{3017010969}{9^3}\right)$.

Note that in order to generate point for elliptic curve stated in Lemma 4.1 and Lemma 4.2, there are five algorithmic method that can be used. The methods are the brute force search, sieve assisted search, homogeneous space search, Heegner point and canonical height search (Silverman, 1999). Among these, canonical height search computed faster with 28 digits of accuracy compared to others. In addition, the non-identity point on the elliptic curve can be generated by an explicit formulae (Everest and Ward, 2000). With q and u, be known as parameter of the elliptic curve of the type $y^2 + xy = x^3 + a_2x^2 + a_6$, the explicit formula of x and y coordinate are denoted as,

$$x = x_u = \sum_{n \in Z} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n \geq 1} \frac{nq^n}{(1-q^n)^2}$$
$$y = y_u = \sum_{n \in Z} \frac{q^{2n} u^2}{(1-q^n u)^3} + \sum_{n \geq 1} \frac{nq^n}{(1-q^n)^2}.$$

5 CONCLUSION

This research proposes a generalization of the equivalent elliptic divisibility sequences and uses the generalization form to derive the elliptic net scalar multiplication of rank one. Furthermore, the term in the proposed elliptic net scalar multiplication was found to be simpler than Stange method. Future research may consider other equivalence theory that satisfies the elliptic net.

ACKNOWLEDGMENTS

The author wishes to thank Universiti Selangor for providing complete research facilities as well as financial support for the project. The author also wishes to thank Miss Edora for formatting paper in Latex. A part of this paper has been presented during the 6^{th} International Cryptology and Information Security Conference (Muslim and Said, 2018).

REFERENCES

Bizim, O. (2009). On the elliptic divisibility sequences over finite. *World Academy of Science, Engineering and Technology*, 35:1011–1015.

Chen, B., Hu, C., and Zhao, C. (2017). A note on scalar multiplication using division polynomials. *IET Information Security*, 11(4):195–198.

Everest, G. and Ward, T. (2000). The canonical height of an algebraic point on an elliptic curve. *New York Journal of Mathematics*, 6:331342.

Gezer, B. and Bizim, O. (2009). Elliptic divisibility sequences in certain ranks over finite fields. *Hacettepe Journal of Mathematics and Statistics*, 38(2):161–171.

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*, E97A(1):300–302.

Lauter, K. E. and Stange, K. E. (2008). The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5381 LNCS:309–327.

Matsuda, S., Kanayama, N., Hess, F., and Okamoto, E. (2009). Optimised versions of the ate and twisted ate pairings. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E92A(7):1660–1667.

Muslim, N. and Said, M. R. (2018). Elliptic net scalar multiplication using generalized equivalent elliptic divisibility sequence. *In Proceedings of the 6th International Cryptology and Information Security Conference 2018*, page 925.

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.

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

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

Silverman, J. H. (1999). Computing rational points on rank 1 elliptic curves via l-series and canonical heights. *Mathematics of Computation*, 68(226):835858.

Silverman, J. H. and Stange, K. E. (2011). Terms in elliptic divisibility sequences divisible by their indices. *Acta Arithmetica*, 146(4):355–378.

Stange, K. E. (2007a). Elliptic nets and points on elliptic curves. *Algorithmic Number Theory*, (1):1–4.

Stange, K. E. (2007b). The tate pairing via elliptic nets. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4575 LNCS(1):329–348.

Tang, C. M., Ni, D. M., Xu, M. Z., Guo, B. A., and Qi, Y. F. (2014). Implementing optimized pairings with elliptic nets. *Science China Information Sciences*, 57(5):1–10.

Ward, M. (1948). Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70(1):31.